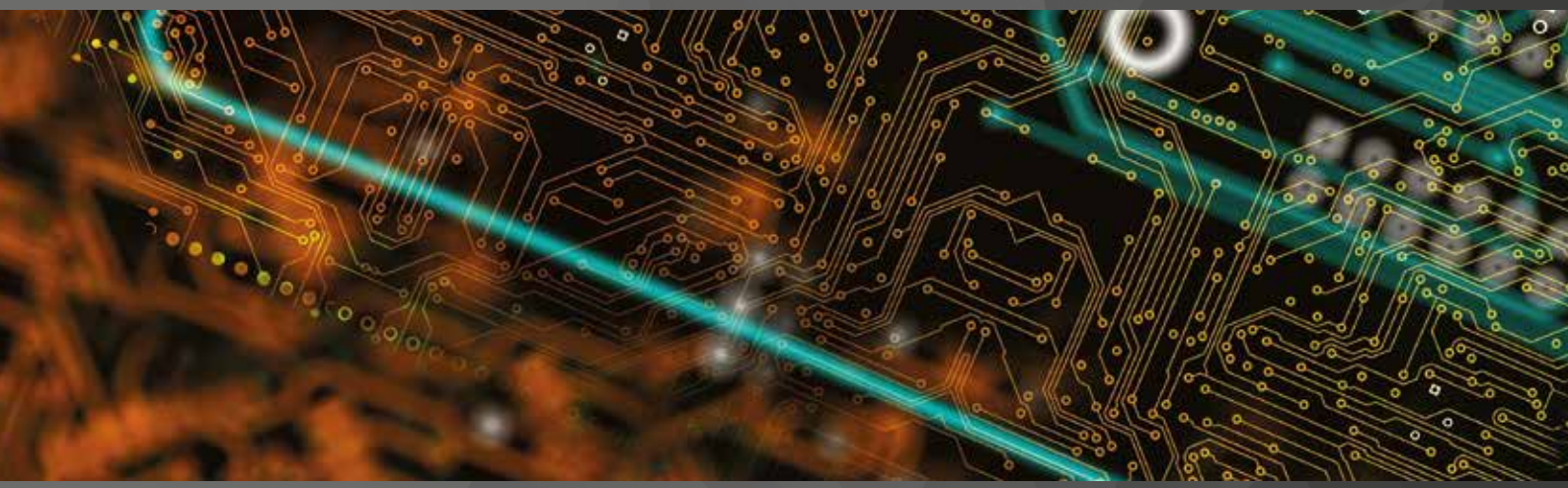
International Comparative Legal Guides



Cybersecurity 2021

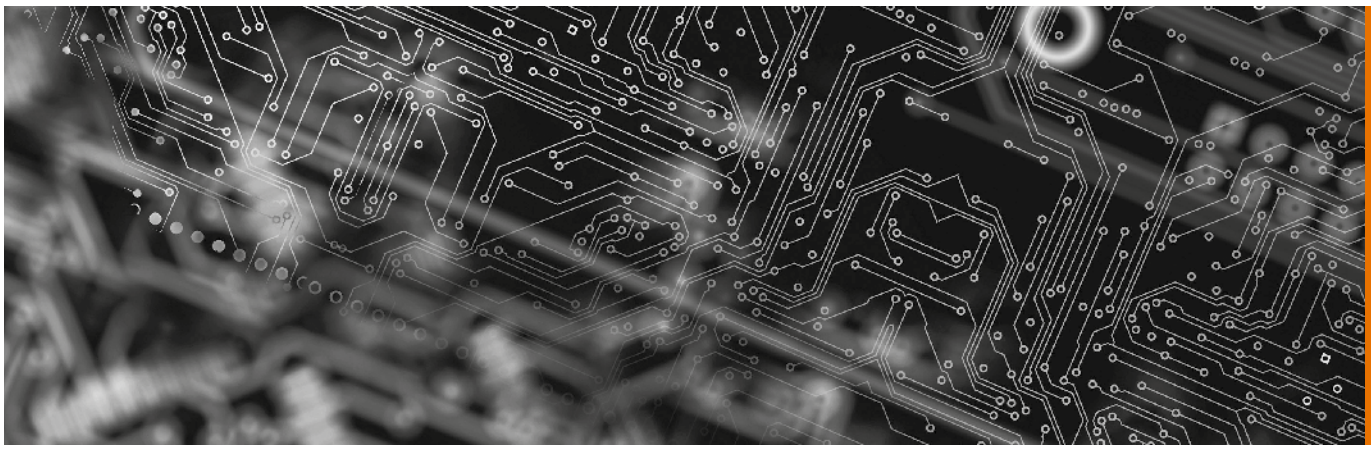
A practical cross-border insight into cybersecurity law

Fourth Edition

Featuring contributions from:

Alburhan
Allen & Overy LLP
Ankura Consulting Group
Creel, García-Cuéllar, Aiza y Enríquez
Drew & Napier LLC
Eversheds Sutherland (Germany) LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Ince
Iwata Godo
Kellerhals Carrard
King & Wood Mallesons
Kluge Advokatfirma AS
Lee & Ko
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan LLP
Mori Hamada & Matsumoto
Nikolinakos & Partners Law Firm
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Ropes & Gray LLP
Rothwell Figg
Rubino Avvocati
Schönherr Rechtsanwälte GmbH
Simion & Baciu
Sirius Legal
Stehlin & Associés
TIME DANOWSKY Advokatbyrå AB

ICLG.com



ISBN 978-1-83918-078-1
ISSN 2515-4206

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Consulting Group Publisher
Rory Smith

Publisher
James Strode

Sub Editor
Jenna Feasey

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Cybersecurity 2021

Fourth Edition

Contributing Editor:
Nigel Parker
Allen & Overy LLP

Expert Chapters

Q&A Chapters

From the Publisher

Dear Reader,

Welcome to the fourth edition of *ICLG – Cybersecurity*, published by Global Legal Group.

This publication provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to cybersecurity laws and regulations around the world, and is also available at www.iclg.com.

This year, five expert chapters provide insight into credential stuffing, emerging risks and threats, directors' liabilities, mitigating risks, and the use of AI.

The question and answer chapters, which in this edition cover 26 jurisdictions, provide detailed answers to common questions raised by professionals dealing with cybersecurity laws and regulations.

As always, this publication has been written by leading cybersecurity lawyers and industry specialists, for whose invaluable contributions the editors and publishers are extremely grateful.

Global Legal Group would also like to extend special thanks to contributing editor Nigel Parker of Allen & Overy LLP for his leadership, support and expertise in bringing this project to fruition.

Rory Smith
Consulting Group Publisher
Global Legal Group

ICLG.com

Get Stuffed! Are You Prepared for a Credential-Stuffing Attack?


Nigel Parker


Nathan Charnock

Allen & Overy LLP

Introduction

Cybercrime is estimated to cost the global economy $600 billion per year,[i] with over 15.1 billion records exposed by data breaches across the world during 2019.[ii] In recent years, and particularly during the onset of the COVID-19 pandemic in 2020, there has been a significant growth in the use of "credential stuffing" as a mode of attack.

These incidents involve an automated system, or "bot", exploiting genuine login credentials, likely stolen from another compromised website, or gained via phishing or other techniques, to try to gain access to a user account on a (previously uncompromised) website. Highlighting how easy it is to obtain compromised credentials, in early 2019 hackers posted an aggregated credential collection that contained the results of multiple data breaches, totalling 2.2 billion unique username and password combinations, all available to download for free. Shortly after, a further 841 million records were made available on the dark web, from 32 websites and apps, including MyHeritage and MyFitnessPal.

Whilst the primary motivation for these attacks is financial – gaining access to your online banking account or to a retail website where your payment card details are stored – access to user accounts can furnish the perpetrators with huge volumes of personal data for use in identity theft.

Many people use the same username and password combinations across multiple websites and credential-stuffing attacks take advantage of this behaviour. The dark web provides a lucrative underground marketplace within which billions of stolen account credentials can be bought and sold. Using a "bot" allows a criminal to scale up the process, enabling thousands of login attempts to be made in parallel, using different stolen credentials across multiple websites.

Companies who fall victim to these attacks can really pay the price; whilst reputational damage, regulatory fines and litigation costs can be significant, a credential-stuffing attack can also overwhelm your website and other technical infrastructure, causing severe business impact and putting a strain on IT, customer services and other resources.

So how do you prepare for a credential-stuffing attack? And how do you react when one occurs?

Preparing for a Credential-Stuffing Attack

Know your enemy

As is the case with other types of cyber-attack, companies should ensure they have, within their ranks, individuals with sufficient understanding of how credential-stuffing attacks typically materialise.

Credential stuffing is reasonably unsophisticated and easy to scale; the "bots" used are often off-the-shelf and readily available online, some free of charge! This makes it a popular weapon for cybercriminals. One of the most successful ways of "stuffing" is the "low and slow" method, which sees attackers hide their attack amongst a smokescreen of legitimate traffic, whilst limiting the number of attempts made. However, the more attempts made, the more valid login credentials will be identified. Just one data breach can put many other businesses at risk, as it can allow further unauthorised logins without breaching a company's infrastructure or triggering any security alerts or measures.

Companies should ensure they keep up to date with events and trends in this space and use that knowledge to inform their cybersecurity planning. Regular scanning of published lists of compromised credentials can also help head-off attacks.

Proactive monitoring

Proactive monitoring is one of the most effective tools to enable cybersecurity teams to identify and respond quickly and efficiently to credential-stuffing attacks. The National Cyber Security Centre recommends that businesses model their user login patterns and set-up of alerts, notifying the relevant IT monitoring teams of unusual activity or high volumes of traffic. For example, alerts could be set up to identify an increase in failed login attempts across numerous accounts, higher than normal volumes of foreign IP addresses or anomalies in browser activity that may indicate the use of automation. Companies can also use analytics to assess if a login attempt is authentic; for example, this could include ensuring the location and IP address of any login attempt is checked against the last successful login attempt, to allow a credibility judgment to be made in respect of each request. There are a number of third-party providers and tools on the market to assist businesses with monitoring activity.

Improve underlying security measures

Whilst monitoring can help companies to identify and respond to incidents, businesses should primarily focus on prevention techniques. Three things are needed to perpetrate credential stuffing: (i) a list of credentials; (ii) a target (this could be a general login on a web page or an API endpoint); and (iii) a bot or mechanism to leverage the stolen credentials. A number of tools can be leveraged to prevent access to the first and the second. Sadly, the bots are still widely available online.

1. **Protect the credentials**
   There are a number of things individual users can do to ensure that, even if their credentials are stolen, they can

protect themselves and the businesses they work for or have a relationship with. However, for businesses, the best way to protect against credential stuffing is to:

- encourage individuals to set unique passwords for different websites that they use;
- implement rules requiring passwords to contain a minimum of eight alphanumeric characters and a mixture of characters, including symbols; and
- force passwords to be reset periodically.

2. **Protect the target website login page or API**
Between May and October 2019, 75% of login attacks against financial services companies involved credential stuffing targeting APIs.[iii] When designing its API or website login page, a business should ensure it takes a number of steps to mitigate the risk of a successful credential-stuffing attack such as:
   - implementing multi-factor authentication;
   - enabling human verification systems such as reCAPTCHA;
   - using geofences to block proxy traffic that comes from certain jurisdictions, enabling access only from those jurisdictions where the business operates or provides services;
   - limiting the number of failed login attempts that can occur before locking the account and alerting the individual account owner of an issue;
   - using device or browser fingerprinting and requesting more information from users if they login from unknown devices;
   - using a neutral message for failed login attempts – for example if a "bot" enters a correct username but an incorrect password, do not inform it that "your password is incorrect" as the "bot" will know the username is correct;
   - run a TOR node to carry out additional checks on authentication attempts; and
   - deploy a network-based bot management solution as part of a multi-layered security implementation – these tools detect and control illegitimate bot traffic at the network edge, blocking attackers before they can get to your applications or overwhelm your infrastructure. Leading bot management platforms use artificial intelligence and machine learning to detect and thwart advanced credential-stuffing attacks.

It is worth noting that, as set out in this *International Comparative Legal Guide*, there are a number of legal obligations relating to cybersecurity that must be met by businesses. For example, under the GDPR, firms are required to process personal data securely by means of appropriate technical and organisational measures and they must take into account "the state of the art" when deciding what is appropriate. The state of the art continues to evolve and businesses should ensure their protections against credential-stuffing attacks evolve with this.

Incident response plan and procedures

Companies should ensure they have detailed incident response procedures in place and should conduct regular testing of these procedures to ensure relevant personnel understand their roles.

Access to appropriate expertise

It is strongly recommended that, as part of cybersecurity response planning, businesses ensure they have appropriate relationships and arrangements in place with a number of third-party advisors who can be called on, at short notice, to assist in the event of an incident, such as specialist cyber advisors and forensic IT experts, legal advisors and PR consultants.

Consider proactive measures

Google recently launched its "Password Check-up" feature which is built into its password manager, and therefore its Google Account and Chrome products. Password Check-up assesses the strength and security of all your saved passwords, tells you where Google finds they have been compromised in prior breaches and gives you personalised actionable recommendations when needed.[iv] This provides proactive protection for individuals, and if done without diminishing consumer experience or blocking legitimate traffic, it could be an effective tool to mitigate the risk of credential stuffing.

What Does an Effective Response to a Credential-Stuffing Attack Involve?

Implementing the measures outlined above will mitigate the risk of your business and your users from falling victim to a credential-stuffing attack. However, if an attack does occur, how should you respond? Each incident will present a unique set of circumstances, but we have set out below some of the steps you may need to take.

1. **Establish the facts** as quickly as possible to enable you to understand the scale and impact of the attack, including, amongst other things, when and how the attack took place, what information is known about the attacker (for example, is the same IP address being used?), the success rate of login attempts, the number of accounts accessed, the types of personal information accessed by the attackers, the value and nature of any financial loss to users or the business and whether other systems or group websites were affected/accessed.
2. **Instigate incident management procedures** involving key stakeholders from across the business which may include representatives from IT, security, legal, customer services, communications/public relations and the relevant product/corporate representatives and ensuring detailed incident logs are maintained to record decisions.
3. **Take initial remediation steps** in an attempt to stop the attack and prevent recurrence. This may involve, amongst other things: (i) temporarily suspending access to the API or login page, either in its entirety or from certain jurisdictions or IP addresses; (ii) conducting searches of the dark web to see if it is possible to identify if credentials have been stolen directly from your business for use in the attacks; (iii) deploying bot management solutions or adapting the way they are used; (iv) force-resetting user passwords to randomly generated passwords and requiring them to set a new password when they next log in; and (v) hiding payment card details or suspending cash-out or withdrawal options available on a user's account.
4. **Inform senior stakeholders** of events to ensure they are up to speed and able to take important decisions quickly, including dealing with any media interest.
5. **Instruct third party advisors** such as external IT/cyber consultants to help investigate and stop the attack and prevent reoccurrence, external legal counsel to advise the legal implications of the incident and to assist with regulatory reporting and PR/media consultants to help manage external and internal communications relating to the incident.

6. **Consider notifying law enforcement** – depending upon the nature, scale and severity of the credential-stuffing attack and local legal requirements, you should consider notifying law enforcement about the incident, as they may be able to assist with the investigation.
7. **Consider regulatory reporting obligations** that often require notifications to be made to the relevant regulator within a short time period (in some cases within just a few hours) after detection. In many jurisdictions, there are specific reporting requirements that apply to certain sectors, such as financial services and telecommunications whilst listed companies may have certain disclosure obligations that need to be met. Credential-stuffing attacks inherently involve the use of and access to personal data, so will often result in personal data breaches that in many jurisdictions may trigger an obligation to report to a data protection supervisory authority.
8. **Consider individual notification obligations** – there may be obligations under local legal requirements to notify affected individuals about the attack. For example, in the EU and the UK, the GDPR requires individuals to be notified without undue delay of personal data breaches that could result in a high risk to their rights and freedoms. There may also be circumstances in which you would choose to voluntarily notify individuals about the incident so that they can take certain steps. In any event, it will be important to ensure that:
    a. individuals are provided with all information required by law;
    b. practical and sensible advice is provided such as advising individuals to:
        i. monitor their payment cards and bank accounts for suspicious activity and report any such activity to their financial service providers;
        ii. reset their passwords, using unique passwords for each of their online accounts;
        iii. consider using a password manager;
        iv. input their usernames and email addresses into https://haveibeenpwned.com/, to see if their credentials have ever been stolen; and
        v. consider using anti-fraud credit monitoring services (which you may offer to pay for);
    c. customer services teams have sufficient information and resources to respond to queries which may be received from customers following distribution of the notifications, including queries received via social media;
    d. the notice is reviewed by communications specialists and legal counsel to ensure it strikes the right tone; and
    e. clearly identify which individuals have been affected and should receive the notification to avoid over-notification if possible.
9. **Consider other notification obligations** such as contractual obligations to notify third parties of certain cyber-incidents or data breaches.
10. **Work with other interested third parties, such as financial service providers** – if customers have had money withdrawn or removed from their accounts or their financial account or payment card details have been stolen, you should consider liaising with financial service providers to help prevent further fraudulent activity using customer information.
11. **Complete a detailed incident review** to understand how the credential-stuffing attack was able to succeed, to analyse how the business responded to the incident and what lessons could be learned, and to identify and agree short-, medium- and long-term remediation actions to be taken across the business to prevent the reoccurrence of credential-stuffing attacks in the future.

The COVID-19 Effect

In early 2020, as the COVID-19 pandemic hit the world, millions of people globally were instructed to self-isolate and people turned to the internet more than usual, often working from home, and away from some of the security protocols that protected them in the office. An opportunity arose for cyber criminals, as security was traded for ease of access, with the use of outdated software, the mixing of personal and corporate emails, and the recycling of passwords between business and personal environments.

There was a large spike in malicious login attempts against European video service providers and broadcasters during the first quarter of 2020. One attack in late March 2020, after many isolation protocols, directed nearly 350 million attempts against a single service provider over a 24-hour period. Separately, one broadcaster was hit with a barrage of attacks over the course of the quarter, resulting in billions of login attempts. Cyber criminals began to retry their credential stuffing lists, like those mentioned earlier in this piece, and test them against services rising in popularity in the pandemic, such as Zoom, that saw usage rise from 10 million users to over 200 million users in the first few months.

Conclusion

Credential stuffing is increasingly the weapon of choice for cyber criminals seeking financial gain. For businesses, it has never been more important to evaluate your cybersecurity offering to ensure you are prepared the threat of these incidents. Whilst the criminals may sometimes remain a few steps ahead, the businesses who implement a range of security measures, use appropriate monitoring and reporting tools and deploy effective incident response procedures are well placed to tell the criminals to "Get Stuffed!"

Endnotes

i. McAfee, "Economic Impact of Cybercrime – No Slowing Down", Report, February 2018, p. 4.
ii. Risk Based Security, "2019 Year End Report, Data Breach Quickview".
iii. Akamai, "Financial Services – Hostile Takeover Attempts", Vol. 6, Issue 1, p. 2.
iv. Tuerk, A., "To stay secure online, Password Check-up has your back", Google Blog, 2 October 2019.

Nigel Parker is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking proactive steps in response to attacks.
Nigel is recognised in *Chambers* and *The Legal 500*. He was named one of the "Top 40 under 40" data lawyers by *Global Data Review*.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3136
Email: nigel.parker@allenovery.com
URL: www.allenovery.com

Nathan Charnock is an associate specialising in commercial contracts, data protection and privacy, intellectual property and information technology law. He advises clients on their response to cybersecurity attacks, including their interactions with regulators and implementation of remediation steps. Nathan also advises on complex commercial arrangements for a range of clients in the technology, retail, telecommunication, life sciences and financial services sector, including IP licensing, outsourcing and service provision arrangements.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3899
Email: nathan.charnock@allenovery.com
URL: www.allenovery.com

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning over 40 offices. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.
We have a strong cybersecurity practice comprising a core team of 19 partners with diverse backgrounds in data protection, bank regulation, antitrust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity Incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.
www.allenovery.com

ALLEN & OVERY

Current and Emerging Cybersecurity Threats and Risks


Robert Olsen


Daron M. Hartvigsen


Brandon Catalan

Ankura Consulting Group

Introduction

Technology is a fundamental element of our global economic and social systems, making all that we experience and upon which we rely subject to cybersecurity risk. The rapid expansion of the internet and the Internet of Things, cloud computing, and related digital capabilities has created a complex network that we each fuel, virtually every moment. In tandem, cyber threats have evolved, becoming increasingly sophisticated and entrepreneurial. Cyber threat actors have proved nimble, adapting their tactics to outmanoeuvre the latest organisational detection abilities and defences. Comprehensive threat intelligence, robust data-security systems, and rigorous adherence to strict data-management policies help shield our economic and social infrastructure; however, recent events underscore that the risk landscape is vast.

Prevailing circumstances are riddled with uncertainty. In dramatic fashion, the world has been forced to contend with the outbreak of COVID-19 and its transformative physical and digital effects. The necessary response to the pandemic propelled an abrupt shift to remote work in both the public and private sectors. Largely, early concerns about bandwidth and resource availability did not occur, but cyber risk conditions did ensue. For most, cyberspace has become the primary venue for information and conjecture about the science and implications of the virus, only increasing interactions of bad actors and targets.

Cyber threat actors, both criminal and nation-state sponsored, have deftly exploited current events – the pandemic, protests, political campaigns – to target would-be victims with socially engineered messaging, social media content, and other methods. Credential theft and password spraying are the typical initial steps to gain access to networks and systems followed by espionage, ransom, financial crimes, and other deleterious effects. State-sponsored information-operations campaigns are especially active around U.S. elections and critical infrastructure, a craft honed through successful information operations campaigns already deployed globally. Further, an increase in the use of extortion by cyber criminals has risen precipitously. This nefarious innovation, representing a maturation of criminal business strategy, requires potential victims to calibrate prevention, detection, and response postures. Victims increasingly include law firms, whose client data and trove of confidential information represent lucrative opportunities for hackers and attackers. According to an American Bar Association study, an estimated 25% of U.S. law firms have been breached.[1]

The near-future will involve ever-increasing sophistication and wide-spread criminal activity enabled by the ubiquitous nature of cyberspace. We expect nation-states and their surrogates to mature efforts to disrupt economic, social, and political environments across the globe. Criminals, whether sponsored by a nation-state or operating independently, will continue to target and steal intellectual property for their gain. Bad actors will exploit gaps in human and technical security to convert data access into money. And, with remote workforces not expected to return to offices for the foreseeable future, the conditions are ripe for illicit access.

Corporate and Industrial Vulnerabilities

The threat landscape for commercial and industrial enterprises continues to evolve. Confidential data, financial information, and intellectual property represent the primary targets for exploitation by criminals and nation-states. Social engineering continues to be the most common tactic for unauthorised access to a target of interest. As an example, an energy sector entity believed a foreign competitor was using ill-gotten confidential and sensitive information to underbid futures contracts. Interviews of employees of interest, together with reviews of relevant logs, systems and tracking mechanisms, revealed that unauthorised access to a vital employee's email was confirmed through email access records that highlighted the effectiveness of advanced tracking mechanisms embedded in and attached to documents in the email. The content of the audit email was consistent with the email traffic suspected of being improperly accessed. Within 12 hours of sending the audit email to the vital employee, the email was opened from a device whose IP was owned and registered to the U.S. subsidiary of a competitor company. Within 24 hours, the email and attachment had been opened in the foreign-based headquarters of the company's competitor. This evidence is being used to pursue a multi-million-dollar recovery.

Fuelled by both the growing number of individuals forced to work remotely due to the COVID-19 pandemic as well as opportunistic threat actors exploiting critical vulnerabilities associated with industrial virtual private network (VPN) platforms, there is a significant rise in the number of compromised VPN accounts being sold across various Dark Web forums and marketplaces.

In response to these types of threats, large companies, financial institutions, and governments have invested hundreds of millions of dollars to protect their data, property, and systems. However, vendors in the supply chain, of varying financial strength and sophistication, may not have matched the pace of investment of large entities. Cyber attackers have targeted and exploited this lack of symmetry and "weakest link", using third parties in a bid to manoeuvre up the ladder to a more lucrative victim. Supply chain connections will require additional attention in the near-term.

State-Sponsored Groups

The "digital information age" is entering its fourth decade and the internet and cyberspace have proven a vital enabler for the exploitation of military, political, and critical infrastructure by nation-states. Prior to the widespread adoption of computers and the use of the World Wide Web, nation-state efforts were conducted through human and signals intelligence activity. Cyberspace changed the paradigm, enabling a new model of access and collections. Now, cyberspace operations and collections are a key component of intelligence, counterintelligence, and effects operations.

For example, as more devices and sensitive data are exposed to the internet, nation-states will continue to invest resources to steal, deny, or destroy them, with the end goal dependent on the demand of the source. Governments will rely on cyber-warfare capabilities to deny access to, degrade, or destroy a resource, such as a power resource. A notable example is the destruction of Iranian centrifuges in late 2009 and early 2010. More recently, state-sponsored actors have been attempting to infiltrate healthcare entities in a bid to obtain information about COVID-19 research and treatments. At the same time, the advent and proliferation of social media has enabled nation-states and their surrogates – as well as unaffiliated individuals who may be inspired by them – to use misinformation and disinformation with the goal of social disruption and/or to undermine political stability.

The U.S. intelligence and counterintelligence communities have identified primary threats to Western interests as originating from four countries:

- China.
- Russia.
- Iran.
- North Korea.

Many countries are developing organic capabilities or outsourcing cyber-exploitation. However, we observe that Chinese, Russian, Iranian, and North Korean tactics surface more often than other sources.

China

To further strategic ambitions, both regionally and internationally, the People's Republic of China has invested heavily in cyber resources devoted to cyber activities in three primary areas: influence operations; financial gain; and intellectual property theft.

China employs thousands of individuals who work online to target people and entities that the government wants to manage and control.[2,3] These entities include the internal population, Chinese dissidents living abroad, international public opinion, commercial concerns, and diplomats. Chinese efforts to influence are often targeted and scale during key periods like important election cycles, yet occur constantly and consistently, executed through news organisations, social media, content delivery services, and other means.

China's cyberspace capabilities have proven effective at supporting and maturing China's economy. To date, China been successful at securing trade secrets, intellectual property, and emerging technology. So much so that President Barack Obama directly asked China to stop, and the U.S. followed on with multiple indictments of Chinese actors for theft.[4,5] Intellectual property theft is likely to expand as the Chinese economy grows and scales. Whether companies have a presence in China or not, they must consider cybersecurity as they innovate and go to market or they may find themselves in competition with their own designs fielded by Chinese firms.

Finally, governments around the world are all too familiar with Chinese strategic objectives, especially in the Asia Pacific region and along the borders of India. Under the current leadership, China is looking to solidify its position as a dominant military, economic, and political power and to extend its influence and economic footholds in countries in Latin America and Africa. As China targets adversaries and pursues its interests, it will continue to invest in increasingly sophisticated intelligence and cyber capabilities.

Russia

Russia's multi-faceted strategic agenda has proved less effective at monetising its cyber efforts. As cyberspace evolved, Russia pursued a different agenda, focusing more on enabling intelligence and less on economic advantage.

When the Russian government does pursue intellectual property, it is often done as a national security objective to produce similar technologies or create countermeasures to adversarial technologies. Where Russia has been successful is in its ability to leverage its cyber espionage and warfare capabilities to collect intelligence and create desired effects. Recently, those desired effects have been realised through influence and disruption campaigns related to elections in the U.S. and around the world. A divided and less cohesive Western world works to Russia's advantage and enables Russia to more freely operate on the global stage.

Russian criminal enterprises have emerged as prime suspects in major financial fraud and cyber-theft cases around the world. The link these criminals have to Russian state entities has been reported in some cases as direct. Whether enabled by the government or not, Russian criminal groups are highly effective. Criminal or civil legal pursuits of Russian criminals are not often productive in generating remedies, though at times civil court actions can provide the victim with information related to the who, what, when, and where that could create some future advantage or insight.

Iran

The Islamic Republic of Iran represents a different type of foe compared to China and Russia. Faced with wide-ranging and deeply damaging economic sanctions that target key industries and high-profile individuals, the government is in survival mode.

Iran's cyber-espionage programmes have been tasked with conducting financial fraud as well as the theft of intellectual property to increase internal revenue. Iran has also used cyber-warfare campaigns to disrupt or destroy foreign industry in retaliation for sanctions or to increase profits at home. The recent drone attacks targeting Saudi oil infrastructure are a likely example of an attempt to drive the price of oil up for their benefit. Another example involved Iranian actors reportedly using Shamoon malware to target offices and installations of Saudi Aramco, Saudi Arabia's state-owned petroleum and petrochemical conglomerate.[6]

In 2020, a U.S.-based research hospital engaged in COVID-19 research was targeted by actors believed to be in Iran and associated with a threat group known as the "Mabna Institute", whose origins date to at least 2013. Available reporting on Mabna Institute links its actors to cyber-exploitation campaigns targeting hundreds of universities and several dozen private companies around the world, as well as several U.S. state and federal government agencies.

Analysis revealed that the actors conducted a "password spray attack", generating several thousand login failures over a one-hour period. The tactic was eventually successful and allowed the actors to derive credentials for several hospital employees. The actors used those passwords during opportune times where the users assumed the resulting Multifactor Authentication (MFA) challenge was for their legitimate access request. Once in, the threat actors conducted reconnaissance and collections activity.

North Korea

As of September 2020, the entire Democratic People's Republic of Korea (DPRK) has only 1,024 IP addresses directly allocated to its announced "STAR-KP" prefix.[7] However, North Korea successfully leverages its seemingly insignificant internet footprint and underdeveloped infrastructure to carry out highly targeted cyber campaigns, generating unknown amounts of illegal revenue and countless gigabytes of stolen intellectual property from unsuspecting foreign governments and private organisations.

Since at least 2009, North Korea has invested heavily in offensive cyber capabilities, with an emphasis on highly skilled human operators educated both inside North Korea and abroad in Russia and China[8] as well as creating proprietary software and hardware to reduce its dependency on foreign technologies. As an example, in 2017, "Lazarus", a threat group attributed to North Korea, successfully carried out a widescale cyber campaign utilising custom-built malicious code to shut down over 300,000 computers across 150 countries, including the U.S., UK, Australia, Canada and New Zealand.[9] Allegedly, North Korean cyber operations have targeted global financial institutions resulting in the theft of millions of U.S. dollars from its victims. For instance, it is believed that North Korean actors were behind a 2016 campaign that targeted a network owned by the Central Bank of Bangladesh, resulting in the exfiltration of $81 million from its New York Federal Reserve accounts.[10]

More recently, Lazarus has been attributed to a cyber espionage campaign targeting several U.S.-based aerospace and defence contractors to steal intelligence on critical military and energy technologies. Analysis revealed that Lazarus threat actors leveraged a newly created remote access trojan, "Blindingcan", which allows an attacker to perform reconnaissance of the infected network as well as search, read, write, move, and execute files on compromised machines.[11]

North Korea will continue to leverage its cyber resources to access desired military and economically valuable technologies as well as to offset financial losses due to increasing international sanctions. Additionally, as North Korea becomes more reliant on Chinese and Russian aid, North Korean infrastructure and manpower will support the intelligence and warfare requirements of these countries.

Criminal Groups

Criminal groups are the most visible, well publicised and, for most companies and professional services firms, largest threat. Unlike nation-states, these actors are primarily motivated by financial gain as they seek to monetise unauthorised access. Among the most active and notorious examples in this category are the ransom and extortion groups Maze, Ryuk, and REvil. Their many victims span economies and governments and have included local and state governments, commercial entities, celebrities, legal practices, agricultural, insurance, and the energy sector.

Data ransom remains a popular tactic. As companies and other potential victims matured defences, this form of attack has shifted from encrypting systems to lock out legitimate owners and users to ransom groups exfiltrating sensitive data before they encrypt the systems. Under this more advanced scenario, in the event the victims opted not to pay the ransom (because they could recover their systems adequately without the decryption key), the bad actors can then threaten to expose their data on the internet, a move that has helped guarantee a payout.

Business email compromises are a common gateway to financial exploitation. Criminals target key individuals in the organisation and send crafted emails designed to mislead the recipient. They so convincingly mimic legitimate traffic that recipients may type credentials into what appears to be an actual login page. After harvesting the employees' credentials through social engineering campaigns or sourcing them through other avenues of security compromise like DarkWeb channels, the criminal actors log on to the environment, conduct reconnaissance and learn about the organisation. Armed with this knowledge, bad actors masquerade as legitimate employees, hijack legitimate conversations, and convince company employees to change routing instructions for payments. We have also observed criminal actors submit false invoices and even access third-party payroll services to re-direct paychecks, using this tactic. Further, there is an emerging threat across various open source and Dark Web forums: suspected "espionage-for-hire" teams who are deploying innovative ransomware and extortion tactics. Taken together, clearly the cybercrime business model is maturing quickly.

Recommendations

The necessity for cybersecurity is evident. Here are our recommendations to bolster security:

- Enable monitoring of mail servers to identify evidence of suspicious redirects or unauthorised commands.
- Use multi-factor authentication to limit the impact of potential credential theft.
- Deploy secure VPN technology for remote workers.
- Implement content scanning and filtering technology to detect and defend against malicious links and attachments.
- Back up systems regularly so that if attacked, the system can be restored (also quickly secure the backed-up environment to prevent re-attack).
- Invest in end-point monitoring, reputable antivirus software, and the best firewall that your company can afford. Configure and monitor all for the best security posture possible.
- Block the macro execution for Microsoft Office documents to prevent the execution of embedded malcode.
- Ensure your cybersecurity defences include processes that detect and contain recently identified variants of malware.
- Conduct employee training to educate end-users on recent social engineering techniques being employed by both criminals and nation-state actors.

Endnotes

1. https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.
2. https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.
3. https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.
4. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
5. https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.
6. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.
7. https://ipinfo.io/AS131279#gen_info.
8. https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/.
9. https://home.treasury.gov/news/press-releases/sm774.
10. https://fas.org/irp/world/dprk/dod-2017.pdf.
11. https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a.

Robert Olsen serves as the global cybersecurity and privacy practice leader, which encompasses the Americas, EMEA and APAC regions. He is a Senior Managing Director at Ankura with over 25 years of experience developing, implementing, and managing complex cybersecurity and enterprise risk management programmes. Additionally, Robert serves as a chief information security officer and board advisor for clients across a diverse set of industries and organisational sizes. He is a thought leader in the provision of technology, cybersecurity and privacy risk advisory services to government, private industry, and not-for-profit clients. Robert is also an advisory board member for Johns Hopkins University's Information Security Institute.

Ankura Consulting Group
250 South President Street, Suite 2300
Baltimore, MD, 21202
USA

Tel: +1 410 340 3560
Email: robert.olsen@ankura.com
URL: www.ankura.com

Daron M. Hartvigsen is a Managing Director at Ankura and a cybersecurity practice leader delivering incident response, cyber investigations, and cyber threat analytics solutions. Daron leverages his 23-year career as a Federal Agent and his experience with U.S. intelligence, counterintelligence, and law enforcement to manage and oversee complex breach events, investigate information compromise issues, pursue nation-state sponsored entities, and assist clients with the prosecution of cyber threat actors.

Ankura Consulting Group
2000 K Street NW, 12th Floor
Washington, D.C., 20006
USA

Tel: +1 202 797 1111
Email: daron.hartvigsen@ankura.com
URL: www.ankura.com

Brandon Catalan is a Senior Director at Ankura, based in Boston. Brandon has 15 years of experience in the threat intelligence and computer forensics field, including a multitude of technical leaderships roles within the Defense Industrial Base directing incident response and tier III intelligence teams. He provides cybersecurity expertise and leadership to clients in threat intelligence and analytics, forensic analysis, malware reverse engineering as well as strategic and tactical cyber operations. In previous roles, Brandon provided counterintelligence support to focused cyber operations and research pertaining to advanced persistent threat (APT) tactics, techniques, and procedures. His work has been published in the *Wall Street Journal* and various other media outlets, company blogs, and by leading defence industry associations. He has been credited for his work on intelligence community assessments relating to cyber threats and has presented at a variety of Department of Defense and commercial conferences and symposiums.

Ankura Consulting Group
1 Beacon Street, Floor 15
Boston, MA, 02108
USA

Tel: +1 202 797 1111
Email: brandon.catalan@ankura.com
URL: www.ankura.com

Phantom Responsibility: How Data Security and Privacy Lapses Lead to Personal Liability for Officers and Directors

Rothwell Figg

Christopher Ott

Boards of directors ignore data security and privacy risks to companies at the peril of their companies and – increasingly – their own personal liability. A business has its operations halted by ransomware approximately every 10 seconds. Billions of records are exposed every fiscal quarter. The global costs of these breaches and online crime reaches the trillions every year. These potential costs have elevated data security and privacy issues from mere "IT issues", or compliance *minutiae*, to the centrepiece of strategic risk management. The law has grown to match this reality. As a result, boards face expanding personal legal liability for the company's data security and privacy failures.

This upwards liability trend is not new. As early as 2014, the National Association of Corporate Directors' (NACD) *Handbook on Cyber-Risk Oversight* provided core cybersecurity principles to members of public companies, private companies, and nonprofit organisations of all sizes and in every industry sector. The NACD directed board members to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an issue for the IT team. As an established enterprise-wide risk, cybersecurity therefore began triggering boards' existing legal obligations. In the same year as the NACD handbook's admonition, 2014, SEC (Securities and Exchange Commission) Commissioner Luis Aquilar stated that "boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility do so at their own peril".

Those perils are changing in real time just as cybersecurity and privacy threats are changing. However, we can identify certain concrete areas of established liability and strategically identify the emergent risks. Right now, the main liability risks to boards include:

- SEC liability for cyber risks;
- SEC liability for privacy risks;
- officer and directors' civil liability for breached fiduciary duties;
- direct liability for violation of state data security and privacy statutes, with special emphasis on California;
- criminal liability for cybersecurity and privacy failures; and
- global civil and regulatory liability, with special focus on the New York Department of Financial Services (NYDFS) and European Union (EU) regulations.

In the following pages, we attempt to explore all of these current trends. To end, we will also tackle a few harder-to-classify risks related to United States national security oversight of cyber readiness.

United States: Officer and Directors' Personal Liability for Cybersecurity and Privacy Failures

On February 21, 2018, the SEC "voted unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents".[1] The SEC did not wait long for the public to absorb this guidance. On April 24, 2018, the SEC "announced that the entity formerly known as Yahoo! Inc. has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts".[2] In the space of two months, the SEC went from "[c]ompanies also may have disclosure obligations" for breaches, to paying $35 million for failure to disclose.[3] When the expectations change so quickly, it is important for officers and directors to understand both the current and developing state of cyber and privacy risks, especially when it comes to personal liability.

SEC liability

The SEC maintains broad (and expanding) authority over directors. This authority begins the moment that a director is named. SEC proxy disclosure rules, among other requirements, mandate that companies disclose, for each director and nominee, the specific experience, qualifications, attributes, or skills that led to the conclusion that the individual should serve as a director of the company in light of its business and structure.[4] This disclosure must be made on an individual basis, and be specifically linked to the biographical description of each director and nominee. These new disclosure requirements theoretically expose directors to greater potential liability if they are identified in an SEC filing as having a particularly valuable skill or expertise that is valued and relied upon by the company.

The pitfalls of director "cyber hype"

Directors and their companies often tout directors' particular skills that they bring to the board. It makes sense, therefore, that a director may tout their particular cybersecurity *bona fides*. However, overselling one's cyber skills can bring individual

liability. In 2003, the SEC amended the proxy disclosure rules to require that a company disclose whether it has at least one "audit committee financial expert" on its audit committee.[5] Prior rules indicated that identifying a director as an expert did not increase their liability for registration statements pursuant to Section 11 of the Securities Act of 1933 (Securities Act), dealing with liability in connection with registration statements. The safe harbor covered more than merely directors' financial expertise. However, the entire safe harbor language was removed in the wake of the Sarbanes-Oxley Act. Therefore, real individual liability risks flow from whenever a board member touts their expertise in any field, including cybersecurity and privacy.

Section 11 of the Securities Act imposes civil liability on directors of an issuer if "any part of the registration statement, when such part became effective, contained an untrue statement of a material fact or omitted to state a material fact required to be stated therein or necessary to make the statements therein not misleading". Therefore, directors face a real dilemma in that they feel that they should tout their material skills to current and potential shareholders, but responsibility and liability flow from those representations. Fortunately, there are many defences available to directors that turn on their level of knowledge.[6] These same defences could be utilised to defend against a Section 11 claim levelled against a director.

Board cybersecurity and privacy risk oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure.[7] The Commission has previously said that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company".[8] The SEC has expressly stated that cybersecurity risks are among those that must be reported to directors, with all of the criminal and civil liability that may flow from that notice.[9]

Cybersecurity risks and scrutiny of board trading activities

Directors also will face scrutiny for their trades after they are advised of cybersecurity risks. In the wrong situation, a trade could be considered to be an insider trade on non-public information. There is a delicate balance that must be reached here. After all, directors should righteously be informed of significant risks, such as cybersecurity or accounting matters. However, directors must internalise that their cybersecurity briefings can be every bit as material as their regular briefings on accounting controls or other vintage risks. Currently, however, director understanding may be lagging behind their responsibilities.

In the recent massive Equifax breach, multiple insiders have been charged for trading on the breach information.[10] The SEC has indicated that it will make this type of trading a particular focus.[11] For this reason, the SEC advises that "[c]ompanies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on the basis of material non-public information about cybersecurity risks and incidents".[12] That may be easier said than done.

As a practical matter, companies can start to protect their officers and directors from this type of scrutiny (and prevent the underlying suspect behaviour) by establishing policies and procedures in place that: (1) expressly address trading blackouts or similar procedures that will prevent directors, officers, and other corporate insiders from trading during the heightened period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material non-public information about the incident; (2) provide regular training to all insiders about cybersecurity risks that must be treated like any other material enterprise risks; and (3) ensure that the company makes quick and timely disclosure of any material non-public cybersecurity information.

Officer and director fiduciary duty law and personal civil liability

Officers and directors can face civil liability if they breach their fiduciary duties, which can lead to a shareholder derivative action wherein the shareholders sue the officers and directors for breaches that harmed the company. Technically, every state has its own standards regarding the fiduciary duties that officers and directors owe to companies and, by extension, the shareholders. Because so many companies are incorporated there, Delaware generally leads the way of fiduciary duty issues. Under Delaware law, directors owe fiduciary duties of care and loyalty to the company.[13] This fiduciary duty of care requires directors to act with a degree of care that ordinary careful and prudent men would use in similar circumstances.[14] Under this standard, directors must act on an informed basis, in good faith, and in the honest belief that the action was in the best interests of the company.[15] Courts have interpreted this duty of loyalty further to include a duty of oversight, which will be breached if directors "utterly fail" to implement any reporting or information systems or controls or if, after implementing these systems, directors fail to monitor or oversee the operation of these plans.[16] Therefore, Delaware law clearly establishes that officers and directors must set up informational and reporting systems and monitor the results of those systems.

It does not take much imagination to see how these standards could be applied to the new information technology and cybersecurity systems that boards oversee in various companies. A number of derivative actions have been filed following high-profile data breaches. These actions are typically based on claims that, by failing to implement adequate information security policies, the directors allowed a breach to occur which damaged shareholders through decreased stock prices. Although claimants in these cases face a high pleading standard, which we will discuss below, the cases remain expensive and disruptive. Indeed, they can often to lead to resignations by officers and directors.

Civil liability for false and misleading public cybersecurity statements

Companies' public cybersecurity statements or even certain kinds of silence can also create officer and director liability. Exchange Act Section 10(b) and Rule 10b-5 prohibit, *inter alia*, making untrue or misleading statements of material fact. These laws further prohibit selective silence about these material facts. Therefore, omitting material facts must not be left unstated if

they are necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading. This last requirement is a mouthful. However, in more accessible language: one has to tell the truth about anything that is important to the company, and one must volunteer facts wherever silence on those facts will actually mislead someone. These requirements to be truthful and forthcoming with the public could conceivably create significant officer and director cyber liability in civil class actions. However, this type of liability will not attach merely when someone wishes to second-guess the content and omissions of companies' cybersecurity statements. As with many liability issues, the quantum of one's knowledge matters.

Unlike Section 11 of the Securities Act, which we discussed earlier when it comes to exaggerating directors' cybersecurity skills, Section 10(b) requires the intent to deceive, manipulate, or defraud, otherwise known as "*scienter*". Without proof that the director acted with corrupt *scienter*, there can be no Section 10(b) liability. This proof of *scienter* will be absent for many, although not all, officers and directors.

Expert experience and director liability

Experience and context matter when it comes to *scienter*. Directors with particular technical or cybersecurity expertise may have difficulty getting Rule 10b-5 claims dismissed because it may be easier for plaintiffs to plead *scienter* as to them. The *In re U.S. Bioscience Securities Litigation*[17] involved a class action by purchasers of a company's stock against the directors. The judge denied a motion to dismiss Section 10(b) claims against certain outside directors of the company for alleged misstatements, contained in the annual Form 10-K, suggesting that one of the company's products was more effective and further along in clinical trials than was warranted by the facts. In rejecting the motion, the judge explained that "[o]utside directors can be of two very different kinds", those whose role is not intended to be hands on and those who have valuable expertise in the industry.[18] In the latter case, the directors' "valuable expertise in [the company's] industry" made it reasonable to assume that the directors had inside director knowledge for which they could be held liable.[19]

Similarly, in *Tischler v. Baltimore Bancorp*,[20] a class action brought by purchasers of Baltimore Bancorp stock, the plaintiff alleged, in relevant part, that the outside directors were liable under Section 10(b) of the Exchange Act and Rule 10b-5 for a purportedly false press release about the adequacy of an offer for the company. In evaluating the defendants' motion to dismiss, the Court dove into the different types of directors and their level of regular briefings. For this reason, the audit committee members substantively briefed about the purchase offer had liability. The judge did not stop there, however. Where the outside directors had special knowledge of the company's field, the judge concluded that they knew, or should have known, of the risks to the company.[21]

Second-guessing board decision-making

As mentioned above, some of these risks flow directly from the content of public disclosures, but others come from evaluating the objective quality – in light of the attendant circumstances – of officer and director decisions. Officers and directors have a duty of care to the corporation. "Duty of care" refers to a fiduciary responsibility held by company directors to live up to a certain baseline standard of care. This ethical and legal duty requires officers and directors to render their decisions in good faith and in a reasonably prudent manner. That second clause, "reasonably prudent manner", provides the legal ammunition to second-guess failed decisions. Shareholders can probe the reasonableness of officer and director decision-making by bringing shareholder derivative actions. These derivative actions argue that officers and directors violated their duty of care when it comes to one or more decisions and therefore injured the company itself. The areas of decision-making failures have run the gamut, from poor business decisions, to accounting fraud, bribery, rampant officer looting, and – increasingly – to failures to provide adequate cybersecurity safeguards.

The Delaware Chancery Court held in *In re Caremark International Inc. Derivative Litigation*[22] (*Caremark*) that the board has an obligation to at least attempt in good faith to invest in or implement a monitoring system that is sufficient to identify legal breaches by the corporation. In *Caremark*, shareholders brought derivative suits against the company, alleging that Caremark's directors breached their duty of care by failing to adequately oversee the conduct of Caremark's employees regarding kickback payments to doctors for Medicare or Medicaid referrals, which is a crime, thereby exposing the company to significant civil and criminal penalties. *Caremark*'s holding outlined director liability for a breach of the duty to exercise appropriate care in two distinct contexts: (1) "from a board decision that results in a loss because that decision was ill advised or 'negligent'"; or (2) "from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss."[23] The *Caremark* Court further held that: "it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility." While all of these individual parts of the *Caremark* decision are important, the board must have failed to provide reasonable oversight in a "sustained and systematic fashion", or the information reporting system must be an "utter failure".

Cybersecurity crises of all stripes, including (but not limited to) ransomware response, have now become a staple of derivative lawsuits. Indeed, these claims have become so prevalent that we now have formal court opinions holding that derivative actions against boards for ransomware failures constitute the types of central case that must be covered by director and officer liability insurance.

This does not mean that these cases are always successful. For example, in *Corporate Risk Holdings LLC v. Rowlands*,[24] the court concluded that the case solely "amounts to an allegation that the Board knew about the risk posed by a cyberattack, but did not adequately monitor [the company]'s cybersecurity efforts".[25] Where plaintiffs "focus on a specific, industry-wide risk [the allegations are] . . . not sufficient to support a *Caremark* claim".[26] For example, directors of banks who failed to recognise the risks associated with the subprime lending market could not be found, merely by ignoring the publicised risks, to have acted in bad faith.[27]

Still, there must be a reporting system so that the board can exercise oversight, and companies often have weak reporting systems. Recently, the *Marchand v. Barnhill, et al.* (*Marchand*)[28] case concerned a listeria outbreak involving Blue Bell ice cream that made many consumers ill and resulted in a total product recall. The *Marchand* court held that the board failed to provide adequate oversight of a key risk area and thus breached its duties. Consistent with *Caremark*: (a) the directors must have utterly failed to implement any reporting or information system or controls; or (b) having implemented appropriate compliance controls, the directors consciously failed to monitor or oversee the operation of that system. In *Marchand*, the court found a lack of board oversight because the Blue Bell board failed to implement any system

for Blue Bell's food safety performance or compliance. It does not take much imagination for this same analysis to apply in the cybersecurity context, especially if the company's products are particularly vulnerable to cyberattack. After all, a reasonableness standard will always move and change over time, and accounting fraud oversight was not the responsibility of the board a generation ago. Now, account committees and special risk committees roam the corporate boardrooms in giant herds. The goal of a company is not to hope that things stay the same. Rather, a dynamic, forward-thinking company tries to anticipate the next risk before their directors face personal liability.

However, for now, directors can and should allege that all such allegations of the breach of cyber duty of care constitute "a classic example of the difference between allegations of a breach of the duty of care (involving gross negligence) as opposed to the duty of loyalty (involving allegations of bad-faith conscious disregard of fiduciary duties)".[29] These standards are even more daunting for plaintiffs when "the claims involve a failure to monitor business risk, as opposed to legal risk".[30]

Special director knowledge, Delaware law, and the Section 141(e) "safe harbor"

Delaware case law paints a slightly different outlook as to whether independent directors will be held to a higher fiduciary duty standard because of their special expertise. The *In re Citigroup Inc. Shareholder Derivative Litigation*[31] involved the fact that that audit committee financial experts on the board violated their fiduciary duties by allowing the company to engage in subprime lending. The Delaware Chancery Court stated that "[d]irectors with special expertise are not held to a higher standard of care in the oversight context simply because of their status as an expert".[32] Rather than a failure of management oversight, the Court viewed the operative issue as a failure to recognise a business risk, emphasising that "[e]ven directors who are experts are shielded from judicial second guessing of their business decisions".[33]

A similar "business decision" deference did not apply to the court's decision regarding *In re Emerging Communications, Inc. Shareholders Litigation*,[34] wherein a director with financial expertise was held to have a duty to voice concerns about the fairness of a proposed transaction's price. The meaning of this case has been widely debated. One interpretation is that, although directors possessing special expertise might not be held to a higher standard under Delaware fiduciary duty law, they may lose the safe harbor protection afforded by Section 141(e) of the Delaware General Corporation Law.

Section 141(e) provides that a director's good faith reliance upon "such information, opinions, reports or statements presented to the corporation . . . as to matters the member reasonably believes are within such other person's professional or expert competence and who has been selected with reasonable care. . . " will be afforded legal and factual deference. However, if a director has a particular expertise, then they may be unable to rely in good faith on an expert's report (or omission). As companies' SEC proxy disclosures expand upon directors' particular qualifications and expertise, they also effectively limit the scope of Section 141(e) deference. Where a director's cyber *bona fides* are trumpeted, even under Delaware law, they will enjoy less "business decision" deference in matters involving cybersecurity.

There is currently a tension developing between these director disclosures, which grow ever more elaborate and more prominent, and the protections of the "business decision" deference. If nothing else, civil plaintiffs may endeavour to weaponise a director's publicly touted expertise to argue that the same director either violated the federal securities laws or their fiduciary duties. While all such claims require proof (in this specific context) of the director's knowledge about specific cybersecurity risks, a company's own admissions about a director's cybersecurity knowledge and expertise make the cases easier to allege and prove. Drafting these director cybersecurity disclosures has, therefore, become a high-stakes balancing act: companies must provide truthful and informative disclosures while also taking care to keep those disclosures lean enough to not create greater litigation risks.

The changes in legal risks appear in *National Ink and Stitch, LLC v. State Auto Property and Casualty Insurance Company*,[35] in which a federal court held that a ransomware attack was covered by standard business loss language in a contract. In other words, the risks of a cyber event are so commonplace that any mention of business risk should contemplate these types of losses.

California liability

The California Consumer Privacy Act (CCPA) went into effect on January 1, 2020. The CCPA gives California residents expansive rights[36] over businesses' collection, use and sharing of their personal information. The CCPA: (1) vests general enforcement authority with the California Attorney General;[37] and (2) creates a private right of action that can only be brought to certain data breach incidents "and shall not be based on violations of any other section of" the CCPA.[38] *More than 50 lawsuits were filed in the first six months after the CCPA went into effect.* Roughly half of these lawsuits related to data breaches. The CCPA created no other types of civil or regulatory liability. However, the CCPA has been used to augment certain existing civil liability theories.

Plaintiffs in the other cases premise claims on alleged violations of consumer rights, often asserting that non-compliance with the CCPA, by extension, constitutes a violation of California's Unfair Competition Law (UCL), Consumer Legal Remedies Act (CLRA), or other causes of action. Many of the suits, whether for data breach or hybridised with another theory, were filed as class action lawsuits.

CCPA enforcement against directors

As mentioned above, the California Attorney General has broad authority to enforce all violations of the CCPA. Businesses that violate the CCPA will be subject to civil enforcement actions by the Attorney General. Violating businesses will be given a notice of non-compliance and a 30-day opportunity to cure the non-compliance. Businesses who fail to comply within the 30 days will be subject to an injunction and a civil penalty: $2,500 for each unintentional violation; and $7,500 for each intentional violation. Because of the nature of privacy and cybersecurity events, these violations, and the related penalties, can compound quickly.

The California Attorney General has exercised broad authority to enforce California laws against directors in the past.[39] However, enforcement of the CCPA only began on July 1, 2020. The regulations issued after enforcement began.[40] These regulations provide no insight as to whether the California Attorney General will seek to hold officers and directors personally liable for a company's violations. Furthermore, active enforcement is still so new that we have few cases to examine that would suggest such authority will be exercised in the future. In general, officers and directors should be aware of the risk that the California Attorney General will seek to utilise the CCPA against them if there are systemic failures under that statute.

CCPA civil suits filed in connection with data security incidents

Most CCPA civil cases allege a data breach and then generally contend that the breach was a violation of the CCPA without offering additional details.[41] The CCPA claims usually join negligence, breach of contract, unjust enrichment, and violation of the California Unfair Competition Law claims.[42] Other cases include greater factual and procedural specificity.[43] However, thus far, none of these cases have sought to hold the officers or directors personally liable.

A number of cases also assert a violation of California's Unfair Competition Law *based upon* a data breach violating the CCPA.[44] The Unfair Competition Law defines "unfair competition" broadly to "mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by [California's false advertising law]". While these cases may seek injunctive relief and restitution, they, like the pure CCPA cases, have not yet articulated any claims against the officers and directors.

These class action cases are not the only types of civil liability that may draw upon the CCPA. One recently filed case is between competing businesses engaged in market research that involves the collection and sale of personal information.[45] The plaintiff alleges that the defendant (the plaintiff's former business partner and now competitor) violated the CCPA by failing to provide sufficient notice of its privacy practices to consumers, and as a result, has gained an unfair and unlawful advantage in violation of the Unfair Competition Law. It is not hard to see insider directors wrapped up in similar theories.

Alleging compliance with the CCPA could even form the basis of some of the derivative actions based upon the fiduciary duties discussed earlier. Basically, such cases would allege that violating the CCPA constitutes a gross dereliction of oversight that amounts to a breach of fiduciary duties. Cases utilising these theories are coming, but as we shall see below, the cases filed thus far have not reached a high level of sophistication.

Privacy litigation under the California Consumer Privacy Act 2018

In March 2020, plaintiffs filed *Cullen v. Zoom Video Comm., Inc.*[46] Since filing, the judge in this Northern District of California federal civil action related and consolidated separate actions. This recaptioned Frankenstein monster of a class action lawsuit claims that Zoom illegally shared millions of users' personal information with Facebook and failed to protect their personal information, thus violating the CCPA. Plaintiffs also allege that Zoom's privacy policy contained misrepresentations, that Zoom made inadequate privacy notices about its data collection and use, and that Zoom failed to implement and maintain reasonable security procedures and thus committed fraud in violation of California's Unfair Competition Law. The lawsuit also alleges violations of California's Consumers Legal Remedies Act and of California consumers' constitutional privacy rights. The viability of these claims will not be tested soon: a hearing on class certification is scheduled for May 27, 2021.

The "*Consolidated Ambry Genetics Cases*"[47] is the collective name for the consumer class action cases filed against genetic testing company Ambry Genetics for a January 2020 data breach. Plaintiffs allege that the breach resulted in unauthorised access to customer personally identifiable information and protected health information, and that Ambry failed to timely report the breach to the government or to customers. These cases were consolidated in June 2020. Despite the wide variety of legal theories on display here, none of the *Consolidated Ambry Genetics Cases* articulate personal liability claims against the officers or directors. The same is true for *Gupta v. Aeries Software, Inc.*,[48] wherein plaintiffs allege that Aeries did not adequately safeguard the personally identifiable information of thousands of vulnerable students, resulting in unauthorised third parties accessing that data. *G.R. v. TikTok*[49] provides yet another CCPA lawsuit that fails to bring claims against the officers and directors. While this case does not directly impact them, officers and directors should take note of the data security and privacy issues that are explored in this case, which alleges unlawful harvesting of biometric identifiers from minor and adult users. These types of issues do not seem to involve data security or privacy, but the laws and regulations – including the CCPA – increasingly cover both biometrics and the protection of minors. The lawsuits will follow the same path as these laws and regulations.

Other state liability

New York State

The New York Department of Financial Services, which is responsible for the regulation of banks, insurers, and other financial institutions that do business in New York, has a growing role in pushing cybersecurity standards. The NYDFS also possesses an expansive view of its own jurisdictional limits, the entities that it regulates, and their respective officers and directors.

New rules developed by the NYDFS under 23 NYCRR Part 500 (the "Regulation"), which went into effect on March 1, 2017, require entities that NYDFS regulates to implement specific cybersecurity standards. These standards include establishing a comprehensive cybersecurity policy, completing a written incident response plan (focusing upon reporting breaches within 72 hours to the NYDFS), and promulgating security policies for third-party vendors. The rules require officers and directors to not only designate a chief information security officer (CISO), but also to certify to the NYDFS that the company is in compliance with the regulations.

The CISO must prepare an annual report to the board of directors of the regulated entity regarding its cybersecurity programme. The report must: (1) specifically address the identification of material cyber risks to the regulated entity, including any past material cybersecurity event; and (2) report on penetration testing and vulnerability assessments. The CISO must also report to the board of directors about, *inter alia*, multifactor authentication and cyber awareness training for all personnel. In short, the boards of covered companies likely received far more cyber information than they ever received prior to the NYDFS rules. With this deep cyber information in hand, officers and directors were required to submit the first cybersecurity compliance certification to the NYDFS by February 15, 2018. This is an annual requirement[50] that will, each year, put directors into the cybersecurity weeds. Moreover, by certifying compliance with these detailed cybersecurity requirements, directors become the primary targets of these regulators if a breach occurs.

Other states

A number of other states are considering enhanced cybersecurity and privacy regulations. In the privacy sphere, many states are considering adopting aspects of California's sweeping CCPA. Other states, like Washington, are likely to adopt a framework similar to that utilised by the European Union,[51] which is discussed in further detail below. In any case, the two main risks to directors are the same as they are in California: (1) enforcement actions against officers and directors brought

by individual state attorneys general; and (2) private actions alleging either substantive violations of the statute or qualitative violations of the duty of care premised upon a failure to comply with the statute.

Global Personal Cyber Risks for Officers and Directors

New legislation in a range of jurisdictions – most notably in the EU, under the new General Data Protection Regulation (GDPR)[52] – will hold organisations to higher cybersecurity and cyber standards than ever. With those growing risks in mind, it is useful to consider the potential liability landscape in all jurisdictions in which they are active.

The United Kingdom

In the United Kingdom (UK), directors' fiduciary duties to the company are largely codified under the Companies Act 2006 (the 2006 Act).[53] Among other things, directors of UK companies possess a duty to promote the success of the company and to exercise reasonable care, skill, and diligence in the conduct of their role.[54] Similar to United States civil liability theories, the board's failure to understand and mitigate cyber risks could constitute a breach of these duties. In evaluating these types of claims, UK law requires that we consider the standard of a reasonably diligent person with the knowledge and skill of the director in question. These standards will be tested, as in the United States, via derivative actions.

Recent UK case law has established that civil lawsuits may be brought against violations of the UK Data Protection Act 1998.[55] Perhaps most concerning to companies assessing their civil cyber risks in the UK is that these Data Protection Act cases can proceed even when the plaintiff has not suffered pecuniary loss. Stated differently, companies face civil losses even where they did not cause anyone to actually lose money. These UK cybersecurity and privacy lawsuits may be brought against the company or the individual directors.

Doing business in the UK will also expose companies to the GDPR. The UK's "Brexit" from the EU will not alter the applicability of the GDPR. The GDPR imposes broad regulations upon companies that control or process personal data. Penalties for GDPR violations can be staggering: non-compliance penalties extend up to the higher of €20 million or 4% of the organisation's worldwide revenue. Moreover, directors of public companies bear the responsibility for compliance with the GDPR and personal liability for any fines and penalties.[56] In addition, the Information Commissioner's Office, the UK's data privacy regulator, can compel future conduct from senior board members to ensure that the company complies with its ongoing data protection obligations.

Directors of regulated entities also need to be aware of their UK personal regulatory obligations. In the financial services sector, the Financial Conduct Authority closely scrutinises directors, and will take action if a director fails to discharge their regulatory duties as a result of not properly managing the organisational cyber risks. Similarly, directors of publicly traded companies must appropriate disclosures under the UK Listing Rules. These disclosures may include a wide range of adverse cyber events. Directors face personal liability for any failure to disclose such events.

The EU

In addition to the GDPR, which we discussed with regard to the UK, the EU is developing a number of new laws and regulations regarding cybersecurity and privacy. For example, the EU Network and Information Security Directive (NIS Directive)[57] will require companies in certain industries (including such far-flung industries as financial services and "water transport"[58]) to implement certain minimum cyber security standards. While enforcement of the NIS Directive is still unclear, and its effectiveness is under review as of October 2020, the mere fact that the NIS Directive will be implemented in the EU should alter the way that directors think about cybersecurity implementation.

Germany

German law provides similar personal liability pitfalls for directors. Under German law, directors can be held liable for breach of their duties. These cybersecurity duties include, *inter alia*, a duty to ensure that adequate IT infrastructure is in place to protect data security and avoid cyber risks. Directors must therefore ensure that certain technical standards are met, which are actually spelled out in the German Data Protection Act (*Bundesdatenschutzgesetz*) and the German IT Safety Act (*Bundessicherheits- und Informationstechnikgesetz*). The German laws also require a high level of ongoing systems monitoring. This can mean that the failure to note intrusions, which can sometimes last months, can itself constitute an organisational failure. While all of these regulatory responsibilities should concern directors, it bears noting that German law generally only permits director liability to the company, and not to third parties, although the risk exists.

United Arab Emirates

Under United Arab Emirates (UAE) law, officers and directors of a company can face personal liability for matters relating to cyber risk. The board of directors of a public joint stock company is liable to the company, its shareholders and third parties for certain acts, including fraud, misuse of power, breach of the UAE Commercial Companies Law or the company's articles of association, or an error in management.[59] While little case law exists on how these provisions may be applied, it is possible that cybersecurity and privacy failures may fall under the law.

Of more concern should be potential criminal liability under UAE law. Officers and directors should be mindful that potential criminal liability exists for the unauthorised disclosure of personal information. Reportedly, in March 2015, three executives in the UAE were all temporarily imprisoned on the grounds of a breach of privacy in connection with the installation of CCTV. Jail time is therefore a real possibility in the UAE.

Canada

Canadian law can impose personal liabilities upon officers and directors of a company for matters relating to cybersecurity and privacy risk under Canadian law. The Canada Business Corporation Act RSC 1985 (CBCA) requires every director to exercise their powers and duties honestly and in good faith, with a view to the best interests of the corporation, and exercise the care, diligence, and skill that a reasonably prudent person would exercise in comparable circumstances.[60] The CBCA provides for shareholder derivative actions for breaches of duties owed by directors to the company and the recovery of monetary damages on behalf of the company.[61] Thus, in theory, companies operating in Canada bear many of the same litigation risks for their cybersecurity and privacy failures.

As in the United States, Canada imposes liability upon directors for omissions or misrepresentations in public disclosures. Moreover, since September 2013, the Canadian Securities Administrators have instructed that issuers should expressly disclose their cyber-crime risks, any cyber-crime incidents, and characterise their cyber-security controls in a prospectus or a continuous disclosure filing.[62]

Officers and directors also face statutory liabilities under privacy statutes in Canada, although these statutes only exist in certain discrete Canadian jurisdictions. Breaching Quebec's privacy statute can lead to monetary fines against directors who ordered or authorised the breaches.[63] Likewise, Ontario's Personal Health Information Protection Act 2004 contains penalties imposed on officers and directors for the wilful collection of health information without reasonable protections.[64]

South Africa

South African law also creates personal liabilities for officers and directors in connection with cybersecurity and privacy risks under South African law. As in other countries utilising a derivation of the English legal system, the failure to implement reasonable cybersecurity measures could constitute a breach of directors' fiduciary duties. As in countries like the United States and England, these fiduciary duties were established by way of the common law, and have later been codified. Just as in these other countries, officers and directors have a duty to maintain certain minimal cybersecurity and privacy procedures and oversight. Officers and directors could theoretically face personal liability to the company and to third parties for a breach of these duties. A breach of directors' fiduciary duties could lead to claims being brought against officers and directors. Similarly, just as in the UK and the United States, directors may face personal liability in contract or tort. This risk is even more acute in South Africa, where the governing laws permit great personal liability, even when working through the "legal fiction" of a corporation.

Moreover, a breach of fiduciary duty could lead to South African regulators taking action against officers and directors. For example, the Companies and Intellectual Property Commission (CIPC) can investigate these complaints, and various mechanisms allow action to be taken against a company or its directors.

Common law, not a statute, primarily protects the South African right to privacy. However, South Africa has also passed the Protection of Personal Information Act, of 2013 (POPI).[65] Under POPI, regulatory action may be taken against an organisation or person for any violation. Therefore, depending on the nature of each violation, a director may face civil fines, administrative fines, penalties, and even a period of imprisonment. POPI does not fully become effective until July 2021, which is when the "grace period" ends.

Australia

As in the UK, United States, and South Africa, officers and directors face certain familiar personal liability risks for a company's cybersecurity and privacy failures. All officers and directors have a key responsibility to ensure that companies adopt appropriate risk management strategies to protect the company and its shareholders via their duty of care and due diligence, both under Section 180 of the Corporations Act 2001[66] and the common law. The Australian corporate regulator, the Australian Securities and Investments Commission (ASIC), has the power to bring an action against officers and directors for a breach of their duties. The consequences are potentially serious, and include a declaration of contravention, pecuniary penalties, compensation orders, and disqualification of the director or officer from managing a corporation. ASIC Report 429[67] states that: it considers board participation important to promoting a strong culture of cyber resilience; and a failure to meet obligations to identify and manage cyber risks may result in stiff penalties. Finally, a failure by officers and directors to take reasonable steps to prevent, or respond appropriately to, a cyber or privacy incident may also give rise to Australian civil proceedings, either via derivative action brought by the shareholders or by affected individuals.

Emergent Areas of Special Cybersecurity and Privacy Concern to Officers and Directors

Data and privacy security is not just the target of criminals. Foreign governments utilise their military and intelligence resources to actively attack the privacy and data assets of private companies. These state actors carry special risks that officers and directors must acknowledge. For example, Chinese military hackers stole U.S. Steel's trade secrets and gave them to Chinese steel companies so that they could better compete in western markets.[68] U.S. Steel attempted to meet this threat by filing an action in the International Trade Court.[69] After a long and costly fight, U.S. Steel withdrew its cybertheft action, but the legal fight is far from over.[70] Whenever nations endeavour to interfere with businesses, the officers and directors should take note.

State actor privacy and data security concerns can even lead to the forced liquidation of assets. The saga of TikTok is well known at this point. However, it bears repeating that the United States' insecurity about the state of TikTok's privacy and data security procedures and controls has led directly to a likely "forced" liquidation of United States assets. Russia's potential control over private data led to similar insecurity over the viral "FaceApp".[71] In other words, state actors are now colliding with privacy and data security in a manner that provides an existential threat to many companies. Where the risks to companies are great, the personal liability risks to officers and directors can be correspondingly large.

Certain business sectors can also face outsized risks of which officers and directors must be aware. If a company services sensitive or classified governmental contracts, they will be both a target of bad actors and also subject to increased regulatory oversight. The dimensions of those standards, whether under the Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity requirement, or under government contracting requirements that National Institute of Standards and Technology guidelines be met, should be the subject of a different chapter. However, for our purposes, we should acknowledge that officers and directors must be aware that these standards exist – and work to satisfy them – or else they face the loss of extremely valuable contracts.

Not only traditional defence and governmental industries face these threats: state-sponsored hackers hacked Yahoo![72] and the World Anti-Doping Agency.[73] Zappos was hacked by a hacker who works for the successor to the KGB.[74] While Zappos is a very cool online commerce company, one would not usually think of it as a geopolitical target. That is all changing. Officers and directors must address these risks now or they face the prospect of personal liability for their failures later.

Endnotes

1. https://www.sec.gov/news/press-release/2018-22.
2. https://www.sec.gov/news/press-release/2018-71.
3. https://www.sec.gov/rules/interp/2018/33-10459.pdf; see also 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].
4. Proxy Disclosure Enhancements, SEC Release Nos 33-9089, 34-61175, IC-29092; 74. Fed. Reg. 68334 (Dec. 23, 2009).
5. Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002, SEC Release Nos 33-8177, 34-47235; 68 Fed. Reg. 5110 (Jan. 31, 2003).
6. Director liability under the operative sections of the federal securities laws turns on the director's knowledge or the reasonableness of their beliefs in a specific situation presumably being impacted by their particular qualifications, background or expertise. A director has a "due diligence" defence to liability under Section 11 if they sustain the burden of proof that, with regard to any part of the registration statement not made under the authority of an expert, the director "had, after reasonable investigation, reasonable ground to believe and did believe, at the time such part of the registration statement became effective, that the statements therein were true and that there was no omission to state a material fact". Federal courts have generally taken the view expressed in *Feit v. Leasco Data Processing Equipment Corp.*, 332 F. Supp. 544, 577 (E.D.N.Y. 1971), that "[w]hat constitutes 'reasonable investigation' and a 'reasonable ground to believe' will vary with the degree of involvement of the individual, h[er] expertise and h[er] access to the pertinent information and data". Thus, directors who are insiders, or directors who are attorneys involved in preparation of the registration statement, generally are expected to make a more complete investigation and have more extensive knowledge of the facts at issue.
7. 17 CFR 229.407(h); 17 CFR 240.14a-101 – Schedule 14A.
8. Final Rule: Proxy Disclosure Enhancements, Release No. 33-9089 (Dec. 16, 2009) [74 FR 68334 (Dec. 23, 2009)], available at http://www.sec.gov/rules/final/2009/33-9089.pdf.
9. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos 33-10459, 34-82746 [Feb. 26, 2018], available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.
10. https://www.sec.gov/litigation/complaints/2018/comp-pr2018-40.pdf; https://www.sec.gov/litigation/complaints/2018/comp-pr2018-115.pdf.
11. https://www.sec.gov/news/testimony/testimony-oversight-us-securities-and-exchange-commission.
12. *Id.* at 3–4.
13. Section 141(a), Delaware General Corporation Law.
14. *Graham v. Allis-Chalmers Mfg Co.*, 188 A 2d 125, 130 (Del 1963).
15. *Smith v. Van Gorkom*, 488 A 2d 858, 872 (Del 1985).
16. *Stone v. Ritter*, 911 A 2d 362, 370 (Del 2006).
17. 806 F. Supp. 1197 (E.D. Pa. 1992).
18. *Id.* at 1203.
19. *Id.* at 1204.
20. 801 F. Supp. 1493 (D. Md. 1992).
21. *Id.* at 1501.
22. 698 A.2d 959 (Del. Ch. 1996).
23. *Id.*
24. No. 17-cv-5225(RJS), 2018 WL 9517195 (Sep. 29, 2018).
25. *Id.* at *6.
26. *Id.* (citing *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d 106, 128 (Del. Ch. 2009)) ("[A] showing of bad faith is a necessary condition to director oversight liability").
27. *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d at 112 ("[A] showing of bad faith is a necessary condition to director oversight liability").
28. No. 533, 2018 (Del. Sup. Ct. 2019).
29. *In re Gen. Motors Co. Derivative Litig.*, C.A. No. 9627-VCG, 2015 WL 3958724, at *17 (Del. Ch. June 26, 2015).
30. *Wayne Cty. Emp.'s Ret. Sys. v. Dimon*, 629 F. App'x 14, 15 (2d Cir. 2015).
31. 964 A.2d 106 (Del. Ch. 2009).
32. *Id.* at 128 n.63.
33. *Id.*
34. C.A. No. 16415, 2004 BL 1814 (Del. Ch. May 3, 2004).
35. 435 F. Supp.3d 679 (D. Md. 2020).
36. The Act provides California residents with the right to seek access to, or deletion of, their personal information, as well as the right to object to the sale or sharing of such information with third parties.
37. See Cal. Civ. Code § 1798.155(b).
38. See Cal. Civ. Code § 1798.150(c) ("The cause of action established by this section shall apply only to violations as defined in subdivision (a) [regarding data breaches] and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution").
39. https://oag.ca.gov/news/press-releases/attorney-general-sues-remove-stakeholder-members-iso-board.
40. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.
41. See, e.g.: Complaint, *Albert Almeida, Mark Munoz, and Angelo Victoriano v. Slickwraps Inc.*, No. 2:20-at-00256, at 28, 48 (E.D. Cal. March 12, 2020); Complaint, *Daniela Hernandez v. PIH Health*, No. 2:20-cv-01662, at 6, 19, 38 (C.D. Cal. Feb. 20, 2020); Complaint, *Bernadette Barnes v. Hanna Andersson, LLC, and Salesforce.Com, Inc.*, No. 4:20-cv-00812-DMR, at 3, 15 (N.D. Cal. Feb. 3, 2020); and Complaint, *Juan Maldonado v. Solara Medical Supplies, LLC*, No. 3:19-cv-02284-H-KSC, at 3, 21 (S.D. Cal. Nov. 29, 2019).
42. See, e.g.: Complaint, *Slickwraps* at 39, 44, 46 and 48; Complaint, *Hernandez* at 22, 27, 30 and 37; Complaint, *Barnes* at 16 and 22; and Complaint, *Maldonado* at 23, 30, 33 and 34; see also *Rahman v. Marriott International, Inc.*, Case No. 8:20-cv-00654 (C.D. Cal., Apr. 3, 2020) (this putative class action on behalf of California residents against Marriott for a data breach that was announced on March 31, 2020 alleges violation of the CCPA and California's Unfair Competition Law, as well as breach of contract and implied contract, negligence, and unjust enrichment).
43. See, e.g.: Complaint, *Michele Pascoe v. Ambry Genetics*, No. 8:20-cv-00838, at 50 (C.D. Cal. May 1, 2020) at 50; and Complaint, *Lopez* at 44.
44. See, e.g.: Complaint, *Slickwraps* at 48; and Complaint, *Hernandez* at 37–38.
45. See Complaint, *Bombora v. ZoomInfo*, No. 20-cv-365858 (Cal. Super. Ct. June 10, 2020).
46. Case No. 20-cv-02155 (N.D. Cal. Mar. 30, 2020).
47. Case No. 8:20-cv-00791 (C.D. Cal.).
48. Case No. 8:20-cv-00995-FMO-ADS (C.D. Cal., May 28, 2020).

49. Case No. 2:20-cv-04537 (C.D. Cal.).
50. https://www.dfs.ny.gov/industry_guidance/cyber_filings/requirements.
51. https://fpf.org/2020/01/13/its-raining-privacy-bills-an-overview-of-the-washington-state-privacy-act-and-other-introduced-bills/#:~:text=The%20Act%20would%20be%20a,creates%20a%20nuanced%20approach%20to.
52. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
53. https://www.legislation.gov.uk/ukpga/2006/46/contents.
54. *Id.* (Sections 172 and 174, 2006 Act).
55. *Google Inc v. Vidal-Hall and other* [2015] EWCA Civ. 311.
56. Per the first and second paragraphs of Article 169, the members of the management board must act as thorough and diligent owners, and they are jointly and severally liable for the damage inflicted on company by their actions.
57. https://eur-lex.europa.eu/eli/dir/2016/1148/oj, 2016/1148/EU.
58. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.
59. Article 162, UAE Federal Law No. 2 of 2015 on Commercial Companies.
60. https://laws-lois.justice.gc.ca/eng/acts/C-44/page-21.html?txthl=duties+duty#s-122.
61. https://laws-lois.justice.gc.ca/eng/acts/C-44/page-41.html?txthl=derivative#s-239.
62. https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20130926_11-326_cyber-security.htm#:~:text=To%20manage%20the%20risks%20of,and%20their%20clients%20or%20stakeholders.
63. http://legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1.
64. https://www.ontario.ca/laws/statute/04p03.
65. https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.
66. http://www5.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s180.html#:~:text=Care%20and%20diligence%2D%2Dcivil%20obligation%20only,-Care%20and%20diligence&text=The%20director's%20or%20officer,in%20their%20position%20would%20hold.
67. https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf.
68. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
69. https://www.wsj.com/articles/u-s-steel-accuses-china-of-hacking-1461859201.
70. https://www.wsj.com/articles/u-s-steel-withdraws-hacking-claim-against-chinese-rival-1487183293.
71. https://www.pbs.org/newshour/science/is-faceapp-a-security-risk-3-privacy-concerns-you-should-take-seriously.
72. https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html.
73. https://www.nytimes.com/2019/10/28/sports/olympics/russia-doping-wada-hacked.html.
74. https://www.forbes.com/sites/thomasbrewster/2017/03/20/alexsey-belan-yahoo-fbi-hacker-allegations/#bc236cd76f24.

Christopher Ott, CIPP/US, leads data security, privacy, and white-collar litigation and investigations. Leveraging his experience from more than 13 years at the U.S. Department of Justice (DOJ), including successfully litigating complex data security matters, conducting hundreds of investigations, and winning dozens of appeals, Mr. Ott works with clients on disputes and strategy relating to data security, privacy, blockchain, and AI issues. Mr. Ott has handled hundreds of matters involving the intersection between white-collar matters (accounting, securities, money laundering) and cybercrimes (from international criminal gangs to state actors). In his most recent governmental role, Mr. Ott acted as Supervisory Cyber Counsel to the National Security Division of the DOJ. Mr. Ott consulted extensively with the intelligence community and coordinated extensively with regulators such as the U.S. Treasury Department, the Federal Communication Commission (FCC), the Federal Trade Commission (FTC), and the Securities Exchange Commission (SEC).

Rothwell Figg
607 14th Street N.W.
Suite 800
Washington, D.C. 20005
USA

Tel: +1 202 783 6040
Fax: +1 202 783 6031
Email: cott@rothwellfigg.com
URL: www.rothwellfigg.com

The Privacy, Data Protection & Cybersecurity team at Rothwell Figg helps clients understand and navigate these rapidly evolving areas of law. We work with our clients to prepare, integrate, and implement compliance strategies, frameworks for risk management, and best practices. We have experience working closely with our clients to: build data inventories and assess their legal obligations; to implement back-end and structural changes that are not only compliant, but also workable; to prepare written policies, assessments, forms, and notices to effectuate legal requirements and best practices; to negotiate, draft, and review agreements for compliance; and to help train staff. We can assist with the design and implementation of incident response plans, and if there ever is an incident, we can serve as trusted advisors, from the investigation stages through to litigation, helping you navigate disclosure requirements to public authorities. Most of the attorneys in the practice group are experienced litigators with deep technical backgrounds and have represented clients in a wide variety of venues, including before numerous government agencies and in state courts, federal district courts and courts of appeal, and the United States Supreme Court.

www.rothwellfigg.com

ROTHWELL FIGG
IP Professionals

Mitigating Cyber-Risk – A Boardroom Priority

Ince

Rory Macfarlane

You Are a Target

Had Benjamin Franklin been alive today, it is probable that he would have added one more event to his list of life's certainties since in the 21st century:

"… *nothing can be said to be certain, except death, taxes and cyber-attack*."

A cyber-attack on your business is a certainty. It is not a question of *if* an attack will come, it is a question of *when*. A cyber-related breach of your business in the next 24 months is also almost certain. Nevertheless, despite this somewhat pessimistic outlook, a *catastrophic loss* following a cyber-breach incident need not be a certainty. This is an important distinction.

Inactivity Provides Opportunity

Deciding how to address cyber-risk is a contentious issue in many boardrooms. Cyber-risk is just one of many risks faced by a company. Most credible corporate surveys rank cyber-risk as the biggest risk to business in 2020.[i] The recent drive to online sales and remote working following the COVID pandemic has further increased this risk. Despite this, only about ⅓ of businesses have a cyber-breach response plan.

At the moment, cyber threat actors are benefitting from, and exploiting, corporate indecision on cyber-risk. This indecision can be driven by budget constraints. More often though, it is a lack of understanding; both of the extent of the risk and the relatively modest cost of effective cyber-risk management that engenders this inactivity. The Bank of Bangladesh lost US$81 million from a single credential-theft event. Inactivity can be very costly. The average total cost flowing from a data-breach in 2020 is US$3.86 million.[ii]

Increased awareness does not always translate into action. This is not necessarily because boards do not want to grasp this issue. Rather, it is because cyber-risk management has not been considered a core business governance function in the same way that finance, sales or marketing have.[iii]

Another reason might be traced back to the unfounded hype following the last big IT scare: the Millennium Bug or Y2K panic. Companies spent heavily on contingency plans due to the fear that, at the turn of the millennium, computers would be unable to differentiate between the years 1900 and 2000. The media was awash with predictions of planes falling from the skies, bank account balances disappearing and millions being wiped off stock markets. As it transpired, it was the bug that did not bite. However, its legacy may be that many corporate decision makers now view cyber-risk in a similar light. This would be a mistake.

Types of Risk

The risks that businesses face from these cyber threats fall into five general categories.[iv]

- business operational risk;
- reputational risk;
- legal risk;
- compliance risk; and
- director's personal risk (director's risk).

Business operational risk

This is the potential for direct or indirect loss resulting from the failure of key business systems, processes or procedures. It includes lost monies from a CEO/fake invoice fraud or lost revenue from business interruption following system compromise. Maersk estimate that the cost to their business following the NotPetya attack in 2017 has been between US$200 million and US$300 million.[v] In December 2015, three Ukrainian power distributors were simultaneously hacked, leaving more than 225,000 people and businesses without electricity.[vi]

Reputational risk

This is the potential for a company to suffer losses arising from damage to its market reputation or public image following a highly publicised cyber-breach incident. Target's share price fell by 2.2% following the attack it sustained in 2013. When Yahoo reported the breach of its user accounts, it was negotiating a merger with Verizon. The reporting caused Verizon to reconsider Yahoo's valuation, resulting in a US$350 million reduction in the purchase price.

Legal risk

Legal risk describes the losses from civil claims brought by third parties who have been impacted or affected by a company's cyber-breach incident. For example, following a breach of company A's system, company B may be tricked into making payments to the wrong bank account. In such circumstances, company B may have a recourse claim against company A based on express or implied contractual terms.[vii] Data subjects will often claim damages following a data breach incident where their personal data is lost or corrupted.

Compliance/regulatory risk

This is the impact of action taken against an organisation by regulatory bodies for breach of any cyber-related legislative or regulatory requirements. The global increase in applicable legislation, including GDPR and the NIS Directive, means that this is an increasing area of risk for companies. Regulators are empowered to impose very large fines in the event of a breach.[viii]

In 2018, BA was fined approximately GBP180 million (1.5% of its global turnover) for its passenger data breach. Pre-GDPR, the highest fine that the Information Commissioner's Office (ICO) could impose was the GBP500,000 fine imposed on Facebook. Had the sanctions under GDPR been available then, a fine of 4% of its revenue would have set Facebook back GBP1.26 billion.[ix]

Regulators can also impose financial sanction in other ways. Following the hack of American healthcare insurance provider Anthem in 2014, the state insurance commissioners required Anthem to upgrade its cybersecurity infrastructure by investing US$260 million. This was despite the commissioners concluding that Anthem's cybersecurity framework, protocols and response strategy had been reasonable.[x]

Director's risk

Risk comes from not knowing what you are doing.[xi] Given the prevalence of high-profile cyber-breach incidents and the amount of guidance now publically available there is simply no reason for any business not to know what needs to be done to improve its cyber-resilience.

Directors who fail to take action to protect a company may find themselves personally exposed to claims from the company, and possibly from shareholders via derivative actions, for breach of their fiduciary duty or the obligations imposed upon them by statute.

Case Studies[xii]

The following two case studies illustrate the interaction between risk and loss.

Case study – *WannaCry*

The background to the May 2017 *WannaCry* incident illustrates how outdated operating systems generate operational risk.

Surprisingly, the United States National Security Agency (NSA) originally created the software exploits used to initiate the *WannaCry* attack. They had developed them to exploit vulnerabilities in the Microsoft Windows operating system. To address this weakness, in March 2017, Microsoft issued a patch, although this only offered protection if organisations updated their systems to apply the patch.

In April 2017, a group of hackers stole the software exploits from the NSA which led to the creation of the *WannaCry* encryption malware that rapidly spread to infect approximately 230,000 computers in over 150 countries. Entities large and small, ranging from the banks to railways, phone networks to car manufacturers were all affected. The malware required those infected to pay a small ransom in bitcoin for the decryption key, or risk losing their data. Fortunately, a UK-based cybersecurity company accidently found a kill-switch, significantly reducing the malware's dissemination.

The *WannaCry* incident highlights the importance of ensuring that you have a functioning Cyber-Risk Management Plan in place. This risk was easily mitigated. The Windows vulnerability was well known and a patch to close the vulnerability was already available. Despite this, many organisations had not updated their systems, leaving themselves exposed.

The design and behaviour of the malware provides another lesson. Part of its success was that it made use of a worm to spread the malware between computers. Unlike those malware attacks that rely on social engineering or human error to continue their spread, such as an email phishing campaign designed to trick a recipient into clicking on an imbedded link, the *WannaCry* worm spread independently from infected systems via file-sharing settings, the malware itself actively seeking out other vulnerable systems.

Companies could have minimised the impact on their systems once infected through better network segregation to protect key digital assets. Simply disabling the file sharing function would also have been effective.

Unhelpfully, the mainstream media downplayed the seriousness of the *WannaCry* attack. Most articles focused on the total figure for ransoms paid, which, at between US$15,000 – US$20,000 in cryptocurrency, was quite small. This low ransom level was partly fortuitous due to the early discovery and activation of the kill-switch that dramatically slowed the spread of the malware. However, this reporting overlooked the business interruption losses. Renault had to shut down its operations in France for a period, FedEx systems were compromised and, as companies including Maersk learned to their cost in the NotPetya malware attack that followed just a couple of months later, business interruption losses will usually far out-strip any decryption ransom demand.

Case study – Target

The Target hack is arguably the most important attack for companies to understand.

The focus of the attack was Target's electronic point of sale (EPS) devices. The hackers installed memory-scraping malware that allowed them to steal the data stored on the electronic strips of cards used in Target's stores. They managed to steal credit and debit card data for 40 million customers in just three weeks. Nearly all of Target's 1,700 stores were compromised.

In terms of losses to Target, the public announcement of the hack on 19 December 2013 resulted in Target's share price falling 2.2% (reputational risk) and its profit dropping by 46% in that quarter (operational risk).

Target also had to make payments of US$18.5 million and US$10 million to settle multistate and class action lawsuits (legal risk). Whilst these losses are not insignificant, they are by no means the outliers in terms of losses. When American healthcare provider Anthem was hacked in 2014, they had to pay US$115 million to settle class action and shareholder lawsuits. Anthem also spent US$2.5 million on forensic computer experts alone.

It is not the losses in the Target attack that are of greatest significance; the crucial aspect of the attack for companies to understand is how the breach occurred.

What is unusual about the Target breach is that the hackers gained access to Target's systems via one of its contractors, Fazio Mechanical Services (FMS). FMS were Target's air-conditioning and heating sub-contractors. The Target breach was actually a sophisticated and well-planned two-stage attack, the breach of Target's EPS System being stage 2.

Stage 1 had been planned several months before when the hackers launched a targeted email spear phishing attack against FMS. Clearly, at least one FMS employee succumbed to it triggering the uploading the hacker's malware.

FMS had been given a direct connection to Target's heating and air-conditioning systems to assist them in conducting routine and preventative maintenance. Once the hackers had access to FMS's system they then used the access credentials granted to FMS by Target to migrate to Target's own systems. It would appear that Target's systems were not sufficiently segregated since the hackers were then able to gain access to Target's EPS system and install the malware necessary to launch stage 2. It is this *inter-company connection* aspect of the hack that must be remembered and acted on.

As companies search for improved efficiencies, internet-based connectivity between them, their customers, suppliers and service providers is becoming the norm. The number of digital of connections between businesses is increasing year on year. Just as Target were exposed by a vulnerability within FMS, if your contractual counterpart or key supplier is compromised and connected digitally to your business, then this presents a threat actor with a vulnerability to exploit, which could lead to a fake invoice fraud, ransom demands following crypto-malware compromise or even business interruption losses due to the induced failure of critical operational systems.

Some Final Thoughts

Viewing cyber-risk as simply an information technology issue is as misguided as considering the safe operation of a car as simply a main engine issue.

Cyber-breach is inevitable; catastrophic loss following a cyber-breach need not be. Cybersecurity is a misnomer. Management focus needs to shift from the concept of security to cyber-risk management. With hackers spending on average over 140 days on a network before being discovered, *detection* is now more important than *protection*.[xiii] Boards need to review and assess risk reduction rather than merely monitor the IT department's progress in implementing cybersecurity function.[xiv]

Maersk, Yahoo, Google, BP, BHP, Saudi Aramco, Rio Tinto, Exon, Fed Ex., Target, Anthem and Sony; even a cursory glance at the list of blue-chip companies who have suffered huge losses from cyber-breach events should dispel the myth that persists in our boardrooms that "*this could not happen to us*".

Warren Buffett often states that "*what we learn from history is that people don't learn from history*". Do not let that be true for your business. Prevention is better than cure. The best way to mitigate your risk is through proactive cyber-risk management.

Let your competitors' assets be the "*low hanging fruit*" that cyber criminals look to harvest.

Endnotes

i. Allianz Risk Barometer 2020. https://bit.ly/35TA2rB.
ii. How much would a data breach cost your business? *IBM*. https://ibm.co/3hVBpIx.
iii. What will Cyber security look like in 2020? *Tech Radar*. https://bit.ly/2sVOCNJ.
iv. Managing Risk in the Information Age (Short Course) – HarvardX.
v. Shipping company Maersk says June cyberattack could cost it up to $300 million, *CNBC*. https://cnb.cx/2vEiXzf.
vi. Managing Risk in the Information Age (Short Course) – HarvardX.
vii. *Frontier Systems (t/a Voiceflex) –v.– Frip Finishing Limited.*
viii. Data Protection Act 2018. https://bit.ly/2s3GV4K.
ix. GDPR fines: where will BA and Marriott's £300m go? *The Guardian*. https://bit.ly/2YM4qh1.
x. McKee, MK (2017). A new in-depth analysis.
xi. Warren Buffett.
xii. Source information for the case studies is Managing Risk in the Information Age (Short Course) – HarvardX.
xiii. Detection more important than prevention in cyber security, says Microsoft CTO, *Teiss*. https://bit.ly/2P8ussL.
xiv. The risk-based approach to cybersecurity. *McKinsey*. https://mck.co/2FMhkaJ.

Rory Macfarlane is an international dispute resolution specialist and established the Ince cyber-risk practice. A dual-qualified solicitor in both England and Hong Kong, he handles all manner of commercial disputes, with particular expertise in commercial fraud, international trade and shipping. Rory has extensive experience in obtaining and enforcing interim injunctions across multiple jurisdictions, as well as the cross-border recovery of judgment debts and arbitration awards.

Following his return to London after 15 years in Hong Kong, Rory continues to lead the Ince Taiwan and Japan market teams. He has an extensive network of relationships with the leading local firms in both jurisdictions and across Asia, making him a valued resource for clients doing business in these markets. He is also a regular speaker on the conference and seminar circuit.

"Diligent and analytical, Rory Macfarlane takes a very commercial approach to problems and sees disputes from a clients' perspective." The Legal 500 Asia Pacific 2017.

Ince Gordon Dadds LLP
Aldgate Tower, 2 Leman Street
London, E1 8QN
United Kingdom

Tel: +44 20 7481 0010
Email: rorymacfarlane@incegd.com
URL: www.incegd.com

About Ince

With a heritage reaching back 150 years, Ince is a dynamic international legal and professional services firm, with offices in seven countries across Europe, Asia and the Middle East. With over 500 people, including over 100 partners worldwide, Ince provides legal advice and strategic guidance to clients ranging from the world's oldest and biggest businesses operating across numerous industries to ultra-high-net-worth individuals.

About The Ince Group plc

The Ince Group is a dynamic international legal and professional services business with offices in seven countries across Europe, Asia and the Middle East. With over 900 people, including over 100 partners worldwide, The Ince Group delivers legal advice, strategic guidance and business solutions to clients ranging from the world's oldest and biggest businesses operating across numerous industries to ultra-high-net-worth individuals.

Through its entrepreneurial culture and "one firm" approach, the business offers its clients over 150 years of experience, insight and relationships. The Group is driven by a unique team of passionate people whose broad expertise and deep sector specialisms provide their clients with solutions to all their complex legal and strategic needs.

www.incegd.com

Ince

Why AI is the Future of Cybersecurity


Akira Matsuda


Hiroki Fujita

Iwata Godo

Overview Surrounding Cybersecurity

What is cybersecurity?

Cybersecurity is defined as the "*preservation of confidentiality, integrity and availability of information in the Cyberspace*" in Article 4.20 of ISO/IEC 27032:2012.

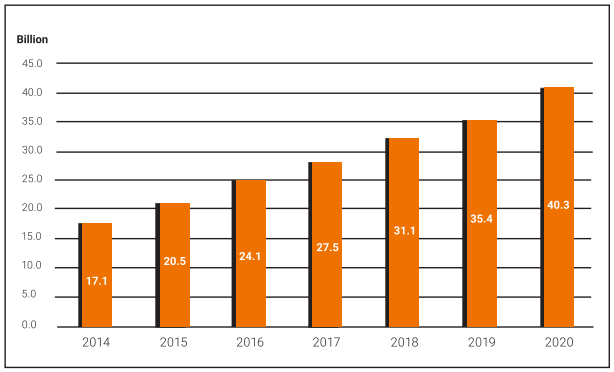
Furthermore, the cyberspace is defined as a "*complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*" in Article 4.21 of ISO/IEC 27032:2012.

Threats in cyberspace

As internet access becomes more pervasive across the world and the Internet of things (IoT) devices become increasingly common and cyberspace expands rapidly, the number of cyber-attacks continues to grow. While an expanding cyberspace can be of great benefit to the public, the malicious use of cyberspace can result in significant economic and social losses. In cyberspace, cyber attackers have an asymmetric advantage over defenders. In particular, if defenders lag behind cyber attackers in terms of technology or defence systems, this advantage is likely to be enhanced. Unlike cyber attackers, it is difficult for defenders to introduce a new trial technology because the defenders' main role is to ensure the stability of the defence systems which could be potentially harmed and undermined by the new trial technology.

Expansion of cyberspace

Along with technological development, cyberspace keeps growing. For example, there were globally 27.5 billion IoT devices active in cyberspace in 2017, and it is estimated that this number will reach about 40 billion by 2020.[1]



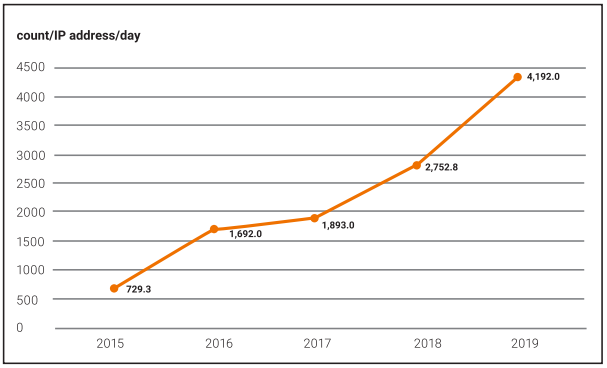
Note: the data is from "Cybersecurity 2019" by National Center of Incident readiness and Strategy for Cybersecurity of Japan

The governments of many countries share the view that digitalisation is transforming every aspect of our economies and societies. Data is increasingly becoming an important source of economic growth, and its effective use should contribute to social well-being around the world. In order to facilitate this process, the "Osaka Track" framework aimed at promoting international policy discussions and the drafting of international rules to enable the free movement of data across borders (international rules on trade-related aspects of electronic commerce at the World Trade Organization) with Japan intending to be a key player, was launched on 28 June 2019.

Threats in cyberspace

As cyberspace keeps growing, the frequency of cyber-attacks is increasing as a global trend. For example, in Japan, the number of unexpected connection attempts detected by the National Police Agency has risen to 4,192 per IP address per day in 2019.

Number of unexpected connection attempts detected by the National Police Agency of Japan



Note: from "Threats in Cyberspace in 2019" by the National Police Agency

New technologies and services, such as Artificial Intelligence (AI) and IoT, could bring about substantial benefits to the society of the future as a society in which new values and services are created continuously, making people's lives more conformable and sustainable. On the other hand, there is a growing concern that these technologies could also be used in malicious ways. The risk is that users and providers of AI- or IoT-related services will not be able to sufficiently and adequately control these technological developments and their use. With the growth of cyberspace, new threats are emerging

and their scale, scope, and frequency are increasing, and threats are escalating as more sophisticated and organised attackers are designing targeted attacks to damage or disrupt critical infrastructures and services. These disruptions can have a huge financial impact or paralyse vital activities. Cyber-attacks can generally lead to loss of money, theft of personal information/identity/IP, and damage to reputation and safety, cause problems with business services, transportation, health and power.

For example, the Central Bank of Bangladesh was hacked in December 2015, resulting in the embezzlement of about US$ 81 million, and a state-owned power company substation was attacked in December 2016 in Ukraine, resulting in a one-hour blackout. In Japan, cyber-attacks were successfully conducted to steal crypto assets in 2018.

Superiority of cyber attackers

Cyberspace is a place where everyone can utilise new information and communication technology without being constrained by location and time. A cyber attacker has the decisive advantage as he can easily copy and disseminate data and information, including computer viruses/malware, and can flexibly use advanced technologies such as AI and blockchain. In contrast, it is generally difficult for defenders to respond to cyber-attacks because the resources they can use are limited, no defensive capability remains indefinitely effective and they are forced to respond with their then currently existing systems and technologies to ensure the stability and resilience of their defence system. Unlike cyber attackers, it is difficult for defenders to introduce a new trial technology because the new trial technology can harm or undermine the stability of defence systems. In addition, it is impossible to completely eliminate vulnerabilities caused by human errors linked to the use of information systems, so that many cyber-attacks involve looking for weaknesses in user behaviour that can be exploited through seemingly legitimate means (so-called "social hacking/social engineering").

Countermeasures

As cyber-attacks are spreading in cyberspace, where attackers seem to have a constant decisive advantage over defenders and their ability to assess and address risks, "Active Cyber Defense" can be considered to be an effective countermeasure to such cyber-attacks. Having an "Active Cyber Defense" means that the organisation proactively protects itself in advance rather than responding to a cyber-attack which has occurred. In Japan, for example, the Ministry of Internal Affairs and Communications, which is the national watchdog in charge of cybersecurity-related laws and regulations, and the National Institute of Information and Communications Technology, which researches and promotes information and communications technology, have collaborated with internet service providers to launch the "NOTICE" programme designed to investigate IoT devices which might be misused/hacked in cyber-attacks because of weak authentification mechanisms (IDs and passwords), and to alert users. We understand that similar objectives are being pursued in many other countries.

To organise an "Active Cyber Defense", the utilisation of AI is considered to be very important. This is because cyber attackers always use new offensive tools to conduct cyber-attacks, so that, in order to respond to cyber-attacks effectively, detection and analysis by AI are necessary. AI technology can be used to track new patterns or offensive strategies which could otherwise not be detected without machine learning mechanisms. In addition, by introducing AI in their defence strategy, humans can focus on their analysis of causes and impact at the time of a cyber-attack and as the case may be react to false detection. It is possible to increase the efficiency and accuracy of defence systems in cyberspace but to stay one step ahead is challenging.

Relationships Between Cybersecurity and AI

Trends/directions followed by AI utilisation

As for the direction of AI utilisation, as a general principle, there is a common understanding that it is extremely important not to excessively rely on AI and that humans should keep some control over the use of AI and AI-generated results and output. Ethics and morality would be negatively impacted by the excessive use of, and total dependence on, the use of AI. At this stage, many governments or integrated areas want to provide directions and guidance for the use of AI by issuing guidelines. For example, the "Principles for a Human-centric AI Society" were published in March 2019 in Japan and the "Ethics Guidelines for Trustworthy AI" were published by the European Commission in April 2019.

Relationships between cybersecurity and AI

The globally accepted and prevalent categorisation of the relationships between cybersecurity and AI is the following and can be divided into four categories: "Attacks using AI"; "Autonomous attacks by AI"; "Attacks against AI"; and "Security measures using AI".

Attacks using AI

Cyber attackers use AI for cyber-attacks. Such attacks are actually occurring in the real world.

Autonomous attacks by AI

AI performs cyber-attacks autonomously without human intervention. However, under the current AI model, this category is not yet in existence. Once it becomes technically possible for AI to perform cyber-attacks autonomously without human intervention, one difficulty will be to allocate responsibility for civil damage caused by cyber-attacks.

Attacks against AI

This category covers cyber-attacks against AI and the so-called "Adversarial Learning"; for example, where a cyber attacker may feed fake data to AI. Such an attack could become realistic in the future if human involvement in AI monitoring declines and the use of AI for critical decisions (such as medical diagnostics and investment decisions, etc.) becomes generalised.

Security measures using AI

This category covers defenders using AI against cyber-attacks. Various attempts have already been made, such as the automation of malware detection. At present, human beings continue to be responsible for determining those issues to be solved by AI and interpreting decisions by AI. Therefore, it is necessary to develop human resources that can fully utilise AI.

We discuss "Security measures using AI" in further detail below.

Security Measures Using AI

Benefits of using AI

There are four benefits of using AI for cybersecurity:

Reducing the cost of detection and response to breaches
Using AI for cybersecurity enables organisations to understand and reuse threat patterns to identify new threats. This leads to an overall reduction in time and effort to identify threats and incidents, investigate them, and remediate incidents.

Becoming faster at responding to breaches
A fast response is essential to protect an organisation from cyber-attacks. According to Capgemini's Reinventing Cybersecurity with Artificial Intelligence Report of 2019, using AI for cybersecurity, the overall time taken to detect threats and breaches is reduced by up to 12% and the time taken to remediate a breach or implement patches in response to an attack is also reduced by 12%. A small subset of organisations even managed to reduce these time metrics by more than 15%.

Increasing efficiency
Cyber analysts spend considerable time going through data logs and/or incident timesheets. Notwithstanding the significant workforce involved in cybersecurity, cyber analysts with deep knowledge of this field are rare. By using good data to analyse potential threats, AI enables cyber analysts to focus on works which only humans can do, such as analysing the incidents identified by the AI cybersecurity algorithms.

Making new revenue streams
As mentioned above, with the proliferation of IoT devices, the number, scope and scale of attacks have significantly increased. This creates opportunities for vendors offering cybersecurity services to manufacturers of IoT devices. Many players are taking advantage of the huge market opportunities.

Present Status of security measures using AI

As mentioned above, the benefits of using AI for cybersecurity purposes are plentiful, but at present AI can only be used to assist human work conducted for the purpose of cybersecurity, and human involvement is necessary. In other words, it is still necessary for human beings to remain in charge of customising teacher data to be learned by AI, determining issues to be solved by AI, and interpreting AI decisions.

In addition, decisions by AI use the "black box" model that lacks transparency, providing only input-output without the underlying rationale, and it is difficult to determine why a decision has been made. In contrast, it is possible to clearly explain how white-box models behave and produce predictions and what the influencing variables are. However, they are yet to be put into practical use.

Security Measures Using AI and Fiduciary Duty of Care

Fiduciary duty of care

In many jurisdictions, directors and officers (hereinafter officers) of a company owe a fiduciary duty of care to the company. If an officer breaches a fiduciary duty of care in performing his/her role, the officer is liable to the company for the damage caused as a result.

Can it be considered that officers appropriately fulfil their fiduciary duty of care by introducing AI for cybersecurity purposes?

Use of AI for security measures and performance of fiduciary duty of care

As mentioned above, there are still many technical hurdles before AI can be used for security measures, so that the introduction of AI itself in corporate procedures and strategies does not necessarily mean that the officer in charge of cybersecurity is appropriately discharging his/her duty and can be exculpated if anything happens. Fairly common standards are used in many jurisdictions to determine the existence of a breach of fiduciary duty: whether the fiduciary duty of care is appropriately fulfilled is determined based on what would normally be expected from an ordinary officer having reasonable skills, experience and knowledge in a company of the same size and industry. Therefore, the introduction of AI does not necessarily mean that officers have appropriately fulfilled their fiduciary duty of care under the present state of the art where it is clear that adequate and sufficient cybersecurity protection cannot be achieved through the mere introduction of AI without appropriate human intervention and monitoring. Unless comprehensive security measures such as appropriate human intervention and human decision-making are introduced, cybersecurity measures could be deemed insufficient. Accordingly, it is important for officers to build comprehensive cybersecurity system frameworks, and AI could be used to achieve this purpose.

However, once these AI issues are resolved and the mere introduction of an AI-based cybersecurity system is widely recognised as appropriate for the cybersecurity protection of the company, it may be possible that an officer will be deemed to perform his fiduciary duty of care by simply introducing the appropriate AI-based cybersecurity system. If the absence of an AI-based cybersecurity system becomes a negative factor in the determination of a breach of fiduciary duty of care, it will be an incentive for all officers to introduce AI.

Future Prospects

As mentioned above, AI still has a lot of issues to overcome to form a stand-alone cybersecurity system. However, even at this early stage, in light of the benefits which could be derived from its use, AI will become an unavoidable tool in any efficient cyber defence strategy (especially where AI is being used in the attack). The Tokyo Olympics, originally scheduled for 2020, had been a target prior to their postponement, and the 2025 World Exposition to be held in Japan is also an obvious target. Major events have become attractive targets for "hacktivists" and fraudsters. The Rio de Janeiro Olympics in 2016 and the Pyeongchang Olympics in 2018 have been under heavy attacks (with allegations of cyberwarfare).

Cybersecurity is a hot topic and will be so for years to come. Every state, business and individual will need to remain wary and watchful: no doubt AI will help.

Endnote

1. National Center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity 2019*, May 23rd, 2019.

Akira Matsuda is an attorney-at-law (admitted in Japan and New York) and a partner at Iwata Godo heading the AI/TMT and Data Protection practice group. He is based in Tokyo and Singapore. His practice focuses on cross-border transactions, including mergers and acquisitions, as well as international disputes (litigation/arbitration), and advice on digital/TMT-related matters. Mr. Matsuda regularly advises Japanese and foreign clients on data security issues (Japanese laws, Singapore PDPA, and EU GDPR) including on the structuring of global compliance systems. He also advises complicated cross-border corporate investigation matters.
He is a graduate of the University of Tokyo (LL.B.) and Columbia Law School (LL.M.).

Iwata Godo
Marunouchi Building 15F
2-4-1 Marunouchi
Chiyoda-ku
Tokyo 100-6315
Japan

Tel: +81 3 3214 6205
Email: amatsuda@iwatagodo.com
URL: www.iwatagodo.com

Hiroki Fujita is an attorney-at-law (admitted in Japan) and associate at Iwata Godo. He is a member of the firm's AI/TMT and Data Protection practice group. His practice focuses on intellectual property law and IT. Mr. Fujita regularly advises clients across a broad range of industries, including electric power utilities and telecom carriers on data protection and cybersecurity issues. Mr. Fujita also advises clients on corporate matters, including mergers and acquisitions and corporate disputes (litigation/arbitration).
He is a graduate of Osaka University (LL.B.) and the Kyoto University School of Law (J.D.).

Iwata Godo
Marunouchi Building 15F
2-4-1 Marunouchi
Chiyoda-ku
Tokyo 100-6315
Japan

Tel: +81 3 3214 6205
Email: hiroki.fujita@iwatagodo.com
URL: www.iwatagodo.com

Iwata Godo is one of Japan's premier and oldest law firms. It was established in 1902 as one of the first business law firms by Chuzo Iwata, an attorney-at-law who subsequently held various positions, including serving as Minister of Justice and president of the Japan Federation of Bar Associations. It is a full-service firm with around 80 attorneys and each of its practice areas is highly regarded. It is the firm of choice for clients with respect to their most challenging legal issues, including in relation to data protection, privacy and cybersecurity.

www.iwatagodo.com

IWATA GODO
Established 1902

Australia


Dennis Miralis


Phillip Gibson


Jasmina Ceic

Nyman Gibson Miralis

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

In Australia, unauthorised access to computer systems is criminalised by both State and Federal legislation. In the Federal jurisdiction, hacking is criminalised under the *Criminal Code Act 1995* (Cth) ("*the Code*"). Most commonly, persons suspected of engaging in cybercrime are charged pursuant to *the Code*, given its universal application in all States and Territories in Australia.

Persons suspected of unauthorised access to computer systems are charged pursuant to s. 478.1 of *the Code*, which provides for the offence of "Unauthorised access to, or modification of, restricted data". The offence comprises three elements of proof. The offence is committed if: a person causes any unauthorised access to, or modification of, restricted data; the person intends to cause the access or modification; and the person knows that the access or modification is unauthorised. The maximum penalty for a contravention of s. 478.1 of *the Code* is two years' imprisonment. For the purposes of this offence, "restricted data" means data to which access is restricted by an access control system associated with a function of the computer.

As an example of state-based legislation criminalising hacking against private computer systems, Part 6 the *New South Wales Crimes Act 1900* ("*NSW Crimes Act*") – Computer Offences sets out multiple offences centred around unauthorised access, modification, or impairment of restricted data and electronic communications.

Denial-of-service attacks

Denial-of-Service attacks ("DoS attacks") or Distributed Denial-of-Service attacks ("DDoS attacks") are criminalised by s. 477.3 of *the Code*, which provides for the offence of "Unauthorised impairment of electronic communication".

The offence comprises two elements and committed if a person causes any unauthorised impairment of electronic communication to or from a computer and the person knows that the impairment is unauthorised. The maximum penalty for a contravention of s. 477.3 of *the Code* is 10 years' imprisonment.

Phishing

Phishing, being a form of online fraud, is criminalised under *the Code* in instances where the victim is said to be a Commonwealth entity. When the victim is a member of the public, charges are brought under parallel State or Territory legislation. In New South Wales ("NSW"), charges could be brought under s. 192E of the *NSW Crimes Act* which criminalises the general offence of fraud.

Prosecutions for Commonwealth fraud could encompass a wide variety of offending conduct, including phishing-style offences which would affect a Federal government body. Depending on the subsequent financial gain or loss suffered subsequent to the activity, the below charges are available:

- S. 134.2(1) – obtaining a financial advantage by deception.
- S. 135.1(1) – general dishonesty – obtaining a gain.
- S. 135.1(3) – general dishonesty – causing a loss.
- S. 135.1(5) – general dishonesty – causing a loss to another.

For the charge to be proven, the prosecution must establish that the accused obtains or causes a financial advantage, gain or loss by way of deception or dishonesty. The maximum penalty for each offence is 10 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

The infection of IT systems with malware is criminalised by s. 478.2 of *the Code*, which provides for the offence of "Unauthorised impairment of data held on a computer disk etc.".

The offence comprises three elements and committed if: a person causes any unauthorised impairment of the reliability, security or operation of data held on a computer disk, a credit card or another device used to store data by electronic means; the person intends to cause the impairment; and the person knows that the impairment is unauthorised. The maximum penalty is two years' imprisonment.

As an example of state-based offences of this nature, conduct of this type would likely be encompassed within the "modification or impairment" aspects of the *NSW Crimes Act* computer offences.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime is criminalised by s. 478.4 of *the Code*, which provides for the offence of producing, supplying or obtaining data with intent to commit a computer offence. The offence comprises two elements.

The offence is committed if: a person produces, supplies or obtains data; and the person does so with the intention that the data be used, by the person or another person, in committing an offence against Division 477 of *the Code* or facilitating the commission of such an offence. The maximum penalty for a contravention of s. 478.4 of *the Code* is three years' imprisonment.

Possession or use of hardware, software or other tools used to commit cybercrime

Possession or use of hardware, software or other tools used to commit cybercrime is criminalised by s. 478.3 of *the Code*, which provides for the offence of possession or control of data with intent to commit a computer offence.

The offence comprises two elements. The offence is committed if: a person has possession or control of data; and the person has that possession or control with the intention that the data be used, by the person or another person, in committing an offence against Division 477 of *the Code* or facilitating the commission of such an offence. The maximum penalty for a contravention of s. 478.3 of *the Code* is three years' imprisonment.

An example of a state equivalent can be found in ss. 308F and 308G of the *NSW Crimes Act*.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity crime, and in particular identity fraud offences, are criminalised by Division 372 of *the Code*. Particular acts that are criminalised include dealing in identification information, dealing in identification information that involves use of a carriage service, possession of identification information and possession of equipment used to make identification information. The offence of "Dealing in identification information that involves use of a carriage service" is most relevant to cybercrime. It is criminalised by s. 372.1A of *the Code* and comprises four elements. The offence is committed if: a person deals in identification information; the person does so using a carriage service; the person intends that any person will use the identification information to pretend to be, or to pass the user off as, another person (whether living, dead, real or fictitious) for the purpose of committing an offence or facilitating the commission of an offence; and the offence is an indictable offence against the law of the Commonwealth, an indictable offence against a law of a State or Territory or a foreign indictable offence. The maximum penalty is five years' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft is criminalised by s. 478.1 of *the Code*. As the offence is committed if a person modifies restricted data, modification is defined in *the Code* as the alteration or removal of the data held in a computer, or an addition of the data held in a computer, the unauthorised copying of data from a computer would contravene the offence provision.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Penetration testing activity without authority could offend the above-mentioned s. 478.1 of *the Code* which provides for the offence of "Unauthorised access to, or modification of, restricted data".

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Part 10.6 of *the Code* creates offences related to telecommunication services. They include offences relating to dishonesty with respect to carriage services and interference with telecommunications.

Additionally, the above-mentioned Part 6 of the *NSW Crimes Act* would likely be an example of state legislation that could cover these types of activities.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Extended geographical jurisdiction applies to offences under Part 10.7 of *the Code* (Divisions 477 and 478).

A person will not commit offences under that Part unless: the conduct constituting the alleged offence occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; or the conduct constituting the alleged offences occurs wholly outside Australia and a result of the conduct occurs wholly or partly in Australia, or wholly or partly on-board an Australian aircraft or an Australian ship; or the conduct constituting the alleged offence occurs wholly outside Australia and at the time of the alleged offence, the person is an Australian citizen or at the time of the alleged offence, the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; or all of the following conditions are satisfied: the alleged offence is an ancillary offence; the conduct constituting the alleged offence occurs wholly outside Australia; and the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs, or is intended by the person to occur, wholly or partly in Australia or wholly or partly on-board an Australian aircraft or an Australian ship.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The *Crimes Act 1914* (Cth) prescribes the sentences applicable to breaches of Federal legislation, such as *the Code*. Relevant matters for consideration on sentences are set out as a non-exhaustive list of factors under s. 16A of the *NSW Crimes Act* (Cth). Matters that generally will mitigate a penalty include the timing of any guilty plea, the offender's character, the offender's prior record, assistance provided by the offender to the authorities and the offender's prospect of rehabilitation and likelihood of reoffending. The absence of intent to cause damage or make a financial gain could be taken into account by a sentencing court as a factor of mitigation.

A number of the offences particularised above cannot be "attempted"; they must actually be committed. For example, a person cannot attempt to commit the offence of "Unauthorised access, modification or impairment with intent to commit a serious offence".

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The following laws in Australia relate to cybersecurity: the *Privacy Act* (Cth) ("*Privacy Act*"); the *Crimes Act 1914* (Cth); the *Security of Critical Infrastructure Act 2018* (Cth); *the Code* (Cth); and the *Telecommunications (Interception and Access) Act 1979* (Cth).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The *Security of Critical Infrastructure Act 2018* (Cth), which commenced on 11 July 2018, seeks to manage national security risks of sabotage, espionage and coercion posed by foreign entities. The Act was implemented as a response to technological changes that have increased cyber connectivity to critical infrastructure. The Australian Government considers "the responsibility for ensuring the continuity of operations and the provision of essential services to the Australian economy and community" as being shared "between owners and operators of critical infrastructure, state and territory governments and the Australian Government". The Act applies to approximately 165 specific assets in the electricity, gas, water and ports sectors.

The Act establishes a Register of Critical Infrastructure Assets, empowers the Secretary of the Department of Home Affairs with an information-gathering power (whereby certain information can be requested of direct interest holders, responsible entities and operators of critical infrastructure assets), and a Minister has the power to issue a direction to an owner or operator of critical infrastructure assets to mitigate national security risks.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Australian Securities and Investments Commission ("ASIC") provides guidance to Australia's integrated corporate markets, financial services and consumer regulator, and organisations through its "cyber reliance good practices". The good practices recommend, *inter alia*, periodic review of cyber strategy by a board of directors, using cyber resilience as a management tool, for corporate governance to be responsive (i.e. keeping cybersecurity policies and procedures up to date), collaboration and information sharing, third-party risk management and implementing continuous monitoring systems.

The Office of the Australian Information Commissioner ("OAIC") recommends that entities have a data breach response plan which includes a strategy for containing, assessing and managing data breaches and strategies for containing and remediating data breaches.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

In February 2018, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* amended the *Privacy Act* to require Australian Privacy Principles ("APP") entities to, as soon as practicable, provide notice to the OAIC and affected individuals of an "eligible data breach", where there are reasonable grounds to believe that an "eligible data breach" has occurred. This process is called the Notifiable Data Breaches Scheme ("NDB Scheme").

Eligible data breaches arise when: there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds; this unauthorised disclosure of personal information, or loss of personal information, is likely to result in serious harm to one or more individuals; and the entity has not been able to prevent the likely risk of serious harm with remedial action. Indicators such as malware signatures, observable network vulnerabilities and other "red-flag" technical characteristics may represent reasonable grounds for an APP entity to form a belief that an eligible data breach has occurred.

The OAIC expects APP entities to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm.

The notification to the OAIC must include the identity and contact details of the organisation, a description of the data breach, the kinds of information concerned and recommendations about the steps individuals should take in response to the data breach.

Under the *Privacy Act*, an APP entity is defined as an "agency" or "organisation". "Agency" includes a Minister, a Department, and most government bodies, whilst "organisation" means an individual, a body corporate, a partnership, any other unincorporated association or a trust that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The affected individual must also be notified of an "eligible data breach", as defined above. The notification must include the identity and contact details of the organisation, a description of the data breach, the kinds of information concerned and recommendations about the steps individuals should take in response to the data breach.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The OAIC is an independent statutory agency within the Attorney-General's Department. The OAIC has three functions; namely, privacy functions conferred by the *Privacy Act*, freedom of information functions, such as reviewing the decisions made by agencies and Ministers pursuant to the *Freedom of Information Act 1982* (Cth), and government information policy functions conferred by the *Australian Information Commissioner Act 2010* (Cth).

In relation to its privacy functions, the OAIC has the power to commence investigations, conduct privacy performance assessments, request an entity to develop an enforceable code, direct an agency to give the OAIC a privacy impact assessment about a proposed activity or function and recognise external dispute resolution schemes to handle privacy-related complaints.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

A failure to comply with the notification obligations can result in the imposition of substantial civil penalties. A serious or repeated interference with privacy attracts a fine of 2,000 penalty units, currently AUD 420,000.00. The maximum penalty that a court can order for a body corporate is five times the amount listed in the civil penalty provision, currently a maximum of AUD 2.1 million.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The *Privacy Act* confers a number of additional enforcement powers on the OAIC, including accepting an enforceable undertaking, bringing proceedings to enforce an enforceable undertaking, making a determination, making orders that the APP entity must redress any loss or damage suffered by the complainant and that the complainant is entitled to payment of compensation for such loss or damage, bringing proceedings to enforce a determination, delivering a report to the responsible Minister and seeking an injunction

The OAIC reported that, in response to Commissioner-initiated investigations, enforceable undertakings were accepted by two APP entities during 2019, namely Wilson Asset Management (International) Pty Ltd, and the Commonwealth Bank of Australia.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There are presently no laws in Australia which prohibit the use of a Beacon or near-field communication technology.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are presently no laws in Australia which prohibit the use of Honeypot technology or similar autonomous deception measures.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are presently no laws in Australia which prohibit the use of Sinkhole technology. The malicious use of Sinkhole methods to steer legitimate traffic away from its intended recipient may, however, constitute an offence under s. 477.3 of *the Code*.

Sinkholes can be lawfully used as a defensive practice for research and in reaction to cyber-attacks. In this capacity, Sinkholes are a tool used by both public and private agencies.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

There are presently no laws in Australia which prohibit organisations from monitoring or intercepting electronic communications on their networks.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There are presently no laws in Australia which prohibit the import or export of technology designed to prevent or mitigate the impact of cyber-attacks.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice varies across different business sectors in NSW. The NDB Scheme, for example, only requires Australian government agencies, private sector companies and not-for-profit organisations with an annual turnover of more than AUD 3 million to report data breaches.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Part IIIA of the *Privacy Act* specifically regulates the handling of personal information about individuals' activities in relation to consumer credit, including the types of personal information that credit providers can disclose. All credit reporting bodies (defined in ss 6 and 6P as a business that involves collecting, holding, using or disclosing personal information about individuals

for the purposes of providing an entity with information about the creditworthiness of an individual) are subject to Part III.

Part 13 of the *Telecommunications Act 1997* (Cth) regulates carriers and carriage service providers in their use and disclosure of personal information. Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth) requires providers of telecommunications services in Australia to collect and retain specific types of data for a minimum period of two years and must comply with the *Privacy Act* in relation to that data.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

A failure by a company to prevent, mitigate, manage or respond to an Incident may result in breaches of provisions of the *Corporations Act 2001* (Cth). *The Corporations Act 2001* (Cth) imposes duties on directors to exercise powers and duties with the care and diligence that a reasonable person would. A director who ignores the real possibility of an Incident may be liable for failing to exercise their duties with care and diligence.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Presently, the Applicable Laws do not require companies to designate a chief information security officer ("CISO"), establish a written Incident response plan or policy, conduct periodic cyber risk assessments or perform penetration tests or vulnerability assessments.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Other than those mentioned in section 2, no further specific disclosure is required in relation to cybersecurity risks or Incidents.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Australian common law does not recognise a general right of privacy. The equitable cause of action for breach of confidence may provide a remedy for invasions of privacy. Traditionally, the elements are that information must be confidential, information must have been imparted in circumstances importing an obligation of confidence and there must be an unauthorised use of that information. The current doctrine of breach of confidence does not currently entertain cases of wrongful intrusion, as opposed to cases of wrongful disclosure of confidential information.

The *Privacy Act* regulates the way Commonwealth agencies handle personal information. A person may obtain an injunction in the Federal Circuit Court against a Commonwealth agency that engages in, or proposes to engage in, conduct that is in breach of the *Privacy Act*. An action cannot be brought against an individual acting in their own capacity. A person may apply to the Court for an order that an entity pay compensation for loss or damage suffered by the person if a civil penalty has been made against the entity, or the entity is found guilty of an offence under the *Privacy Act*.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

No relevant civil proceedings or other private actions have been brought by individuals in relation to an Incident. Given the evolution of the doctrine of breach of confidence, it is likely such cases will be forthcoming.

Investigations conducted by the OAIC most commonly result in out-of-court outcomes. For example, a joint investigation conducted by the Australian Privacy Commissioner and the Privacy Commissioner of Canada into a highly publicised hacking breach of confidential data held by online adult dating service Ashley Madison resulted in an enforceable undertaking being entered into by the company pursuant to s. 33E of the *Privacy Act*.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The High Court in *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 sanctioned the recognition of a tort of invasion of privacy. Judge Hampel in the case of *Doe v ABC* (2007) VCC 281 imposed liability in tort for the invasion of the plaintiff's privacy. Such reasoning may apply to an action in relation to a failure to prevent an Incident.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations are permitted to take out insurance against Incidents in Australia. This includes breaches of the *Privacy Act*.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limits specifically targeted at losses associated with Incidents. Numerous entities offer insurance for data breaches, business interruptions, email forgery, ransomware attacks, costs of rebuilding an IT system, theft of crypto-currencies and legal fees associated with the investigation of Incidents. Coverage is governed generally by the *Insurance Act 1973* (Cth), the *Insurance Contracts Act 1984* (Cth), *Corporations Act 2001* (Cth) and the common law.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

A number of well-established legal investigatory powers are deployed by law enforcement authorities when investigating an Incident. These powers can include the issuing of search warrants, the seizure of IT equipment for forensic analysis, decryption (whether at encrypted or decrypted data points) and the compulsory examination of suspects in certain circumstances.

The Australian Signals Directorate ("ASD") assumes responsibilities for defending Australia from global threats and advances its national interests through the provision of foreign signals intelligence, cybersecurity and offensive cyber operations as directed by the Australian Government. One of the express strategic objections of the ASD is to provide advice and assistance to law enforcement. To this end, the ASD can collaborate with the Federal, State and Territory police forces in relation to matters of national interest, including emerging areas such as cyberterrorism.

See the answer to question 8.2 below for statutory notices which can be issued by law enforcement agencies to access data held by designated communications providers.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

On 8 December 2018, the Federal Parliament passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. The Bill provides for the facilitation of covert access to data for the purposes of disrupting and investigating criminal activity, as well as establishing a framework to facilitate lawful assistance from communications providers.

The legislation allows various Australian law enforcement and intelligence agencies to make a Technical Assistance Notice ("TAN"), ordering designated communications providers to provide data or assistance in relation to criminal investigations or matters of security. This may include access to encryption keys or provision of decrypted data. Similarly, a Technical Capability Notice ("TCN") can be issued, mandating that a designated communications provider establish new capability to intercept and decrypt communications that would otherwise be encrypted or inaccessible.

The above notices may be issued in a broad variety of circumstances, including the enforcement of criminal laws and laws imposing pecuniary penalties, either in Australia or in a foreign country, or if it is in the interests of Australia's national security, Australia's foreign relations, or Australia's national economic wellbeing.

A designated communications provider, including an individual employed or acting on behalf of such providers, who has been compelled to provide data or assistance under a computer access warrant and fails to do so, may face up to 10 years' imprisonment, a fine of up to 600 penalty units (currently AUD 126,000) or both.

S. 3LA of the *Crimes Act 1914* (Cth) also provides law enforcement authorities a mechanism by which a person must provide information or assistance that is reasonable and necessary to allow a constable to: access data held in, or accessible from, a computer or data storage device that is on warrant premises or that has been moved to a place for examination under subsection 3K(2) of the *Crimes Act 1914* (Cth); copy data held in, or accessible from, a computer or storage device; and convert into documentary form, or another form intelligible to a constable, data held in, or accessible from, a computer or data storage device, or data held in a data storage device to which the data was copied, or data held in a data storage device removed from warrant premises under subsection 3L(1A) of the *Crimes Act 1914 (Cth)*.

Dennis Miralis is a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions. His areas of expertise include cybercrime, global investigations, proceeds of crime, bribery and corruption, anti-money laundering, worldwide freezing orders, national security law, Interpol Red Notices, extradition and mutual legal assistance law. Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies.
Full biography: https://ngm.com.au/our-team/dennis-miralis-partner-defence-lawyer/.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: dm@ngm.com.au
URL: www.ngm.com.au

Phillip Gibson is one of Australia's leading criminal defence lawyers, with over 30 years of experience in all areas of criminal law. Phillip has significant experience in transnational cases across multiple jurisdictions, often involving: white-collar and corporate crime; asset forfeiture; money laundering and proceeds of crime; extradition; mutual legal assistance; Royal Commissions; bribery and corruption; and the Independent Commission Against Corruption ("ICAC") and Crime Commission matters. He has extensive experience in dealing with all major Australian and international investigative agencies.
Full biography: https://ngm.com.au/our-team/phillip-gibson-partner-specialist-defence-lawyer/.

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: pg@ngm.com.au
URL: www.ngm.com.au

Jasmina Ceic is an accomplished criminal trial advocate. She advises and acts in complex criminal law matters at all levels of the court system, with a specialist focus on serious matters that proceed to trial in the Superior Courts, as well as conviction and sentence appeals heard in the Court of Criminal Appeal. She has represented and advised persons and companies being investigated for white-collar and corporate crime, complex international fraud and transnational money laundering.
Full biography: https://ngm.com.au/our-team/jasmina-ceic-senior-associate/.

Nyman Gibson Miralis
Suite 8, Level 2
154 Marsden Street
Parramatta NSW 2150
Australia

Tel: +61 2 9633 4966
Email: jc@ngm.com.au
URL: www.ngm.com.au

Nyman Gibson Miralis is an international award-winning criminal defence law firm based in Sydney, Australia. For over 50 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia's most significant criminal cases.

Our international law practice focuses on cybercrime, white-collar and corporate crime, transnational financial crime, bribery and corruption, international money laundering, international asset freezing or forfeiture, extradition and mutual legal assistance law.

Nyman Gibson Miralis strategically advises and appears in matters where transnational cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with international partners, we have advised and acted in investigations involving the USA, Canada, the UK, the EU, China, Hong Kong, Singapore, Taiwan, Macao, Vietnam, Cambodia, Russia, Mexico, South Korea, the British Virgin Islands, New Zealand and South Africa.

www.ngm.com.au

NYMAN GIBSON MIRALIS
Defence Lawyers and Advisors est. 1966

Austria


Christoph Haid


Veronika Wolfbauer


Michael Lindtner

Schönherr Rechtsanwälte GmbH

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Hacking may constitute the criminal offences of illegal access to a computer system (Sec. 118a of the Austrian Criminal Code, "**ACC**") or illegal interception of messages or data (Secs 119, 119a ACC). Depending on the circumstances of the case, these offences provide a fine of up to 360 daily rates or imprisonment of up to six months, and in severe cases even up to three years (i.e. if critical infrastructure is affected and the perpetrators act within a criminal organisation).

Hacking may involve unlawful access, use, alteration or disclosure of personal data. If personal data is processed unlawfully, this constitutes an administrative offence, with a fine of up to EUR 20 million or up to 4% of the total worldwide annual turnover, whichever is higher (Art. 83 General Data Protection Regulation, "**GDPR**"). If not covered by Art. 83 GDPR, intentionally and illegally gaining access to data processing or maintaining an obviously illegal means of access may lead to an administrative fine of up to EUR 50,000 (Sec. 62 (1) Austrian Data Protection Act, "**ADPA**").

Furthermore, the unlawful processing of personal data may also constitute the criminal offence of data processing with the intention to make a profit or to cause harm (Sec. 63 ADPA), with a fine of up to 720 daily rates or imprisonment of up to one year.

Denial-of-service attacks

Denial-of-service attacks may constitute the criminal offence of disruption of IT systems, pursuant to Sec. 126b ACC. According to this provision, anyone who seriously disrupts the functioning of an IT system, which he may not have at his disposal or not alone in his disposal, by entering or transmitting data shall be punished by imprisonment of up to six months or a fine of up to 360 daily rates, and in severe cases by imprisonment of between six months and five years (e.g. if the damage exceeds EUR 300,000). Further, denial-of-service attacks could also constitute data corruption, pursuant to Sec. 126a ACC, if data is destroyed or manipulated by the attack. Sec. 126a ACC provides punishment by imprisonment of up to six months or a fine of up to 360 daily rates or, in severe cases, by imprisonment of between six months and five years (e.g. if the damage exceeds EUR 300,000).

Denial-of-service attacks usually do not involve the processing of personal data. However, in case personal data is processed unlawfully, see "Hacking (i.e. unauthorised access)" above.

Phishing

Phishing can constitute various criminal offences, which highly depends on the circumstances of the case. If the victim is, for example, deceived and misled to a self-damaging act (e.g. a bank transfer), phishing may constitute fraud according to Sec. 146 *et seq.* ACC, which shall be punished in severe cases by imprisonment of between one and 10 years (if the damage exceeds EUR 300,000). Phishing could also constitute misuse of software or access data, pursuant to Sec. 126c ACC, under certain conditions, e.g. if the perpetrator thereby obtains access data (e.g. passwords) with the intent to damage the respective IT system. Sec. 126c ACC will be punished by imprisonment of up to six months or a fine of up to 360 daily rates. Moreover, phishing can constitute a breach of Sec. 241h ACC, which covers, *inter alia*, spying-out data of non-cash means of payment with the intent to illegally enrich oneself or third parties thereby, and will be punished by imprisonment of up to one year or 720 daily rates (in severe cases, imprisonment of up to three years).

Phishing typically involves the unlawful processing of personal data. For further information on the administrative and criminal penalties, see "Hacking (i.e. unauthorised access)" above.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Infection of IT systems with malware may constitute various offences under the ACC. Malware that manipulates or destroys data may, for example, constitute data corruption (Sec. 126a ACC), which will be punished by imprisonment of up to six months or a fine of up to 360 daily rates or, in severe cases, imprisonment of between six months and five years (e.g. if the damage exceeds EUR 300,000). If the IT system is seriously disrupted by the infection, this could also constitute disruption of IT systems (Sec. 126b ACC), which shall be punished

by imprisonment of up to six months or a fine of up to 360 daily rates, and in severe cases, by imprisonment of between six months and five years. Further, infection of IT systems with malware could also constitute illegal interception of messages or data (Secs 119, 119a ACC) under certain conditions, which will be punished by imprisonment of up to six months or a fine of up to 360 daily rates. The use of ransomware may further constitute blackmail (Sec. 144 ACC) punished by imprisonment of between six months and five years (in severe cases between one year and 10 years).

Where malware is used to unlawfully access, use, alter or disclose (or, more generally, process) personal data, the administrative and criminal penalties listed under "Hacking (i.e. unauthorised access)" apply.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Distribution of software or hardware or other tools which are, according to their specific nature, designed for certain cyber-crimes (e.g. spy-software, worms, trojans, viruses, etc.), may be punished under Sec. 126c ACC (misuse of software or access data) by imprisonment of up to six months or a fine of up to 360 daily rates.

Possession or use of hardware, software or other tools used to commit cybercrime

The possession of such means is punishable under Sec. 126c ACC (misuse of software or access data) if the perpetrator also has the intent to use these means for cyber-crimes. Otherwise, the mere possession of such means is not punishable under the ACC.

Identity theft or identity fraud (e.g. in connection with access devices)

Austrian criminal law does not provide for a specific offence covering identity theft. However, identity theft may constitute processing with the intention to make a profit or to cause harm according to Sec. 63 ADPA, or data falsification under Sec. 225a ACC, which covers the creation of false data or falsification of data by entering, manipulation, deletion or suppression with the intent of using them in legal transactions to prove a right, a legal relationship or a fact. Breaches of Sec. 225a ACC will be punished by imprisonment of up to one year or a fine of up to 720 daily rates. Further, depending on the specifics of the case, fraud (Sec. 146 ACC), defamation (Sec. 297 ACC) or insult (Sec. 115 ACC) could be relevant, providing penalties ranging from (i) imprisonment of one to 10 years (severe fraud), to (ii) imprisonment of up to three months or a fine of up to 180 daily rates (insult).

Identity theft or identity fraud requires the unlawful processing of personal data and thus constitutes an administrative offence with a fine of up to EUR 20 million or up to 4% of the total worldwide annual turnover, whichever is higher (Art. 83 GDPR).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft may in particular constitute the criminal offences of (i) processing with the intention to make a profit or to cause harm according to Sec. 63 ADPA (imprisonment of up to one year or a fine of up to 720 daily rates), (ii) violation of business secrets according to Sec. 11 of the Austrian Unfair Competition Act (imprisonment of up to three months or a fine of up to 180 daily rates), (iii) spying-out business secrets, pursuant to Sec. 123 ACC, if the secrets were not accessible by the perpetrator in his/her ordinary business activities and he/she acts also with the intent to disclose or utilise the business secrets (imprisonment of up to two years) or, under certain conditions, (iv) illegal access to a computer system according to Sec. 118a ACC if the perpetrator overcomes specific security measures in the IT system. Moreover, Secs 121 and 122 ACC protect special business secrets and could thus be relevant. However, the scope of these offences is, in practice, rather narrow. Depending on the circumstances of the case, the above-mentioned offences relating to phishing can also be relevant regarding electronic theft.

In case personal data is processed unlawfully, see "Hacking (i.e. unauthorised access)" above. In addition, transmitting data intentionally in violation of the rules on confidentiality (in particular by employees) is an administrative offence punishable by a fine of up to EUR 50,000 (Sec. 62 (1) (2) ADPA).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Austrian criminal law does not explicitly govern "white-hat-hacking", which is why such cases need to be assessed on a case-by-case basis. However, there are good arguments that unsolicited testing of IT systems only to determine their vulnerabilities and weak points should not trigger criminal liability if the hacker does obviously not act with the intent to commit a criminal act and ensures the protection of the IT system, its data and third parties during the test.

In case personal data is processed unlawfully, see "Hacking (i.e. unauthorised access)" above.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The most relevant cyber-crime provisions in the ACC consist of illegal access to a computer system (Sec. 118a ACC), violation of telecommunication secrecy (Sec. 119 ACC) and illegal interception of data (Sec. 119a), data corruption (Sec. 126a), disruption of IT systems (Sec. 126b ACC), misuse of software or access data (Sec. 126c ACC) and spying-out data of non-cash means of payment (Sec. 241h ACC).

In case personal data is processed unlawfully, see "Hacking (i.e. unauthorised access)" above.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The GDPR may be applicable to controllers established outside the EU/EEA in accordance with Art. 3 (2) GDPR.

The offences in the ACC, mentioned under question 1.1 above, have no explicit extraterritorial application. However, the ACC applies on all acts committed within Austria, which is the case if the perpetrator either acted in Austria or the effects of the offence occurred in Austria. Therefore, the ACC may also apply in cases where the perpetrator is physically not present in Austria but, for example, attacks an Austrian-based IT system from abroad.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

If the hacker does not act with the intent to constitute the

respective criminal offence and ensures that there will be no damage, criminal liability would probably not be given. However, due to lack of jurisdiction, clear legal guidelines for ethical hacking are still missing, which is why we recommend assessing such cases on an individual basis. Nonetheless, even if a criminal offence would be constituted, Sec. 34 ACC stipulates mitigating factors for setting the actual punishment such as "noteworthy motives" or "absence of damages although the offence was committed", which could lower the penalty.

If personal data is processed unlawfully, the administrative fines under the GDPR and the ADPA apply irrespective of the intentions of the perpetrator or any ethical considerations. However, such considerations may be relevant when deciding the severity of the penalty (see Sec. 11 ADPA and Art. 82 (2) GDPR). Furthermore, in the case of first-time infringements, the ADPA shall use its corrective powers in accordance with Art. 58 GDPR, in particular by issuing reprimands.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The most relevant laws on cybersecurity include the GDPR, ADPA and the Network and Information System Security Act (*Netz- und Informationssystemsicherheitsgesetz*, "**NISG**"). For sector-specific laws on cybersecurity, please refer to question 4.2 below.

From a criminal law perspective, the ACC, with its cybercrime provisions under Sec. 118a *et seq.*, is the most relevant law in terms of cybersecurity. Further, the Austrian Unfair Competition Act also contains certain laws indirectly relating to cybersecurity, such as provisions protecting business secrets.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Austria has implemented the NIS Directive (Directive EU 2016/1148) with the NISG. According to Sec. 17 NISG, operators of essential services shall take *appropriate and proportionate technical and organisational measures* ("**TOMs**") to manage the risks posed to the security of network and information systems that they use in their operations. Those measures shall ensure a level of security of network and information systems appropriate to the risk posed and conform to the state of the art.

The NISG applies to services in the sectors of energy, transport, banking, financial market infrastructures, health, drinking water supply and digital infrastructure. The service must be essential, in particular, for the maintenance of the public health service, the public supply of water, energy and vital goods, public transport or the functioning of public information and communication technology, and whose availability depends on network and information systems.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

With regard to personal data, the principle of integrity and confidentiality (Art. 5 (1) (f) GDPR) requires organisations to ensure appropriate security of the data and implement technical and/or organisational measures including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (also in relation to Arts 24, 25 and 32 GDPR).

According to Secs 17 and 21 NISG, operators of essential services and digital service providers shall take appropriate and proportionate TOMs to manage the risks posed to the security of network and information systems that they use in their operations.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

In the case of a personal data breach, the notification requirements of Art. 33 (1) GDPR apply. The notification must be made to the Austrian Data Protection Authority ("**DSB**"). The nature and scope of information that must be provided is stipulated by Art. 33 (3) GDPR. The DSB provides a German/English bilingual template on its website, to provide some guidance on the information required under the GDPR: https://www.dsb.gv.at. The reported data breaches are not published.

According to Secs 19 and 21 (2) NISG, operators of essential services and digital service providers shall notify any incident to the computer security incident response team (and in case no such team is established, to GovCERT). The notice must contain all relevant information on the incident and the technical framework conditions that are known at the time of the initial report, in particular the suspected or actual cause, the technology involved and the type of facility or system involved (Sec. 19 (3) NISG).

Operators of public communications networks or services must notify to the RTR-GmbH (the regulatory authority for telecommunications in Austria) any security breaches or losses of integrity where the incident has a significant impact on the operation of networks or services (Sec. 16a (5) Telecommunications Act "**TKG**"). The RTR-GmbH provides a template on its website to provide some guidance (only available in German): https://www.rtr.at. In case the incident involves a breach of the security of personal data, the provider of public communications services shall, without delay, notify the personal data breach to the DSB (Sec. 95a TKG).

Sec. 286 para. 1 ACC stipulates that anyone who intentionally fails to prevent an imminent or already in-progress intentional criminal act or, in cases where notification makes prevention

possible, does not notify the authority or the person threatened, shall be punished by imprisonment of up to two years, if the offence to prevent has at least been attempted and is punishable by imprisonment exceeding one year. Nonetheless, the punishment may not be more severe in nature than the law threatens for the act not prevented.

According to Sec. 286 para. 2 ACC, however, the offender shall not be punished if he:

(i) could not easily prevent or notify the act without exposing himself or a relative to a risk of considerable harm;
(ii) has become aware of the offence subject to punishment exclusively by means of a communication entrusted to him in his capacity as a pastor; or
(iii) would violate another legally recognised duty of confidentiality by the prevention or notification and would have weighed the consequences threatening from the violation of this duty more heavily than the adverse consequences from the omission of the prevention or notification.

Sec. 286 ACC is thus very complex, but ultimately states a general legal duty to prevent specific (cyber-)crimes under certain conditions, for example by notifying the authorities (i.e. the criminal police, the public prosecutor or the Cybercrime-Competence-Center at the Federal Criminal Police Office).

The nature and scope of information to be reported is not defined by the law, but we understand that the notification shall contain all information available and necessary to enable the authorities to prevent the respective crime and to protect the potential victim. However, if such information could harm the organisation if it were to be disclosed, an in-depth assessment to establish exceptions from the notification duty under Sec. 286 para. 2 ACC is recommended.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

A personal data breach must be notified to the data subject when it is likely to result in a *high risk* to the rights and freedoms of the data subject (Art. 34 GDPR). The nature and scope of information that must be provided is stipulated by Art. 34 (2) GDPR. The overall approach is to provide the data subject with information on the nature of the personal data breach as well as recommendations for the person affected as to how to mitigate potential adverse effects. Such communication has to be made in a timely manner, as soon as reasonably feasible.

From a criminal law perspective, such a notification obligation could arise from Sec. 286 para. 1 ACC (notification of the authorities or the affected person to prevent certain crimes). We thus refer to our answers under question 2.4 above.

Similar to the GDPR obligations, providers of public communications services must notify the affected individuals in cases where a breach is likely to adversely affect their privacy or personal data (Sec. 95a TKG). The content of the notification must comply with Art. 3 of the EU Regulation 611/2013, which, *inter alia*, requires the description of the nature and content of the personal data concerned, the circumstances and the likely consequences of the breach. A notification to the individuals affected can only be omitted if the operator demonstrates to the satisfaction of the DSB that it has implemented appropriate technological protection measures in accordance with Regulation (EU) 611/2013.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

In Austria, the supervisory authority, according to Art. 55 GDPR, is the DSB. With regard to the NISG, the competent authority is the Federal Ministry of the Interior.

The RTR-GmbH is the regulatory authority for telecommunications in Austria.

From a criminal law perspective, in particular the criminal police and the public prosecutors' offices are competent to prevent and prosecute Incidents. Further, there exists the so-called "Cybercrime-Competence-Center", which is established at the Federal Criminal Police Office and offers a reporting line for cyber-crimes (against-cybercrime@bmi.gv.at).

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Violations of the GDPR may lead to an administrative fine of up to EUR 20 million or up to 4% of the total worldwide annual turnover, whichever is higher (Art. 83 GDPR).

Violations of the NISG may lead to an administrative fine of up to EUR 50,000, or up to EUR 100,000 in case of repeat offences (Sec. 26 NISG).

Violations of the TKG may lead to an administrative fine of up to EUR 58,000.

A violation of Sec. 286 ACC shall be punished by imprisonment of up to two years; however, the punishment may not be more severe in nature than the law provides for the crime not prevented. Further, civil law claims of the victim against the perpetrator are also possible in case of a violation of Sec. 286 ACC (e.g. tort claims).

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The primary means of enforcement are the fines mentioned in question 2.7 above.

The DSB has the corrective powers stipulated by Art. 58 (2) GDPR, e.g. to issue warnings, orders, impose a temporary or definitive limitation including a ban on processing, etc.

There is currently no relevant case law on Sec. 286 ACC and Incidents.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Austrian law does not explicitly regulate the use of beacons. However, beacons could, *inter alia*, conflict with applicable data protection laws if they collect personal data (such as IP addresses). The justification of the use of beacons should thus be assessed on a case-by-case basis, and from a criminal law perspective.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Austrian law does not regulate the use of honeypots. However, if honeypots are used to counteract an actual cyber-attack, we believe that their usage could be justified from a criminal law perspective and subject to an individual assessment.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Austrian law does not regulate the use of sinkholes. However, if sinkholes are used to counteract an actual cyber-attack and do not harm third parties, their usage could, subject to an individual assessment, be justified.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

In general, according to the secrecy of communication (Sec. 93 (3) TKG), eavesdropping, recording, intercepting or other monitoring of messages and the associated traffic and location data as well as the disclosure such information by persons other than a user without the consent of all users involved is not permitted.

Furthermore, all processing of personal data must comply with the GDPR. Control measures and technical systems to control employees as well as systems that automatically process employees' personal data may also require consent by the works council (Secs 96 and 97 ArbVG).

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Austrian law does not specifically regulate the import or export of such technology. However, if such technology is to be regarded as military- or weapons-related, restrictions could arise from both Austrian and EU law. We thus recommend legal assessment on a case-by-case basis.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Under the GDPR, every data controller (and also every processor) is obliged to guarantee a level of data security that is appropriate to the risk. Such a level of "adequate" data protection must be assessed on a case-by-case basis. The requirements with respect to the TOMs depend, *inter alia*, on the state of the art, the cost of implementation and the nature, scope, context and purposes of data processing as well as the risks involved. Thus, the required TOMs differ significantly depending on the business sector, the specific activities, the categories of data processed, the size of the company, etc.

The authors are not aware of any market practice deviating from the legal requirements.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Specific rules exist that aim to mitigate potential risks in sectors where Incidents may endanger society as a whole and/or constitute a grave invasion of the privacy of individuals. These sectors include, *inter alia*, operators of essential services and digital service providers (NISG), telecommunication service providers (TKG), healthcare service providers (the Health Telematics Law or "**GTelG**"), financial and payment service providers (e.g. the Payment Services Act or "**ZadiG**") and energy/gas providers (the Electricity Industry and Organisation Act or "**ElWOG**"; the Gas Act or "**GWG**").

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Austrian company law (e.g. Sec. 84 of the Austrian Stock Corporation Act) requires the management to act with due diligence and in the best interest of the company. From this general duty of care, it may also follow that directors need to prevent, mitigate, manage and respond to Incidents in order to avoid or at least reduce damages of the company. Therefore, if the directors violate their duty of care relating to Incidents, civil liability of the directors is possible. However, the actual requirements and conditions of such a liability highly depend on the circumstances of the case (e.g. the size and sector of the company and the actual possibility of the directors to take adequate actions), which is why we recommend a case-by-case assessment. In that context, Sec. 286 ACC should also be taken into consideration (*cf.* question 2.4 above).

In general, according to the Austrian Act on Administrative Criminal Law ("**VStG**"), a legal representative of a company (e.g. a managing board member) is responsible under penal law for the legal compliance of the company (Sec. 9 VStG). Thus, administrative fines will be preliminarily imposed on the legal representative of a company. This, however, requires that the legal representative acted culpably, e.g. by neglecting duties of control and supervision. In recent years (and due to the rather high possible fines deriving from EU regulations), exceptions to this rule have been stipulated in national administrative provisions. Such an exception is in place, e.g., with regard to fines under the GDPR. According to Sec. 30 (2) ADPA, administrative fines are primarily imposed on *a legal entity* (and only in exceptional cases on individuals) if infringements of provisions of the GDPR were committed by persons who acted on behalf of the legal entity.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There are no explicit legal obligations to designate a CISO, to

establish an Incident response plan or policy, to conduct periodic cyber risk assessments or to perform penetration tests/vulnerability assessments. However, depending on the specific case (in particular the size of the company, the scope of processing activities and the risks involved), such measures may be required to be implemented as state-of-the-art TOMs. Also, the designation of CISOs is common in most bigger companies, depending on the common practice within the specific industry.

Besides, the GDPR requires the designation of a Data Protection Officer ("**DPO**") in some specific cases; accordingly, a DPO has to be designated if: (i) the controller is a public authority/body; (ii) the core activity of the controller requires large-scale, regular and systematic monitoring of individuals; or (iii) the core activity of the controller consist of large-scale processing of special categories of data (e.g. health data) or data relating to criminal convictions and offences. Kindly note that there are no further obligations to designate a DPO under Austrian national law.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no specific statutory provisions in this regard. However, disclosure obligations could arise in special situations or industries (e.g. capital markets and *ad hoc* reports). We thus recommend an individual assessment in this regard.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

A company may face tort claims from persons who suffered damages by the company's failure to act with due care. Nonetheless, victims would generally need to prove, *inter alia*, the damage and a breach of legal duties by the company, or, respectively, its management.

However, please note that anyone can file a criminal complaint (even anonymously) against a suspected company or person (e.g. the director of a company) and induce the criminal authorities thereby to investigate possible criminal conduct. It is also possible for victims to participate in a criminal proceeding as a "private party" to enforce their civil claims in the criminal proceeding.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There are currently no such examples publicly available.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes. Civil law liability in tort may result if damage occurred due to a breach of legal duties. As mentioned under question 5.1 above, the legal duty to prevent Incidents may arise from general company law but also from Sec. 286 ACC (*cf.* question 2.4 above), which could then be a legal basis for tort claims of victims.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, companies are permitted to do so.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The investigatory powers differ between the various authorities and depend on the respective laws they act on (e.g. criminal police, public prosecutor, data protection authority). However, in general, authorities have a wide scope to investigate Incidents and can under certain conditions, *inter alia*, perform house searches, request information from witnesses or seize IT hardware.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There is currently no specific obligation to implement backdoors. However, it is recognised that witnesses have to disclose encryption keys, passwords and generally answer questions from law enforcement authorities under their obligation to testify completely and correctly. Further, *everyone* must grant access to information to be seized and stored on data carriers under certain conditions stipulated in the Austrian Criminal Procedure Code, which may thus also include the provision of encryption keys to the criminal authorities.

Christoph Haid is co-head of our crisis management & internal investigations practice. Christoph helps clients respond to crisis situations and conducts investigations for corporates and financial institutions, covering all relevant compliance aspects.

Schönherr Rechtsanwälte GmbH
Schottenring 19
1010 Vienna
Austria

Tel: +43 1 534 375 0119
Email: c.haid@schoenherr.eu
URL: www.schoenherr.eu

Veronika Wolfbauer has been with Schoenherr's regulatory practice group since 2013, became an attorney at law in 2016 and counsel in February 2019. Prior to joining Schoenherr, Veronika gained experience at well-known national law firms in Vienna and worked as legal counsel at a gas trading hub.
Veronika is a leading member in the firm's privacy and data protection team. In addition, she leads the technology regulation and audiovisual media law team. Veronika serves not only national but also international corporate clients, and lectures in those areas. She has vast experience in giving strategic and legal advice, as well as leading administrative law proceedings before the DP regulator and "appeal proceedings", including addressing the Austrian Highest Administrative Court, the Austrian Constitutional Court and the European Court of Justice.

Schönherr Rechtsanwälte GmbH
Schottenring 19
1010 Vienna
Austria

Tel: +43 1 534 375 0791
Email: v.wolfbauer@schoenherr.eu
URL: www.schoenherr.eu

Michael Lindtner has been an associate in Schoenherr's Vienna office since 2016 and his main area of practice is criminal compliance and white-collar crime, with a focus on anti-corruption law. Michael graduated from Vienna University of Economics and Business (Bachelor of Laws, 2012; Master of Laws, 2014; Doctorate, 2019). Before joining Schoenherr, he worked as an associate at a well-known national law firm in Vienna, completed the judicial clerk in Vienna and gained experience as a legal intern in well-known national law firms and as a consultant in an international tax consultancy firm.

Schönherr Rechtsanwälte GmbH
Schottenring 19
1010 Vienna
Austria

Tel: +43 1 534 375 0260
Email: m.lindtner@schoenherr.eu
URL: www.schoenherr.eu

Schoenherr is a leading full-service law firm in Central and Eastern Europe. Operating in a rapidly evolving environment, we are a dynamic and innovative firm with an effective blend of experienced lawyers and young talent. As one of the first international law firms to move into CEE/SEE, we have grown to be one of the largest firms in the region. Our comprehensive coverage of the region means we can offer solutions that perfectly fit the given industry, jurisdiction and company.

www.schoenherr.eu

schönherr

Belgium

Roeland Lembrechts

Bart Van den Brande

Sirius Legal

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking, as an unauthorised access to an IT system, is criminalised under article 550*bis* of the Belgian Criminal Code (BCC).

The first distinction that has to be made is between the basic crime (external and internal) and the subsequent actions.

External hacking happens when a person not possessing any access rights knowingly intrudes in or maintains access to an IT system. The penalties are between six months and two years of imprisonment and/or a fine of between 208 EUR and 200,000 EUR. In cases where fraudulent purpose is found, the maximum imprisonment is increased to three years.

Internal hacking happens when a person, who has access rights, exceeds those rights with a fraudulent purpose or with the intention to cause damage. The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 200,000 EUR.

Subsequent actions are aggravating circumstances with increased penalties: imprisonment between one and five years; and/or a fine between 208 EUR and 400,000 EUR. Subsequent actions can include stealing data, damaging an IT system or taking over an IT system to hack another system.

Instructing or commissioning a third party to commit hacking is punishable with between six months and five years of imprisonment and/or a fine of between 800 EUR and 1,600,000 EUR.

Knowingly disseminating or using data obtained as a result of hacking is punishable with imprisonment of between six months and three years and/or a fine of between 208 EUR and 800,000 EUR.

Denial-of-service attacks
Denial-of-service attacks are criminalised as computer sabotage, i.e. "knowingly and without authorisation, directly or indirectly introducing, altering or deleting data in an IT system, or changing by any other technological means the normal use of any data in an IT system" (article 550*ter*, §1 BCC).

The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 200,000 EUR. If real damage is caused to the IT system, the maximum imprisonment is increased to five years and the maximum fine to 600,000 EUR.

In cases with fraudulent purpose or intention of causing harm, the penalties are increased to a maximum of five years' imprisonment. The same increase applies to attacks against critical infrastructures.

Causing a disruption of the correct working of an IT system is an aggravating circumstance: penalties are increased to between one and five years' imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

Phishing
This is, in most cases, punishable by article 504*quater* BCC, i.e. "with fraudulent purpose, acquiring an unlawful economic advantage for himself or for someone else, by introducing, modifying, deleting data that is stored, processed or transferred in an IT system, by means of an IT system or changing the normal use of data in an IT system by any other technological means".

The penalties are between six months and five years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR. An attempt is punishable by six months to three years of imprisonment and/or a fine of between 208 EUR and 400,000 EUR.

Phishing may also be punishable under article 145, §3, 1° of the Electronic Communications Act (ECA) of 13 June 2005, prohibiting the fraudulent initiation of electronic communications, by means of an electronic communications network, with the intent to obtain an illegitimate economic advantage (for oneself or for another). This criminal offence is punishable with between one and four years of imprisonment and/or a fine of between 4,000 EUR and 400,000 EUR.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
This is an act of computer sabotage (article 550*ter*, §1 BCC).

The same criminal penalties apply as those applicable to denial-of-service attacks.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Article 550*bis* §5 BCC provides a specific provision to penalise anyone who unlawfully imports, distributes, carries out or makes available in any way, any tool, including computer data, primarily designed or modified to enable hacking.

The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

Possession or use of hardware, software or other tools used to commit cybercrime
It is a criminal offence on its own to illegitimately possess, produce, sell, procure for use, import, distribute, disseminate or otherwise make available any instrument, including computer data, designed or adapted to enable hacking (article 550*bis*, §5 BCC) or computer sabotage (article 550*ter*, §4 BCC).

The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

When this offence intercepts communication that is not publicly accessible, the penalties are between six months and two years of imprisonment and/or a fine of between 1,600 EUR and 80,000 EUR (article 314*bis*, §2*bis* BCC). If committed by a public officer, the penalties are between six months and three years of imprisonment and/or a fine of between 4,000 EUR and 160,000 EUR (article 259*bis*, §2*bis* BCC).

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft is often a precursor to another criminal offence, e.g. theft, fraud, computer fraud, hacking or computer sabotage committed by using the stolen identity.

Identity fraud may directly be a criminal offence only if the fraud relates to the appropriation of the capacity of a civil servant or military functions, nobility titles, the title of attorney-at-law or the public use of a false family name (articles 227–231 BCC). Penalties are usually limited to fines (up to 8,000 EUR).

Additionally, identity theft or fraud can be qualified as an illegitimate process of personal data. Depending on the specific qualification, these offences are punished by the Belgian GDPR Act of 30 July 2018 with a fine of between 2,000 EUR and 120,000 EUR (article 222), 800 EUR to 160,000 EUR (article 227) or 4,000 EUR to 240,000 EUR (article 223).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

There is no general qualification for electronic theft. Although there has been discussion, case law ruled that, e.g., theft of computer data can be punished under the general definition of theft (article 431 BCC).

As a subsequent action to theft, according to articles XI.304 and XV.105 of the Belgian Economic Law Code, knowingly putting an unlawful copy of a computer program on the market or having it for commercial purposes, or putting on the market or having resources for commercial purposes that are exclusively intended for the unauthorised person to facilitate the removal or circumvention of technical provisions to protect a computer program, is punishable with imprisonment of between one and five years.

Other intellectual properties are secured by articles XV.103–XV.106 of the Belgian Economic Law Code with imprisonment between one and five years and/or a fine between of 4,000 EUR and 800,000 EUR in cases of infringement (piracy and counterfeit) with fraudulent and malicious purpose.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Unsolicited penetration testing is punished in the same way as hacking. It is sufficient that the hacker knows that he is not entitled to enter the IT system. The fact that there would be no damage or malicious intent is in principle irrelevant for criminalisation. Even the hacking attempt will be punished with the same penalties as a completed hacking.

Even with solicited penetration testing, the "white hat hacker" must be careful. The very broad moral element in the use and possession of hacker tools (article 550*bis*, §5 BCC) constitutes a criminal offence, even when they are used with the permission of the owner of the hacked IT system.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Article 210*bis* BCC punishes the committing of falsehood, i.e. "by entering data that are stored, processed or transferred through an IT system, into an IT system, to change, to delete or to change the possible use of data in an IT system with any other technological means, which changes the legal scope of such data".

The penalties are between six months and five years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Usually, there is no extraterritorial application of Belgian laws.

Article 3 BCC provides that the criminal courts shall be competent for all crimes in Belgian territory. To localise a criminal offence, Belgium applies the ubiquity doctrine, which provides that a criminal offence is situated in all places where there is a constitutive element to the offence.

This theory is supplemented with the principle of indivisibility, which allows courts to take into consideration all elements that are indivisibly connected with a criminal offence located in Belgium and to declare themselves competent with regard to a co-perpetrator located in a foreign country.

In the context of specific criminal offences, the Belgian criminal law provisions apply extraterritorially, e.g. in case of terrorism. The General Data Protection Regulation (GDPR) applies extraterritorially considering the criteria in its article 3.2.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

A court may consider mitigating circumstances, such as the behaviour of the perpetrator, in determining the criminal sanctions or giving suspension/postponement of punishment. A pro-active notification or a declaration or plea of guilt may induce a court to impose lower penalties. An amicable settlement with the Public Prosecutor can also be possible.

Article 550*bis* §1 has no reason not to criminalise ethical hacking. It is sufficient that the hacker knows that he is not entitled to enter the IT system. The fact that there would be no damage or malicious intent is in principle irrelevant for criminalisation. Even the hacking attempt will be punished with the same penalties as a completed hacking.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity

- The Act of 1 July 2011 on the security and protection of critical infrastructures.
- Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

- The Act of 7 April 2019 establishing a framework for the security of network and information systems of general interest for public security.
- The Royal Decree of 12 July 2019, implementing the law of 7 April 2019, establishing a framework for the security of network and information systems of general interest for public security and the law of 1 July 2011 on the security and protection of critical infrastructures.
- Regulation (EU) 2019/881 of 17 April 2019 on the European Union Agency for Cybersecurity (ENISA), information and communications technology, cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act).
- Commission Implementing Regulation (EU) 2018/151 of 30 January 2018, laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems, and of the parameters for determining whether an Incident has a substantial impact.

Cybercrime
- The BCC, as amended by the Act of 28 November 2000 on cybercrime, and the Act of 15 May 2006 on cybercrime.
- The Belgian Code of Criminal Proceedings.
- The ECA.

Data protection
- Article 22 of the Belgian Constitution.
- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and the free movement of such data, and repealing Directive 95/46/EC (GDPR).
- The Act of 3 December 2017 establishing the Data Protection Authority (DPA).
- The Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.
- The Act of 5 September 2018 setting up the information security committee and amending various laws on the implementation of the GDPR and repealing Directive 95/46/EC.

Electronic communications, security of electronic communications and secrecy of electronic communications
- Article 22 of the Belgian Constitution.
- Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications.
- The ECA.
- Articles 259*bis* and 314*bis* BCC.
- Coming soon: Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

Trust services and electronic signatures
- Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, and repealing Directive 1999/93/EC (eIDAS Regulation).
- Title 2 of Book XII of the Belgian Code of Economic Law.
- The Act of 18 July 2017 on electronic identification.
- The Act of 20 September 2018 on the harmonisation of the concepts of electronic signature and durable data carrier and the elimination of obstacles to the conclusion of contracts by electronic means.
- The Royal Decree of 25 September 2018 on the harmonisation of the concepts of electronic signature and durable data carrier.

Intellectual property rights
- Book XI of the Belgian Code of Economic Law.

Employee surveillance and BYOD
- Article 22 of the Belgian Constitution.
- The GDPR.
- The Electronic Communications Act.
- Articles 259*bis* and 314*bis* BCC.
- Collective Bargaining Agreement (CBA) No. 68 on employee camera surveillance.
- CBA No. 81 on the protection of employees in relation to the surveillance of electronic online communication data.

Professional secrecy
- Article 458 BCC.
- The Act of 30 July 2018 on the protection of trade secrets.

Due diligence and due care
- Articles 1382 and 1383 of the Belgian Civil Code.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Critical infrastructures are governed by the Critical Infrastructures Act (CIA). The scope of this Act is larger than that of Directive 2008/114/EC, which it implements into Belgian law. The CIA not only covers the energy and transportation sectors, but also the financial and electronic communications sectors.

There are no specific cybersecurity provisions in the CIA. It applies to all risks that may disrupt or destroy critical infrastructures, including cyber risks. Critical infrastructures must establish and execute a security plan, which may include cybersecurity measures.

The Belgian Cyber Security Act of 7 April 2019 (CSA) implements the NIS-Directive, applicable for operators of essential services and digital service providers. This Act provides a wide range of powers and means for the implementation, monitoring and sanctioning of obligations under the NIS-Directive, e.g. security plans, annual internal audits, triennial external audits and administrative and criminal sanctions.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Operators of essential services must take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems that they use in their operations, e.g. security plan, annual internal audit, triennial external audit, etc. (articles 20–23 CSA).

Digital service providers must identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of their network and information systems. They shall take into account the following

elements: (a) the security of systems and facilities; (b) Incident handling; (c) business continuity management; (d) monitoring, auditing and testing; and (e) compliance with international standards (articles 33–34 CSA).

Critical infrastructures must establish and implement a security plan (BPE) (article 13 CIA). This obligation implicitly includes Incident prevention and handling.

Providers of electronic communications services or electronic communications networks must implement adequate measures to manage the security risks in relation to their services or networks, including measures to mitigate the impact of security Incidents in relation to the end-users and other connected networks (article 114, §1 ECA).

Taking into account the state of the art, the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR).

Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide (article 19 eIDAS Regulation).

The general principles of due diligence and due care will, in all likelihood, induce organisations to implement measures to prevent and handle Incidents in order to avoid or limit claims for damages. It does not, however, explicitly impose Incident prevention and handling.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Operators of essential services report immediately all Incidents that have a significant impact on the availability, confidentiality, integrity or authenticity of the network and information systems on which the essential service or services it provides depend on. This notification is simultaneously made to the national computer security incident response team (CSIRT), the sectoral government, or its sectoral CSIRT, and the Directorate General Crisis Centre of the Ministry of Interior Affairs.

The notification is required even if the operator only has partial access to the relevant information to determine whether the Incident has a significant impact (articles 24–25 CSA).

Digital service providers have the same duty for the services offered by them in the European Union. The notification is made in accordance with the implementing Regulation 2018/151 of 30 January 2018 on a secured platform (articles 35–36 CSA).

The controller under the GDPR shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Belgian DPA, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification must include the following information:

- the nature of the personal data breach;
- contact details of the data protection officer (DPO) or other contact point;
- the likely consequences of the personal data breach; and
- the measures taken or proposed to be taken.

Providers of electronic communications services/networks are subject to a binding personal data breach notification with the Belgian DPA and, if impacted, the end-user, unless the provider has implemented mitigation measures (article 114/1, §3 ECA). They also have to notify the Belgian Institute for Post and Telecommunications and the end-users about special security risks (article 114/1, §1 ECA). Security Incidents also have to be notified to the Belgian Institute for Post and Telecommunications (article 114/1, §2 ECA).

Trust service providers must notify the Belgian Ministry of Economic Affairs or the DPA about any breach of security or loss of integrity that has a significant impact on the trust service (article 19 eIDAS Regulation).

Critical infrastructures must notify any Incident that imperils the security of the critical infrastructure to the Communication and Information Centre (article 14, §1 CIA).

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Article 34 GDPR: When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate this breach to the data subject without undue delay. The information provided must, at least, include contact details of the DPO, likely consequences and measures taken or to be taken.

Article 114/1, §1 ECA: If there is a particular risk of network security breaches, the undertakings providing a publicly available electronic communications service shall inform subscribers and the Institute. If the risk requires measures other than those that can be taken by the undertakings providing the service, they shall indicate any means of combatting that risk, including an indication of the expected costs.

Article 19 eIDAS Regulation: When it is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall notify the natural or legal person of the breach of security or loss of integrity without undue delay.

The nature and scope of information is different for each notification duty.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The following regulators are responsible for enforcement (excluding criminal actions):

- Data protection: the Belgian DPA.
- Electronic communications: the Belgian Institute for Post and Telecommunications.
- Trust services: the Ministry of Economic Affairs.
- Critical infrastructures: the Ministry of Interior Affairs.
- Operators of essential services and digital service providers: Centre for Cybersecurity Belgium (CCB), the Ministry of Economic Affairs and sectoral governments.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

The following penalties apply:

- Data protection: criminal penalties (indirectly to subsequent failures under article 226 Belgian GDPR Act) and administrative penalties (article 83, §4 GDPR).
- Electronic communications: criminal penalties (articles 114 and 145 ECA).
- Critical infrastructures: criminal penalties (article 26 CIA).
- Operators of essential services and digital service providers: criminal and administrative penalties (articles 51 and 52 Belgian CSA).

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

No specific information on enforcement is yet available. The focus is currently mainly on prevention and awareness with various government initiatives to increase maturity around cyber security. The DPA took its first series of decisions in 2020, including one decision with regard to taking adequate technical and organisational measures (decision 22/2020 of 8 May 2020). The authority ruled that there was no infringement as a Master IT Service Agreement had been concluded with the processor with the necessary provisions under the GDPR, the necessary internal risk assessment methods had been used, the effectiveness of the elaborated procedures had been evaluated by annual internal and external audits and the company had acted in a transparent manner when reporting to the authority.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
This is not explicitly forbidden. It is only when the IP address is considered to be personal data under the GDPR that the processing has to be compliant with the GDPR. An informed consent can be required in that case. Beacons, fingerprints and cookies also require informed consent under the ECA if they are not merely functional and/or collect personal data.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
This is not explicitly forbidden.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
This is not explicitly forbidden.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Organisations have a limited ability to intercept electronic communications, but in practice this is virtually impossible without committing a criminal act. Article 314*bis* BCC prohibits the deliberate interception, access or recording of communications in which one does not participate and without the consent of all participants. Article 124 of the ECA of prohibits the deliberate knowledge of the existence of that communication, the identification of persons and the processing of the electronic communications that was obtained (deliberately or not) without the consent of all participants. Exceptions are provided for this last article, for example CBA No. 81, which provides for such an exception when necessary to prevent the organisation's computers from being hacked. However, the correct application is a subject of discussion in case law and legal doctrine.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

No, there is no explicit prohibition, except for the use of hacker tools, which is punishable by article 550*bis* §5 BCC.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice in relation to Incident handling varies greatly depending on the sector and nature of the activities.

Typically, the financial sector has implemented strict information security measures.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

The telecommunications sector is subject to specific obligations under the ECA (article 114/1).

Although these are technically not legal requirements, the financial services sector is subject to specific cybersecurity obligations in the context of the prudential supervision by the National Bank of Belgium.

In addition to this, the financial services sector and the telecommunications sector, together with the sectors of energy, transport, finance, healthcare, water and digital infrastructure, are governed by the CIA, which imposes security obligations.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

A director and/or officer may be held liable for a breach of his duties as a director if he fails to act with due care and due diligence.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) There is no specific obligation to designate a chief information security officer (CISO) as such. Under the GDPR, it can be required to designate a DPO (article 37). Operators of essential services and digital service providers are obliged to designate a contact point for the security of network and information systems (articles 23 and 34 CSA). The same obligation applies to critical infrastructures (articles 12 and 13 CIA).

(b) A written response plan or policy is required under articles 20 and 21 (operators of essential services) and article 33, §1, b) (digital service providers) CSA.
Article 13 CIA requires that the operator is responsible for organising exercises and for updating the security plan.
It may be required under the GDPR, depending on the company's individual context. This is the case under article 35, §7, d) GDPR when a data protection impact assessment is needed and may also be required as a general but implicit security measure under article 32 GDPR.

(c) CSA explicitly requires an annual internal audit and a triennial external audit for operators of essential services (article 38, §1 and 2). Article 13, §6 CIA: The operator is responsible for organising exercises and for updating the BPE, based on the lessons learned from the exercises or from any change to the risk analysis. It may be required under the GDPR, depending on the company's individual context.

(d) *Idem* as (c).

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no other specific disclosure requirements for companies in relation to cybersecurity risks or Incidents. If cybersecurity risks or Incidents have a major financial impact, there is a disclosure requirement in relation to the financial impact (e.g. in the annual report). If they have an impact on personal data, there is a disclosure obligation to the DPA.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In the case of negligence, any person suffering damage may file an action to obtain compensation. That person is required to adduce evidence of the existence of negligence (which may be adduced by evidencing a breach of Applicable Laws), the damages suffered and the causal link between the negligence and the damage.

If the Incident is the result of an unfair market practice or a breach of data protection law, cease-and-desist proceedings are possible.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

Although there have been several Incidents, there have recently been no noteworthy cases in relation to Incidents.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes, see question 6.1.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber insurance is permitted and even encouraged in Belgium.

The number of Incidents has even led to a greater general awareness and demand for insurance against Incidents.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are generally no legal or regulatory limitations in relation to insurance coverage, except the possibility for insurance against criminal penalties. Administrative fines may, however, be covered by insurance.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement authorities have a variety of investigatory powers at their disposal, including:

- conducting (international) network searches;
- the right to copy, block or seize electronic data;
- intercepting, localising and accessing electronic communications;
- imposing technical cooperation from persons with knowledge about the relevant IT systems; and
- under very specific circumstances, hacking and computer sabotage, as well as decryption.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Organisations are not required to implement backdoors. However, law enforcement authorities may require any person with the relevant knowledge to provide them with encryption keys.

Roeland Lembrechts is a Master of Criminology (2005) and Master of Laws (2009). He started his career in 2009 at the Bar of Mechelen with a broad focus on criminal, civil and corporate law, and specialised in contractual and non-contractual liabilities.
In addition, Roeland was active as a board member of the department of contract law at the Bar of Antwerp (2018–2019) and is the secretary of the professional journal *Today's Lawyer*, a magazine that centres on the lawyer as an ethical and innovative entrepreneur with a focus on digitising the profession.
Roeland has a special interest in contract and liability law within the digital single market. He has been a certified DPO since 2017.

Sirius Legal
Veemarkt 70
2800 Mechelen
Belgium

Tel: +32 15 490 221
Email: roeland@siriuslegal.be
URL: www.siriuslegal.be

Bart Van den Brande has been a member of the Dutch-speaking Brussels Bar Association since 2001.
Bart has worked at several well-known Brussels law firms and has built extensive expertise in media and advertisement law, market practices and consumer protection, intellectual property, internet and e-commerce, privacy and data protection, IT, software development and gambling law.
Parallel to his law practice, Bart was a part-time teaching assistant at Brussels University VUB between 2005 and 2013. He is the author of several articles, is an experienced speaker at seminars and for training courses and is regularly asked to comment on current legal events in the national media. Several court cases handled by Bart were later published.

Sirius Legal
Veemarkt 70
2800 Mechelen
Belgium

Tel: +32 15 490 221
Email: bart@siriuslegal.be
URL: www.siriuslegal.be

Canada


Lyndsay A. Wasser


Kristen Pennington

McMillan LLP

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Wilful interception of private communications is a criminal offence under Section 184 of the *Criminal Code of Canada*, RSC 1985, c C-46 (the "**Code**"), with a maximum sentence of five years' imprisonment.

Section 342.1 of the Code prohibits fraudulently obtaining any computer service or intercepting any function of a computer system. Use of a computer system with intent to commit such an offence and use or possession of a computer password to enable such an offence are also prohibited. The maximum sentence is 10 years' imprisonment. The elements of this offence were recently discussed by the Alberta Court of Appeal in *R v. McNish*.

Hacking has also been prosecuted under:

- Section 380(1) of the Code, which prohibits defrauding the public or any person of property, money, valuable security or a service, and carries a maximum penalty of 14 years' imprisonment where the subject matter of the offence exceeds $5,000. In *R v. Kalonji*, the accused was found guilty of fraud and conspiracy to commit fraud in connection with an account take-over scheme involving the hacking of bank accounts.
- Section 430 of the Code, particularly when the hacking is related to "smurfing" (e.g. overloading computer systems causing chaos). In *R v. Geller*, an accused was charged with mischief to data after obtaining credit card numbers and other information through hacking, then accessing the internet using fake identification.

Denial-of-service attacks
Denial-of-service attacks could be considered "mischief" under Section 430(1.1) of the Code, which prohibits obstructing, interrupting or interfering with the lawful use of computer data and denying access to computer data to a person who is entitled to such access. The maximum penalty is 10 years' imprisonment.

Phishing
Phishing may constitute fraud pursuant to Section 380(1) of the Code. In *R v. Usifoh*, the accused was found guilty of receiving funds from various victims of phishing scams.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Section 430 of the Code prohibits "mischief", which includes wilfully destroying or damaging property, rendering property useless, inoperative or ineffective, or obstructing, interrupting or interfering with the lawful use, enjoyment or operation of property. Section 430(1.1) of the Code specifically prohibits wilfully destroying or altering computer data, rendering computer data meaningless, useless or ineffective, obstructing, interrupting or interfering with the lawful use of computer data and denying access to computer data to a person who is entitled to such access. The maximum penalty is 10 years' imprisonment.

Section 8(1) of the *Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23 ("**CASL**") prohibits, during the course of a commercial activity, installing or causing to be installed a computer program on any other person's computer system, unless an owner or authorised user of the computer system consents (subject to certain conditions) or the person is acting in accordance with a court order.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Pursuant to Section 342.2 of the Code, it is illegal to sell or offer for sale a device that is designed or adapted primarily to commit an offence under Section 342.1 (hacking) or Section 430 (mischief).

Possession or use of hardware, software or other tools used to commit cybercrime
Pursuant to Section 342.2 of the Code, it is illegal to make, possess, import, obtain for use, distribute or make available a device that is designed or adapted primarily to commit an offence under Section 342.1 (hacking) or Section 430 (mischief), knowing that the device has been used or is intended to be used to commit such an offence. The maximum penalty is up to two years' imprisonment and/or an order to forfeit the offending device(s).

Identity theft or identity fraud (e.g. in connection with access devices)
Section 402.2 of the Code prohibits obtaining or possessing another person's identity information with the intent to use it to commit an indictable offence such as fraud. The maximum sentence is five years' imprisonment. In *R v. Levesque*, the

accused held multiple forms of identity information, including credit cards and passports. The only reasonable inference the Court could make in the circumstances was that the accused intended to commit fraud or personation.

Fraudulently "personating" another with the intent of gaining an advantage, obtaining property, causing disadvantage to another or to avoid arrest or prosecution is prohibited under Section 403 of the Code. The maximum penalty is 10 years' imprisonment. Personating includes pretending to be the person or using the person's identity information, including their name, signature, username or password. In *R v. Mackie*, the accused was found guilty of personation after gaining access to young peoples' Facebook accounts and pretending to be a victim in order to contact other children.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Pursuant to Section 342.1 of the Code, it is an offence to fraudulently obtain, without colour of right, any computer service, including data processing, and the storage or retrieval of computer data. See, for instance, *R v. St-Martin*, where a police officer fraudulently obtained electronic information regarding multiple individuals using a police database.

Section 41.1(1) of the *Copyright Act*, RSC 1985, c C-42 prohibits circumvention of a "technological protection measure", including any technology, device or component that controls access to a work or sound recording or restricts violations of certain copyright provisions. Circumventing a technological protection measure includes descrambling a scrambled work, decrypting an encrypted work or otherwise avoiding, bypassing, removing, deactivating or impairing the technological protection measure without consent. Some violations of Section 41 can lead to fines of up to $1 million, imprisonment for up to five years or both. In *Nintendo of America Inc. v. King*, the respondent was found to have trafficked in circumvention devices for Nintendo's technological protection measures.

Some Data Protection Statutes (as defined in question 2.1) also allow for the imposition of administrative penalties or fines for improperly collecting, using, disclosing, gaining or attempting to gain access to personal information ("**PI**"). For example, pursuant to Section 107 of the *Health Information Act*, RSA 2000, c H-5 (Alberta), a person who knowingly gains or attempts to gain access to health information in contravention of the Act is guilty of an offence and can be fined up to $50,000. Alberta's private sector privacy legislation, the *Personal Information Protection Act*, SA 2003, c P-6.5, also makes it an offence to collect, use, disclose, gain or attempt to gain access to PI in contravention of the Act, subject to a fine of up to $10,000 for an individual and up to $100,000 for a person other than an individual.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

It is possible that unsolicited penetration testing could be prosecuted under Section 430(1.1) (mischief) and/or Section 342.1 (hacking) of the Code.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Pursuant to Section 83.2 of the Code, an individual who commits an indictable offence for the benefit of, at the direction of, or in association with an organisation that commits a terrorist activity is liable to imprisonment for life. Section 83.01 of the Code defines a "terrorist activity" to include an act or omission that intentionally causes serious interference with or disruption of an essential service, facility or system, whether public or private, other than in non-violent protests.

Section 19 of the *Security of Information Act*, RSC 1985, c O-5, makes it an offence to communicate a trade secret with another person, group or organisation, or to obtain, retain, alter or destroy a trade secret, for the benefit of or in association with a foreign economic entity that undermines Canada's economic interests, international relations, or national defence and security. Defences include independent development or reverse engineering, among others. A guilty party may be ordered to serve up to 10 years in prison.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Section 6(2) of the Code provides that "no person shall be convicted of an offence that takes place outside of Canada" (see also Section 478(1) of the Code). However, pursuant to Sections 7(3.74) and 7(3.75) of the Code, certain terrorism offences and indictable offences that are considered terrorist activities may be deemed to have been committed in Canada, including when the offence is committed by or against a Canadian citizen.

The Supreme Court of Canada has held that, where a "significant portion" of the activities constituting an offence took place in Canada, a Canadian court may assume jurisdiction. A court will consider whether there is a "real and substantial link" between the alleged crime and the jurisdiction seeking to enforce the law (see *R v. Libman*).

Pursuant to Section 26(1) of the *Security of Information Act*, a person is deemed to have committed an offence in Canada, despite the fact the act or omission took place elsewhere, if the person: is a Canadian citizen; is someone who owes allegiance to Her Majesty in right of Canada; performs functions for a Canadian mission; or returns to Canada after the offence was committed.

Certain provisions of CASL may have extraterritorial application. For example, Section 8 (installation of computer program) applies if the computer system is located in Canada at the relevant time, or if the person is either in Canada at the relevant time or is acting under the direction of a person who is in Canada at the time when they give the directions.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Sentencing in Canada is determined on a case-by-case basis, relying on statutory guidance under Section 718 of the Code. The basic principle is that the sentence must "be proportionate to the gravity of the offence and the degree of responsibility of the offender" (Section 718.1 of the Code). Additionally, "the degree of planning involved in carrying out the offence and the duration and complexity of the offence" are also considerations (Section 718.21(b) of the Code).

Certain criminal offences require proof of criminal intent (e.g. *mens rea*). Also, some offences may not apply where the action was undertaken with consent. For a recent discussion of intent as it related to Section 430(1.1) (mischief), Section 342.1 (hacking), and Section 24 (attempts) of the Code, see *R v. Livingston*.

The penalties for some offences depend upon the financial repercussions of the offence. For example, Section 380(1) of the Code (see Section 1.1) carries a maximum sentence of 14 years'

imprisonment for fraud involving $5,000 or more, whereas the maximum sentence is reduced to two years' imprisonment if the value of the subject-matter of the offence is less than $5,000. There are also other aggravating factors, such as the number of victims or the complexity of the fraud, that may increase the severity of the punishment (see Section 380.1(1)).

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

CASL prohibits, in the course of a commercial activity: (a) alteration of the transmission data in an electronic message so that the message is delivered somewhere other than, or in addition to, the destination specified by the sender (Section 7(1)); (b) installation of a computer program on another's computer system without consent (Section 8(1)); and (c) aiding, inducing, procuring or causing any of the above (Section 9). Violations of CASL can result in administrative monetary penalties of up to $1 million per violation by an individual and $10 million per violation by an organisation.

See also question 1.1 for discussion of Section 19 of the *Security Information Act*, which relates to trade secrets.

Canada also has a number of statutes that apply to the protection of PI, including (collectively "**Data Protection Statutes**"):

- the Federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ("**PIPEDA**") applies to the protection of PI handled in the course of commercial activities (except in provinces that have substantially similar legislation), and to the protection of employee PI by federally regulated organisations;
- the Provinces of Alberta, British Columbia and Quebec each have legislation that is substantially similar to PIPEDA, which applies to the protection of PI by private sector organisations within these provinces;
- each Canadian jurisdiction has legislation governing the protection of PI by government bodies/institutions; and
- most provinces have legislation that applies to the protection of personal health information by certain types of custodians, such as doctors and hospitals.

Quebec has proposed significant potential amendments to its privacy laws by tabling Bill 64, *An Act to modernise legislative provisions as regards the protection of personal information* ("**Bill 64**"). Bill 64, if passed, is intended to modernise the province's legislative framework with respect to the protection of PI in both the public and private sectors. Quebec already has in force *An Act to establish a legal framework for information technology*, SQ 2001, c 32, which requires that certain measures be taken to protect confidential information stored in electronic documents and format, and sets out rules governing the use, retention and transmission of electronic data, including biometric information.

As part of the National Cyber Security Strategy, the federal government has released a 10-principle Digital Charter ("**Charter**"), including a "safety and security" principle that represents Canadians' right to rely on the integrity, authenticity and security of the services they use and to feel safe online. Though the Charter does not have the force of law, its principles are intended to guide the government's policy and actions.

Export control laws can also have cybersecurity implications. For example, Canada's Export Control List (the "**ECL**") identifies specific goods and technologies that are controlled for export, including some computer systems, equipment, components and software designed or modified for the generation, command and control or delivery of "intrusion software", as defined in the ECL.

Organisations are also required to comply with any representations they make to the public regarding their handling of PI, including the safeguards taken by the organisation to prevent an Incident. As discussed further at question 2.6, the Competition Bureau can investigate false and misleading statements and representations about consumers' privacy and the handling of their PI.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Communications Security Establishment ("**CSE**") is the technical authority for cybersecurity and information assurance in Canada. Its mandate includes providing advice, guidance and services to ensure the protection of computer networks and electronic information of importance to the Canadian government, including combatting foreign-based cyberattacks on critical infrastructure. The CSE establishes IT security standards, practices and directives for IT security practitioners across the federal government.

Public Safety Canada has issued a document providing a set of recommended security steps for organisations involved in critical infrastructure to implement, in order to combat insider risk of cyberattacks.

The Canadian Centre for Cyber Security has issued alerts notifying health organisations of the increased risk to their cybersecurity in light of the current worldwide pandemic and has provided guidance on key vulnerabilities and mitigation strategies.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Data Protection Statutes require protection of PI. For example, PIPEDA requires that PI be protected against loss or theft, unauthorised access, disclosure, copying, use or modification. The nature of the safeguards should vary depending on the sensitivity, amount, distribution, format and method of storage of the PI, and should include technological measures such as passwords and encryption.

Some of the Data Protection Statutes contain breach reporting, recording and notification obligations in the event of an Incident that impacts PI, as described further at question 2.5.

Certain industry regulators also require organisations to monitor, detect, prevent and/or mitigate Incidents, including:

- The Canadian Securities Administrators ("**CSA**") has issued several Staff Notices relevant to cybersecurity, including without limitation: Staff Notice 11-326 ("Cyber Security"); Staff Notice 11-332 ("Cyber Security"); Staff Notice 33-321 ("Cyber Security and Social Media"); Staff Notice 11-338 ("CSA Market Disruption Coordination Plan"); and Multilateral Staff Notice 51-347. These Staff Notices address matters such as the CSA's expectations for market participants (e.g. that they adopt a cybersecurity

framework that is appropriate to their size and scale) and the measures firms should take to prevent and respond to Incidents (e.g. implementing preventative practices, adequate and current staff training and a written Incident response plan). Firms are expected to conduct a cybersecurity risk assessment at least annually.

- The Office of the Superintendent of Financial Institutions ("**OSFI**") has issued several publications related to cybersecurity, including the "Cyber Security Self-Assessment Guidance" memorandum for Federally Regulated Financial Institutions ("**FRFI**"), which indicates that FRFI senior management is expected to review cyber risk management policies and practices to ensure that they remain appropriate and effective based on evolving circumstances and risks. OSFI has also published a cybersecurity self-assessment template that it encourages organisations to use and may require an organisation to complete. OSFI's "Guideline B-10" sets out expectations for FRFIs regarding the protection of information disclosed to service providers.
- The Investment Industry Regulatory Organization ("**IIROC**") has released a "Cybersecurity Best Practices Guide", which provides dealer members with a voluntary risk-based cybersecurity framework comprising industry standards and best practices. IIROC's "Cyber Incident Management Planning Guide" assists dealer members in preparing internal response plans for Incidents. IIROC has also recently amended its Dealer Member Rules to mandate certain reporting requirements, which are discussed further at question 2.4.
- The Mutual Fund Dealers Association of Canada ("**MFDA**") has released bulletins on cybersecurity describing sources of threats and providing guidance on creating a cybersecurity framework. The MFDA actively engages with members to identify risks in their cybersecurity practices and provide recommendations for improvements, including pursuant to its Cybersecurity Assessment Program.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Some Data Protection Statutes contain breach reporting and recording obligations in the event of an Incident. For example, PIPEDA requires organisations to keep records of any Incident involving loss of unauthorised access to or unauthorised disclosure of PI due to a breach of (or failure to establish) the security safeguards required by PIPEDA. If an Incident gives rise to a real risk of significant harm to any individual(s), the Incident must be reported to the Office of the Privacy Commissioner of Canada ("**OPC**") and the organisation must notify affected individuals and any organisation or government institution that may be able to reduce or mitigate the risk of harm. PIPEDA prescribes the minimum content for reports to the OPC, including (without limitation) a description of the Incident, timing of the Incident, the PI impacted, the number of individuals impacted and the steps taken to mitigate/reduce the risk of harm.

Some of the Data Protection Statutes also contain breach reporting and notification requirements, including private sector legislation in Alberta, public sector legislation in the Northwest Territories and Nunavut, and legislation applicable to personal health information custodians in Ontario and Alberta.

As discussed further at question 5.3, the CSA requires organisations to consider disclosure of cybercrime risks, Incidents and related controls in their prospectus or continuous disclosure filings. In addition, regulated exchanges, marketplaces, clearing agencies and alternative trading systems may be subject to Incident reporting requirements under recognition or exemption orders issued by various CSA jurisdictions, including those set out in Instruments NI 21-101, NI 23-101 and NI 24-102. Many exchanges, marketplaces and clearing agencies are required to promptly notify the CSA of a material systems issue, security breach or system intrusion. The CSA also expects that systematically important clearing agencies and settlement systems will inform the Bank of Canada of a market disruption event.

OSFI's "Technology and Cyber Security Incident Reporting" memorandum requires that an Incident be reported to OSFI when it could materially impact the normal operations of a FRFI (including the confidentiality, integrity or availability of its systems and information) and is assessed to be of a high or critical severity level. The memorandum lists characteristics of reportable Incidents and requires reporting to OSFI (including certain specified information) as soon as possible, but no later than 72 hours after it is determined that the Incident is reportable. FRFIs have an ongoing obligation to provide updates to OSFI as new information becomes available.

IIROC amended its Dealer Member Rules in November 2019 to require mandatory reporting of Incidents where: there has been or there is a reasonable likelihood of substantial harm to any person or a material impact on the Dealer's operations; the Dealer invokes a business continuity or disaster recovery plan; or there is a requirement to notify any government body or regulatory authority. Dealers must file an initial report with IIROC describing the Incident within three calendar days of its discovery. Within 30 days of the Dealer's discovery of an Incident, a more detailed report outlining their findings in the course of their investigation must be submitted.

The MFDA requires that members report any breach of client confidentiality, including as a result of a cyberattack.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Some of the Data Protection Statutes contain notification obligations in the event of an Incident that impacts PI. For example, PIPEDA requires that individuals be notified of any breach of security safeguards involving PI under the organisation's control, as soon as feasible, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

PIPEDA prescribes the content and manner of delivering the notice. The notice must contain sufficient information to allow individuals to understand the significance of the Incident

to them and to take steps to reduce/mitigate the risk of harm, and must contain certain prescribed content, including (without limitation) a description of the Incident, timing of the Incident, the PI impacted and the steps taken by the organisation to mitigate/reduce the risk of harm.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Compliance with PIPEDA is generally enforced by the OPC; however, certain offences can be prosecuted by the Attorney General ("**AG**"). Each province has a regulator responsible for enforcing the relevant provincial Data Protection Statutes.

CASL is enforced by the Canadian Radio-television and Telecommunications Commission ("**CRTC**"), the OPC and the Competition Bureau.

The Competition Bureau also has jurisdiction to investigate false and misleading statements and representations about consumers' privacy and the handling of their PI, including how such PI is maintained, pursuant to its authority under the *Competition Act*, RSC 1985, c C-34.

See, also, the industry-specific regulators described in question 2.3, which oversee compliance with their cybersecurity policies, guidelines and industry-specific Applicable Laws.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

The OPC can make non-binding recommendations in the event of non-compliance with PIPEDA and, following the OPC's decision, an application can be made to the Federal Court for damages to complainants. The AG can prosecute an organisation for failure to comply with the breach reporting, notification and recording obligations under PIPEDA, which can result in fines of up to $10,000 on summary conviction or $100,000 for an indictable offence. Some of the provincial Data Protection Statutes also provide for fines in the event of non-compliance.

Organisations that violate the *Competition Act* by making a false or misleading representation to the public in a material respect, including with respect to consumers' privacy and the handling of their PI, can be subject to penalties of up to $10 million for a first offence, and up to $15 million for subsequent offences.

Criminal offences and failure to comply with CASL carry the penalties as described in questions 1.1 and 2.1.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The OPC has investigated a number of Incidents involving breaches of PI, including:

- PIPEDA Report of Findings #2016-005 – Investigation of Ashley Madison in connection with hacking and online posting of users' account information (resulted in recommendations by the OPC);
- PIPEDA Report of Findings #2019-001 – Investigation into Equifax after an attacker accessed sensitive PI of customers (resulted in a compliance agreement);
- PIPEDA Report of Findings #2018-001 – Investigation into VTech Holdings Limited following the potential compromise of PI respecting over 553,000 Canadians, including children's names, genders, dates of birth, pictures, voice recordings and chat discussions with parents;
- PIPEDA Report of Findings #2007-389 – Investigation into TJX after a network computer intrusion affected payment card information; and
- PIPEDA Report of Findings #2018-006 – Investigation into the World Anti-Doping Agency following a breach of its database, which resulted in the public disclosure of the PI of Olympic athletes.

The CRTC has also taken enforcement action under CASL, including against Datablocks Inc. (fine of $100,000) and Sunlight Media Network Inc. (fine of $150,000) for violations of Sections 8 and 9 of CASL. The CRTC found that advertisements distributed through the companies' services resulted in the unlawful installation of malicious programs on computer systems by third parties, and that neither company took appropriate steps to prevent such CASL breaches, thereby aiding the violations.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Organisations subject to the Data Protection Statutes are generally required to provide notice and/or obtain consent to the collection and use of PI. The OPC considers metadata collected using beacons to be PI and has indicated that organisations should not undertake types of web tracking that individuals cannot stop or control without taking extraordinary measures (or at all), as these forms of tracking do not allow for individuals to consent or withdraw consent, contrary to PIPEDA.

It is possible that beacons used only for data security purposes may fall within the exceptions to notification and/or consent requirements under the applicable Data Protection Statute(s). However, a specific evaluation of Applicable Laws in the relevant jurisdiction(s) should be undertaken.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

The use of honeypots is not expressly prohibited by Applicable Laws. However, to the extent the honeypot involves the collection, use or disclosure of PI, notice and consent considerations may apply. Honeypots may be problematic under CASL, depending upon the manner in which they operate.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

The use of sinkholes is not expressly prohibited by Applicable Laws. However, to the extent the sinkhole involves the collection, use or disclosure of PI, notice and consent considerations may apply. Compliance with CASL should also be considered.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Such monitoring or interception would generally be permissible,

provided it is reasonable and complies with the requirements of any applicable Data Protection Laws, and provided the organisation has a "colour of right" pursuant to Section 342.1 of the Code (hacking). Advance notice/consent in a form prescribed by Data Protection Laws may be required. Monitoring of employees in a unionised workplace raises additional concerns that should be evaluated on a case-by-case basis for compliance with any applicable collective agreement(s). Organisations should consult local counsel in the relevant jurisdiction(s) to ensure full compliance with all Applicable Laws.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Canadian export controls' limitations vary in scope depending on the type of product and its ultimate destination. Canada controls the flow of encryption items out of the country through the *Export and Import Permits Act*, RSC 1985, c E-19, Group 1, Category 5 – Part 2: Information Security. Cryptography falls under the "Dual-Use List", as encryption products can be used for military purposes as well as civil and commercial applications. Exceptions to the export controls may apply for certain countries under a General Export Permit. See, for instance, *General Export Permit No. 45 – Cryptography for the Development or Production of a Product* (SOR/2012-160).

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Many organisations in various industries have recognised that compliance with statutory requirements should not be the end goal for data protection and have voluntarily committed to a higher standard. Examples include, without limitation, the telecommunications and financial services industries, as well as service providers to healthcare institutions and government institutions/bodies. Payment processors in Canada also typically comply with the Payment Card Industry Data Security Standard (PCI-DSS).

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Organisations in the financial services and telecommunications sectors must comply with PIPEDA, including (in many cases) with respect to employee PI. See Section 2 for additional requirements applicable to the financial sector, including pursuant to OSFI's guidance documents.

The Bank of Canada, Department of Finance and OSFI have also collaborated with G-7 partners to publish the following guidelines: (a) G-7 Fundamental Elements of Cybersecurity for the Financial Sector; (b) G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector; and (c) G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector.

The Canadian Security Telecommunications Advisory Committee has developed Security Best Practices for telecommunications service providers that supply and support Canada's telecommunications critical infrastructure. These voluntary practices include ongoing security testing, network security monitoring, Incident response capabilities and developing breach notification procedures.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Directors' and officers' personal liability with respect to Incidents has not been expressly considered by Canadian courts. However, directors and officers can be held liable for breaches of fiduciary duties if they fail to: act honestly and in good faith with a view to the best interests of the company; or exercise the care, diligence and skill of a reasonably prudent person in comparable circumstances. Therefore, failure to take steps to address cybersecurity concerns of which the director or officer was aware (and that a reasonable person would have remedied) could potentially expose them to personal liability. A due diligence defence may apply if the director or officer relied in good faith on statements, documents and reports created by professionals.

There may also be a risk of personal liability if directors and officers misrepresent the organisation's cybersecurity measures, fail to disclose cybersecurity risks or Incidents in annual reporting (if applicable), or are otherwise untruthful or careless about cybersecurity Incidents or risks.

Directors and officers may also be held personally responsible for violations of certain statutes at the federal and provincial level. For example, pursuant to Section 31 of CASL (subject to a defence of due diligence), an officer, director, agent or mandatary of a corporation may be liable if they directed, authorised, assented to, acquiesced in, or participated in the commission of a violation of the Act.

Pursuant to Section 93 of Quebec's *Act respecting the protection of personal information in the private sector*, a director or representative of a corporation is liable as a party to an offence if it is found that the corporation committed an offence and the director ordered or authorised the act or omission constituting the offence. For the first offence, fines range between $1,000 and $10,000 for anyone who collects, holds, communicates to third parties, or uses PI for purposes contravening the Act. Fines increase with repeated offences (see Section 91).

Under some provincial health privacy legislation, a director or officer may be liable as a party to a corporation's offence if they authorised the offence or could have prevented the offence from being committed and knowingly did not do so.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Some federal and provincial privacy statutes require organisations to designate a person responsible for compliance with the applicable legislation. For example, PIPEDA Schedule 1, Principle 4.1 requires designation of one or more individual(s) who are accountable for compliance with the PIPEDA principles, including those set out under Principle 4.7, "Safeguards".

Guidance documents and findings in prior cases published by the OPC and other regulators indicate that all organisations should have a written Incident response plan/policy, and should conduct periodic cyber risk and vulnerability assessments, as well as penetration tests. Failure to do so would typically be considered non-compliant with the organisation's general obligations to protect information under the Applicable Laws.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

As discussed in question 2.4, some institutions are required to disclose cybersecurity risks or Incidents as part of their prospectus or ongoing disclosure obligations. Factors relevant to assessing disclosure obligations include the probability that an Incident will occur and the anticipated magnitude of its effects. The issuer is expected to provide disclosure that is detailed and entity-specific. In addition, regulated exchanges, marketplaces, clearing agencies and alternative trading systems may be subject to Incident reporting requirements under recognition or exemption orders issued by various CSA jurisdictions, including those set out in Instruments NI 21-101, NI 23-101 and NI 24-102.

The CSA's Multilateral Staff Notice 51-347 ("Disclosure of cybersecurity risks and incidents"), a joint publication of the British Columbia Securities Commission, the Ontario Securities Commission and Quebec's Autorité des marchés financiers, provides that issuers must undertake a contextual analysis when determining whether and when an Incident constitutes a material fact or material change that requires disclosure in accordance with securities legislation. Issuers are expected to address in their Incident remediation plans for how an Incident will be assessed to determine whether, what, when and how the Incident will be disclosed.

Some laws of general application and/or specific sectoral or provincial laws have requirements that are relevant to cybersecurity (e.g. Quebec's *An Act to Establish a Legal Framework for Information Technology*). Organisations should consult local counsel in the relevant jurisdiction(s) to ensure full compliance with all Applicable Laws.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

It is common for class action lawsuits to be filed in Canada following an Incident involving the breach of PI. Representative plaintiffs commonly allege negligence, intrusion upon seclusion, breach of fiduciary duty, breach of contract, breach of warranty, breach of confidence, violation of privacy, publicity given to private life/public disclosure of private facts, breach of consumer protection legislation and/or conspiracy.

With respect to a claim of negligence, a plaintiff would generally have to prove the existence of a duty of care, breach of the standard of care, causation, and damages.

With respect to the tort of intrusion upon seclusion, the test requires proof on an objective standard that the alleged invasion of privacy would be highly offensive to a reasonable person.

With respect to a claim for breach of a fiduciary duty, a plaintiff would first have to prove the existence of a fiduciary relationship, then show that the fiduciary breached its obligations with respect to the fiduciary relationship by doing something that is contrary to the plaintiff's interests.

To make out a claim for breach of contract or breach of warranty, a plaintiff would have to show the existence of a valid and binding contract between the parties, a breach of the terms of the contract, and damages as a result of such breach. A breach of warranty typically entitles a successful plaintiff exclusively to damages.

With respect to a claim of breach of confidence, proof that the information was confidential, that it was communicated in confidence, and that it was misused by the recipient of the communication is required.

With respect to the tort of public disclosure of private facts, a plaintiff must prove that the disclosure was public, that the facts disclosed were private, and that the matter made public or the act of the publication would be highly offensive to a reasonable person and not of legitimate concern to the public.

The tort of simple motive conspiracy generally requires a plaintiff to show that the defendant engaged in conduct with the predominant purpose of causing the plaintiff injury, and that this conduct resulted in injury to the plaintiff.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

Some examples of class action lawsuits filed in connection with Incidents include:

- *Kaplan v. Casino Rama*, 2019 ONSC 2025 – Alleging that Casino Rama breached its privacy policy by failing to take reasonable security measures to protect against unauthorised access to class members' personal and confidential information.
- *Lozanski v. The Home Depot Inc.*, 2016 ONSC 5447 – Regarding a payment card system hacked by criminal intruders using custom-built malware.
- *Drew v. Walmart Canada Inc.*, 2017 ONSC 3308 – Following the breach of an online photo centre operated by a third-party service provider.
- *Tucci v. Peoples Trust Company*, 2017 BCSC 1525 – Alleging breach of contract, confidence and privacy, negligence and intrusion upon seclusion or, in the alternative, unjust enrichment and waiver of tort regarding a compromised database.
- *Maksimovic v. Sony of Canada Ltd.*, 2013 CanLII 41305 – Following a cyber-attack resulting in access to account holder information.
- *Zuckerman v. Target Corporation*, 2017 QCCS 110 – Regarding a breach affecting payment card data, including name and credit/debit card number, expiration date and security code.
- *Dentons Canada LLP v. Trisura Guarantee Insurance Company*, 2018 ONSC 7311 – Regarding a social engineering fraud, which resulted in a lawyer mistakenly transferring client funds to a fraudulent account.
- *Bourbonnière c. Yahoo! Inc.*, 2019 QCCS 2624 – Regarding stolen PI and financial information caused by various Incidents experienced by Yahoo!.
- *Del Giudice v. Thompson*, 2020 ONSC 2676 – Regarding an Incident which resulted in unauthorised access to the PI of those who applied for credit products.

Class action lawsuits were also filed in connection with the Incidents experienced by Ashley Madison and Equifax (see question 2.8).

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

As indicated above, it is common in Canada for class action lawsuits to be filed following an Incident. Representative plaintiffs have alleged various torts, including negligence and privacy torts, such as intrusion upon seclusion. As none of these cases have yet proceeded to trial (although some have settled), the liability of organisations that experience an Incident is still unsettled law in Canada.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Many general commercial liability policies do not cover Incidents, but specialised cyber risk policies are available and typically tailored to an organisation's particular risk profile as well as its size. Policies vary from first-party coverage, which protects the policy holder, to third-party coverage, which protects the policy holder from third-party claims.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are not.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Canadian government has broad powers to investigate criminal activities, including terrorism offences. For example, Section 487 of the Code permits searches of computer systems, and generation and seizure of data printouts, and allows a court to order the preservation of computer data in some circumstances.

The *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 allows the Director of Service or a designate to seek a warrant triggering broad powers to investigate a threat to Canadian security, both within and outside of Canada.

In connection with the federal government's National Cyber Security Strategy, the Royal Canadian Mounted Police ("**RCMP**") have established the National Cybercrime Coordination Unit ("**NC3**"). The NC3, once fully operational, will coordinate cybercrime investigations and provide investigative advice to law enforcement across Canada.

Regulators that are responsible for enforcing the Applicable Laws described in Section 2 (e.g. the OPC and the CRTC) also have broad investigatory powers. For example, the OPC can, amongst other powers: (a) summon and enforce the appearance of persons and compel them to give oral or written evidence on oath and to produce records in the same manner and to the same extent as a superior court of record; and/or (b) at any reasonable time, enter any premises (except a dwelling house), and converse in private with any person or examine or obtain copies/extracts from records found in such premises.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, currently there are none.

Lyndsay A. Wasser is the Co-Chair of McMillan's Privacy & Data Protection Group and its Cybersecurity Group. She is a Certified Information Privacy Professional/Canada and regularly advises and assists clients on a broad range of privacy and cybersecurity issues, including advising on legal requirements related to data security, workplace privacy issues, handling personal health information and transferring personal information across borders. She assists clients to develop privacy compliance programmes and data sharing agreements. She has assisted many clients with responding to privacy and data breaches involving various types of information (e.g., payment card information, patient data, employee personal information and sensitive identity information), including assisting with risk assessment, breach response strategy, notification obligations and communications with regulators. Lyndsay regularly writes and speaks on cybersecurity topics and is the co-author of *Privacy in the Workplace*, 4th ed. and the Privacy chapter in the *Ultimate Corporate Counsel Guide*.

McMillan LLP
Brookfield Place, Suite 4400
181 Bay Street, Toronto
Ontario, M5J 2T3
Canada

Tel: +1 416 865 7083
Fax: +1 416 865 7048
Email: lyndsay.wasser@mcmillan.ca
URL: www.mcmillan.ca

Kristen Pennington is an Associate Lawyer in the Toronto office of McMillan, where she practises both privacy and employment law. Kristen advises organisations with respect to legal requirements related to data security and workplace privacy issues, including employee background checks, the processing of personal information in connection with coronavirus, and cross-border transfers of personal information. She assists clients with developing practical, up-to-date privacy compliance programmes and with drafting appropriate data sharing terms with service providers and other third parties. Kristen regularly writes and speaks about emerging Canadian privacy topics and has been featured in a variety of leading industry publications.

McMillan LLP
Brookfield Place, Suite 4400
181 Bay Street, Toronto
Ontario, M5J 2T3
Canada

Tel: +1 416 865 7000
Fax: +1 416 865 7048
Email: kristen.pennington@mcmillan.ca
URL: www.mcmillan.ca

McMillan is a leading Canadian business law firm with recognised expertise and acknowledged leadership in major business sectors, which provides solutions-oriented legal advice through our offices in Vancouver, Calgary, Toronto, Ottawa, Montréal and Hong Kong. McMillan's privacy, data protection and cybersecurity experts have a thorough understanding of legal and regulatory obligations related to cybersecurity, and regularly assist organisations to proactively address and effectively respond to rapidly evolving cyber threats, including by: drafting security and data protection policies and protocols; drafting and reviewing insurance policies addressing cyber risk; negotiating agreements with third party suppliers and service providers to analyse cyber risk implications; advising on compliance with applicable data protection laws and other legislation; strategic handling of data breaches; and advising on and defending claims related to data protection, including defending class action litigation.

www.mcmillan.ca

China

Susan Ning

Han Wu

King & Wood Mallesons

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Under the Criminal Law of the People's Republic of China ("*Criminal Law*"), cybercrimes are mainly provided in the section: "Crimes of Disturbing Public Order". Articles 285, 286, and 287 are the three major Articles that directly relate to cybercrimes. Moreover, Article 253(1) indirectly relates to cybersecurity and applies to cases involving internet-related personal information infringement acts. The punishments for violating Articles 285, 286, and 287 include imprisonment, detention, and fines. For example, the offender may be sentenced to up to seven years' imprisonment for illegally obtaining data from a computer information system in serious cases. Entities may be convicted for violating Articles 285, 286, and 287, as unit crime has been provided for in all three Articles.

It is worth noting that Articles 286 and 287 set up the principle that if a person uses computers (for example, through hacking, phishing or other internet-related illegal action) to commit other crimes, i.e. crimes that traditionally had no relationship with the internet, such as financial fraud, theft, embezzlement, misappropriation of public funds and theft of state secrets, the offender shall be convicted of the crime for which the penalty is heavier.

Pursuant to Article 285 of the *Criminal Law*, activities which involve invading a computer information system in the areas of State affairs, national defence or advanced science and technology constitute the "crime of invading a computer information system". The offender shall be sentenced to a fixed-term imprisonment of not more than three years or detention. For activities of invading a computer information system other than those in the above areas, it may constitute a "crime of obtaining data from a computer information system and controlling a computer information system" and the offender shall be sentenced to a fixed-term imprisonment of not more than three years or detention, or imprisonment for three to seven years in serious cases. If an entity commits those crimes, such entities shall be fined, and the persons who are directly in charge and the other persons who are directly liable for the offences shall be punished accordingly.

For example, in the criminal case of "Wang's illegal obtainment of computer information system data and controlling a computer system", according to the final decision made by Fuyang Intermediate People's Court in Anhui Province in May 2018, the defendant was sentenced to three years in prison but suspended for five years and fined RMB 8,000 for illegally obtaining more than 9,000 pieces of personal information by using self-learning hacking technology.

Article 285 of the *Criminal Law* further provides that whoever, in violation of the state provisions, intrudes into a computer information system other than that prescribed in the preceding paragraph or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system or exercise illegal control over the said computer information system shall, if the circumstances are serious, be sentenced to a fixed-term imprisonment of no more than three years or criminal detention, and/or be fined; or if the circumstances are extremely serious, shall be sentenced to a fixed-term imprisonment of no less than three years but not more than seven years, and be fined.

It is noteworthy that the use of web crawlers may be regarded as invading conduct in violation of Article 285 if a technical method is adopted to crack anti-crawling measures set by websites or to bypass identity check processes set in a computer server. This is supported by various criminal cases in China. For example, according to a verdict of the Beijing Haidian District People's Court against Shanghai Shengpin Network Technology Limited and its employees, the employees of the accused company colluded to adopt technical measures to obtain video data stored in the server of the victim Beijing Byte Dance Technology Co., Ltd. Meanwhile, the chief technology officer of the company instructed other employees to crack-down the anti-crawling measures set in the victim's server. During the data-crawling process, the company used the forged device ID to bypass the server's identity check process, and used fake User Agent and IP addresses to avoid the server's access restrictions. The court finally decided that the conduct of the company and its employees violated Article 285 of the *Criminal Law*. A fine of RMB 200,000 was imposed on the company and the employees were sentenced to imprisonment, together with fines.

Pursuant to Article 29(1) of the Public Security Administration Punishments Law of the People's Republic of China ("Public Security Administration Punishments Law"), if a person, in violation of national regulations, invades a computer information system that causes harm to such system, he/she will be detained for not more than five days, and will be detained for more than five days but less than 10 days if the circumstances are serious.

Article 27 of the Cybersecurity Law of the People's Republic of China ("Cybersecurity Law") prohibits any person from endangering network security, such as illegally intruding into any other person's network, interfering with the normal functions of any

other person's network, and stealing network data. According to Article 63, any violation of the provision, if not regarded as committing a crime, will be subject to administrative penalties including confiscation of illegal income, detention of no more than five days, and a fine between RMB 50,000 to RMB 500,000. If the circumstances are relatively serious, the violator shall be detained for not less than five days but not more than 15 days, and may be fined between RMB 100,000 to RMB 1,000,000. Where an entity carries out any of the above conduct, the public security authority shall confiscate its illegal income, impose a fine of between RMB 100,000 to RMB 1,000,000, and punish its directly responsible person in charge and other directly liable persons in accordance with the provisions of the preceding paragraph. Article 63 of the *Cybersecurity Law* further provides that the person given a public security punishment due to his or her violation of Article 27 shall not hold a key position of cybersecurity management and network operation for five years; and a person given any criminal punishment shall be prohibited for life from holding a key position of cybersecurity management and network operation.

Denial-of-service attacks

Pursuant to Article 286 of the *Criminal Law*, denial-of-service attacks could constitute the "crime of sabotaging [a] computer information system", and a sentence of more than five years' imprisonment may be given in particularly serious cases.

Denial-of-service attacks may also lead to administrative penalties. Pursuant to Article 29(2) of the *Public Security Administration Punishments Law*, if a person, in violation of national regulations, deletes, changes, increases or interferes with the functions of a computer information system, making it impossible for the system to operate normally, an administrative penalty of detention of less than five days, or in serious cases, detention of more than five days but less than 10 days, will be imposed.

In terms of *Cybersecurity Law*, a denial-of-service attack will also be regarded as endangering network security and will also be subject to penalties under Article 63 of the *Cybersecurity Law*.

Phishing

Phishing is usually performed to steal or otherwise acquire the personal information of citizens, which is considered the "crime of infringing a citizen's personal information" provided in Article 253(1); up to seven years' imprisonment may be sentenced in serious cases.

For example, in the criminal case of "Zhang Dawei's infringement upon a citizen's personal information", the defendant established a phishing website to counterfeit the official website of Apple iCloud. In this way, the defendant obtained a victim's Apple ID and password and then sold them for profit. The court decided that the defendant committed the "crime of infringing a citizen's personal information" and imposed seven months' imprisonment.

Furthermore, as most phishing is conducted by spreading a computer virus, the administrative penalty for this is for detention of less than five days, or in serious cases, detention of more than five days but less than 10 days, pursuant to Article 29 of the *Public Security Administration Punishments Law*. Article 63 of the Cybersecurity Law may also apply.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

For intentional creation or dissemination of a computer virus or other destructive programs, including, but not limited to, ransomware, spyware, worms, trojans and viruses, which affect the normal operation of a computer information system, if serious consequences are caused, such activities constitute the "crime of sabotaging a computer information system" under Article 286 of the *Criminal Law*. The offender may be sentenced to five years' imprisonment in serious cases.

In addition, intentionally making up or transmitting such destructive programs that adversely affect the normal operation of a computer information system is illegal, pursuant to Article 29 of the *Public Security Administration Punishments Law*. The violator may be subject to detention of less than five days, or in serious cases, detention of more than five days but less than 10 days. Article 63 of the *Cybersecurity Law* may also apply.

Besides, Article 47 of the *Cybersecurity Law* provides that electronic information sent by and application software provided by any individual or organisation shall not be installed with malware, and the violator, according to Article 60 of the *Cybersecurity Law*, will be ordered to take corrective action and be given a warning by the competent authorities. If the violator refuses to take corrective action, or such consequences as endangering cybersecurity are caused, it shall be fined between RMB 50,000 to RMB 500,000, and its directly responsible person in charge shall be fined between RMB 10,000 to RMB 100,000.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

If a person provides hardware, software or other tools specially used for invading or illegally controlling computer information systems, or if the person knows that any other person is committing the criminal act of invading or illegally controlling a computer information system and still provides programs or tools for such a person, he/she shall commit the crime of "providing program[s] or tools for invading or illegally controlling computer information systems", pursuant to Article 285 of the *Criminal Law*.

In addition, if a person intentionally makes up or transmits destructive programs such as computer viruses that adversely affect the normal operation of a computer information system, and if not severe enough to constitute a crime, he/she will be penalised according to Article 29 of the *Public Security Administration Punishments Law*. Furthermore, Articles 27 and 63 of the *Cybersecurity Law* also prohibit provision of programs or tools specifically used for conducting any activity endangering cybersecurity, or provision of technical support, advertising promotions, payments and settlement services or any other assistance to any person conducting any activity endangering cybersecurity.

Possession or use of hardware, software or other tools used to commit cybercrime

If a person possesses or uses hardware, software or other tools to commit cybercrime as prescribed in the *Criminal Law*, depending on the crime committed, the offender may be convicted in accordance with the corresponding Article in the *Criminal Law*, such as the "crime of invading a computer information system".

There is also an offence, i.e. "illegal use of information networks", which involves activities that take advantage of an information network to establish websites and communication groups for criminal activities, such as defrauding, teaching criminal methods, producing or selling prohibited items and controlled substances. If the criminal activity also constitutes another offence, the offender shall be convicted of the crime which imposes a heavier penalty.

Identity theft or identity fraud (e.g. in connection with access devices)

Under the *Criminal Law*, for identity theft, if the offender obtains identities by stealing or otherwise illegally acquires the personal

information of citizens, such activity may be convicted as the "crime of infringing a citizen's personal information", pursuant to Article 253(1). If a person uses the stolen identity of others as his/her own proof of identity, such behaviour may constitute the "crime of identity theft" under Article 280(1) of the *Criminal Law*; in case such person uses the stolen identity to commit fraud or other criminal activities, he/she should be convicted of the crime the penalty of which is higher.

The *Cybersecurity Law* protects network information security, including the security of personal information. Stealing or illegally acquiring the personal information of citizens may also cause administrative penalties if the violation is not severe enough to constitute a crime.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

If a current or former employee breaches confidentiality obligations and causes infringement of personal information, trade secrets, or state secrets, etc., the offender will be convicted pursuant to Article 287 and punished in accordance with the relevant provisions of the *Criminal Law*, such as the "crime of infringing trade secrets".

The infringement of trade secrets, under the Anti-unfair Competition Law of the People's Republic of China (the "*Anti-unfair Competition Law*"), will be subject to administrative penalties, including being ordered to cease the infringing conduct, the confiscation of illegal income, a fine ranging from RMB 100,000 to RMB 1 million, and a fine ranging from RMB 500,000 to RMB 5 million if the circumstances are serious.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Unsolicited penetration testing could be seen as an illegal invasion of another person's computer information system, without getting prior permission or consent.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

If a person, in violation of laws and regulations, deletes, amends, adds or disturbs the functions of a computer information system and causes the computer information system's inability to work normally, or conducts operations of deletion, amendment or addition towards the data or application programs which are stored, disposed of or transmitted in a computer information system, and serious consequences result, such activities constitute the "crime of sabotaging [a] computer information system" under Article 286 of the *Criminal Law*. The offender shall be sentenced to a fixed-term imprisonment of more than five years if serious consequences result.

If a person, in violation of national regulations, deletes, changes, or increases the stored, processed, or transmitted data and the application program of a computer information system, the person shall be detained for less than five days, or in serious cases, detained for more than five days but less than 10 days, pursuant to Article 29 of the *Public Security Administration Punishments Law*. Besides, any conduct in addition to what is described above that endangers network security will be regulated under Articles 27 and 63 of the *Cybersecurity Law*.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the above-mentioned crimes have extraterritorial application. Firstly, if the criminal act or its consequences take place within the territory of China, the crime shall be deemed to have been committed within the territory of China. Secondly, the *Criminal Law* is applicable to citizens of China who commit crimes prescribed in the *Criminal Law* outside the territory of China; however, if the maximum penalty of such crime prescribed in the *Criminal Law* is a fixed-term imprisonment of not more than three years, the offender could be exempted from punishment. Thirdly, if a foreigner commits a crime outside the territory of China against the State or against Chinese citizens, the offender may be convicted pursuant to the *Criminal Law* if the *Criminal Law* prescribes a minimum punishment of fixed-term imprisonment of not less than three years; however, the *Criminal Law* shall not apply if it is not punishable according to the law of the place where it was committed.

The *Public Security Administration Punishments Law* is applicable within the territory of the People's Republic of China (except where specially provided for by other laws), or to acts against the administration of public security committed aboard ships or aircrafts of the People's Republic of China (except where specially provided for by other laws).

The *Cybersecurity Law* generally applies to the construction, operation, maintenance and use of the network within the territory of the People's Republic of China. Where any overseas institution, organisation or individual attacks, intrudes into, disturbs, destroys or otherwise damages the critical information infrastructure of the People's Republic of China, causing any serious consequence, the violator shall be subject to legal liability; and the public security department of the State Council and relevant authorities may decide to freeze the property of or take any other necessary sanctions measure against the institution, organisation or individual.

The *Anti-unfair Competition Law* does not explicitly provide that it has extraterrestrial application. In principle, any conduct that disrupts market competition or harms the legitimate rights and interests of business operators or consumers will be regulated under this Law.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

For the above-mentioned offences, there are no specific mitigation conditions prescribed in these Articles. However, the mitigation conditions prescribed in the *Criminal Law* for all crimes are applicable. For example, if an offender voluntarily gives oneself up to the police and confesses his crimes or exposes others' crimes that can be verified, the offender would be given a mitigated punishment.

The *Anti-unfair Competition Law* provides in Article 25 that where a business operator who engages in unfair competition takes the initiative to eliminate or mitigate the harmful consequences of the illegal act, the administrative punishment shall be reduced or mitigated; where the illegal act is trivial and promptly corrected and does not cause harmful consequences, no administrative punishment shall be imposed. The *Law of the People's Republic of China on Administrative Penalty* (the "*Administrative Penalty Law*") generally sets out circumstances where the administrative penalties could be mitigated, including taking the initiative to eliminate or mitigate the harmful consequences of the illegal act, being coerced by another person to commit the illegal act, and performing meritorious deeds in coordination with the authorities to conduct an investigation, etc.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The *Cybersecurity Law*, which came into force on 1 June 2017, is the law covering various aspects of network security and has laid the foundation for a comprehensive cybersecurity regulatory regime in China. So far, a series of specific measures aimed at facilitating the implementation of the *Cybersecurity Law* have already been enacted, such as the *Measures on the Security Review of Network Products and Services (for Trial Implementation)*, the *National Emergency Response Plan for Cybersecurity Incidents*, and the *Provisions on Protection of Children's Personal Information Online*.

The *Cybersecurity Law* recognises the graded cybersecurity protection as the basic legal system to ensure network security in China. While the *Regulation on Graded Protection of Cybersecurity* is still seeking opinions, relevant authorities have officially been promulgating recommended national standards regarding graded cybersecurity protection since May 2019 for guiding the graded protection. These national standards include, but are not limited to: the *Information Security Technology-Baseline for Classified Protection of Cybersecurity* (GB/T 22239-2019), which replaces GB/T 22239-2008; the *Information Security Technology-Evaluation Requirement for Classified Protection of Cybersecurity* (GB/T 28448-2019), which replaces GB/T 28448-2012; the *Information Security Technology-Technical Requirement of Security Design for Classified Protection of Cybersecurity* (GB/T 25070-2019), which replaces GB/T 25070-2010; the *Implementation Guide for Classified Protection Of Cybersecurity* (GB/T 25058-2019), which replaces GB/T 25058-2010; and the *Classification Guide for Classified Protection Of Cybersecurity* (GB/T 22240-2020), which replaces GB/T 22240-2008.

Meanwhile, the draft regulations and guidelines on the protection of critical information infrastructure ("*CII*"), data processing and security assessment of outbound data transfers have been finished and the relevant authorities are now seeking opinions, including the draft *Regulations on the Security Protection of Critical Information Infrastructure,* the draft *Measures for Cybersecurity Censorship*, the draft *Administrative Measures on Data Security*, the draft *Measures for Security Assessment for Cross-border Transfer of Personal Information*, the draft *Guidelines for the Security Assessment of Cross-Border Data Transfer*, and the draft *Administrative Provisions on Cybersecurity Loophole*.

Furthermore, since 2019, China has strengthened the regulation of personal information collection, especially with regard to the personal information collected by apps, and several regulative documents or guidelines, including the *Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps*, the *Methods for Determining the Illegal Collection and Use of Personal Information by Apps*, and the *Guide to Self-Assessment of the Collection and Use of Personal Information by Apps*, etc., have been issued.

Moreover, the *Cryptography Law of the People's Republic of China* ("*Cryptography Law*"), which came into effect on 1 January 2020, provides regulation on the management and use of cryptography.

In July 2020, China promulgated the *Data Security Law (Exposure Draft)*, which applies to the collection, storage, processing, use, provision, transaction and disclosure of all types of data.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The *Cybersecurity Law* includes provisions on the security protection of CII. The draft *Regulations on the Security Protection of Critical Information Infrastructure* further specify the requirements on the security protection of critical information infrastructure, including CII operators' obligations relating to the setting up, suspension of operation and occurrence of security Incidents of CII, daily security maintenance, security monitoring and assessment, local data storage and security assessment of outbound data transfers, and security of network products and services procured, etc.

The *Cybersecurity Review Measures* enacted in June 2020 require CII operators to conduct a cybersecurity review if their purchase of a network, product or service affects or may affect national security. Article 27 of the *Cryptography Law* provides that for CII operators, laws, administrative regulations, and relevant national regulations require protection by commercial cryptography; thus, the CII operators thereof shall use commercial cryptography for protection and conduct a security assessment of commercial cryptography applications.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. The *Cybersecurity Law*, the *Regulations on the Security Protection of Computer Information System*, the *National Emergency Response Plan for Cybersecurity Incidents*, and other relevant laws and regulations have provided for network operators' legal duties when facing cybersecurity Incidents, which in general could be categorised into the following:

(1) regular preventive work: network operators must adopt regular measures to prevent cybersecurity Incidents, including adopting technical measures to prevent cybersecurity violations such as computer viruses, cyberattacks and network intrusions, adopting technical measures to monitor and record the network operation status and cybersecurity events, and maintaining cyber-related logs for no less than six months, etc.;

(2) emergency measures for security Incidents: network operators must develop an emergency plan for cybersecurity Incidents in order to promptly respond to security risks, to take remedial actions immediately, to notify affected data subjects, and to report the case to the competent authorities as required; and

(3) after-action review: to keep communication with and assist the authorities in finishing their investigation and review after an Incident, such as providing a summary of the cause, nature, and influence of the security Incident and improvement measures.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes.

(a) The reporting obligation will be triggered by the occurrence of an Incident threatening network security.

(b) Pursuant to the *Cybersecurity Law* and relevant regulations, network operators shall at least timely notify the local government, industry regulators, public security authorities and local cyberspace administrations. Pursuant to the *Regulations of the People's Republic of China on the Security Protection of Computer Information System*, any case arising from computer information systems shall be reported to the public security authority within 24 hours. Moreover, if there is a possibility of information leakage related to national security, the national security authorities shall also be informed.

(c) At least the following contents are required to be reported: information of the notification party; description of the network security Incident; detailed information about the Incident; nature of the Incident; affected properties (if any); personal information being affected/breached (if any); preliminary containment measures that have been taken; and preliminary assessment on the severity of the Incident.

(d) If the publication of Incident-related information will jeopardise national security or public interest, then such publication shall be prohibited.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes.

(a) Under the *Cybersecurity Law*, in case of disclosure, damage or loss, or possible disclosure, damage or loss, of user information, the network operator is obligated to take immediate remedies and notify the affected users promptly. In addition, for any risk, such as a security defect or bug that is found in a network product or service, the product/service provider concerned shall inform the users of the said risk.

(b) Currently, relevant laws and regulations do not provide specific requirements regarding the nature and scope of information to be reported; according to the Information Security Techniques – Personal Information Security Specification, recommended standards formulated by the National Standardization Committee, operators shall at least inform data subjects of the general description of the Incident and its impact, any remedial measures taken or to be taken, suggestions for individual data subjects to mitigate risks, and contact information of the person responsible for dealing with the Incident, etc.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Any regulators identified under question 2.4 above to which network operators are required to report an Incident shall have the authority to enforce the requirements identified under questions 2.3 to 2.5. Specifically, the enforcement authorities include the Cyberspace Administration of China ("*CAC*"), the Ministry of Industry and Information Technology ("*MIIT*"), the Ministry of Public Security ("*MPS*"), the State Secrecy Bureau, the State Encryption Administration and industry regulators, etc.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Pursuant to the *Cybersecurity Law*, in case of non-compliance, network operators may be given a warning, ordered to take rectification measures, and/or imposed fines by the relevant authorities. In case of refusal to make rectifications or in severe circumstances, further penalties such as suspension of related business, winding up for rectification, shutdown of websites, and revocation of a business licence may be imposed by the competent authorities.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

One of the first enforcement actions taken since the implementation of the *Cybersecurity Law* relates to the failure to maintain web logs. The cybersecurity team of the public security bureau of Chongqing Municipality gave warnings to a company providing a data centre service for failure to keep a web log, as required by the *Cybersecurity Law*, and ordered it to rectify the non-compliance.

In January 2018, a local library was fined by the local public security bureau in Henan Province due to its failure to adopt technical measures to prevent computer viruses which resulted in attacks on the website. A fine of RMB 20,000 was imposed on the library.

Each year, the CAC, MIIT, and MPS, together with the National Work Group for "Combating Pornography and Illegal Publications", initiate a special campaign called "Jingwang" (clean the internet), aiming at investigating and preventing illegal activities in cyberspace or cybercrimes. The Jingwang 2020 campaign was initiated in May 2020 and the public security authorities have successfully detected a high number of cybercrimes, including dissemination of pornographic materials through the Internet.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

The use of Beacons may result in the collection and use of users' personal information. Pursuant to the *Cybersecurity Law*, organisations shall notify users and obtain their consent before collecting information. Considering the difficulty of obtaining consent when collecting information through Beacons, they are generally regarded as not complying with the basic requirements under the *Cybersecurity Law*.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Relevant laws and regulations do not explicitly prohibit organisations from using Honeypots to detect and deflect Incidents in their own network.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Relevant laws and regulations do not explicitly prohibit organisations from using Sinkholes to detect and deflect Incidents in their own network.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Monitoring or intercepting electronic communications may trigger privacy issues, as they usually involve collection of private or personal communication information. The *Civil Code of People's Republic of China* ("*Civil Code*"), which will be enacted on 1 January 2021, explicitly prohibits individuals or organisations from infringing upon a natural person's right to privacy. Specifically, Article 1033 of the *Civil Code* provides that unless otherwise prescribed by the law or specifically agreed by the right holders, no organisation or individuals are allowed to deal with the private information of others.

Furthermore, Article 65 of the *Telecommunications Regulations of the People's Republic of China* ("*Telecommunications Regulations*") provides that except for the inspection of telecommunications contents by the public security authorities, the national security authorities, or the People's Procuratorate in accordance with the procedures stipulated by the law for the purposes of national security or a criminal investigation, no organisation or individual shall inspect telecommunications contents for any reason.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Pursuant to Article 28 of the *Cryptography Law*, the commerce department of the State Council and the state cryptography administration shall implement import licensing for commercial cryptography that involves State security and public interest and that have encryption protection functions. They shall implement export controls on commercial cryptography that involves State security and public interest or that involves the international obligations of China.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Although industries or sectors such as telecoms, credit reporting, banking and finance, and insurance have some specific requirements with respect to the collection and protection of information, the prevention of information leakage, and the emergency response to Incidents, these requirements are, in general, in line with those under the *Cybersecurity Law* without deviations.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes. For example, the *Provisional Rules on Management of the Individual Credit Information Database* are promulgated by the People's Bank of China to ensure the secure and legitimate use of personal credit information, the *Measures of the People's Bank of China for the Protection of Financial Consumers' Rights and Interests* (updated by the People's Bank of China in September 2020) obliges financial institutions to ensure the security of personal financial information, and the *Anti-Money Laundering Law*, as well as the *Administrative Measures for the Identification of Clients and the Keeping of Clients' Identity Information and Transaction Records by Financial Institutions*, require financial institutions to take technical measures to prevent the loss, destruction or leakage of their client's identity information or transaction data. In addition, pursuant to the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users*, telecommunication business operators or internet information service providers shall record information such as the staff members who perform operations on the personal information of users, the time and place of such operations, and the matters involved, to prevent user information from being divulged, damaged, tampered with or lost.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Under the *Cybersecurity Law*, if a company, as a network operator, fails to fulfil the obligation of security protection to ensure that the network is free from interference, disruption or unauthorised access, and to prevent network data from being disclosed, stolen or tampered with, fails to satisfy the mandatory requirements set forth in the applicable national standards, or fails to develop an emergency plan for cybersecurity Incidents, a warning shall be imposed on the company, and a fine will be imposed on both the company and the responsible person directly in charge if such company refuses to make rectifications or causes threats to cybersecurity.

Moreover, as mentioned in question 1.1 above, pursuant to Article 286(1) of the *Criminal Law*, if a network service provider fails to perform its duties of security protection on the information network as required by laws and administrative regulations, and refuses to correct their conduct after the regulatory authorities order them to rectify the non-performance, the network operator shall be fined, and the persons directly in charge and the other persons directly liable for the offences may be sentenced.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the *Cybersecurity Law*, all network operators are required to designate a person in charge of cybersecurity, such as a chief information security officer ("*CISO*"), to establish an emergency

plan for cybersecurity Incidents, and to take technical measures to monitor and record network operation and cybersecurity events.

In addition, pursuant to Article 38 of the *Cybersecurity Law*, CII operators are required to conduct, by themselves or entrusting a service provider, an examination and assessment of their cybersecurity and the potential risks at least once a year, and submit the examination and assessment results, as well as improvement measures, to the competent authorities in charge of the security of the CII. That is to say, periodic cyber risk assessments and vulnerability assessments are mandatory for CII operators.

There is no clear requirement to include third-party vendors in the scope of the risk assessment. However, critical network equipment and special-purpose cybersecurity products provided by third-party vendors should satisfy the compulsory requirements set forth in the national standards and shall not be sold or supplied until such equipment or product successfully passes security certification or security tests by a qualified organisation.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Please refer to the answers to questions 2.4 and 2.5 above.

In addition, listed companies may have the duty to disclose cybersecurity risks or Incidents to the China Securities Regulatory Commission or disclose such information in their annual reports, depending on whether such information is deemed as significant and required to be disclosed.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

From the perspective of individuals, if an Incident results in unauthorised access to or disclosure of personal information collected and kept by the network operator, the individuals affected could bring a lawsuit against such network operator for breach of security protection obligations or for disclosing personal information by negligence on the basis of tort pursuant to the *Civil Code*. In two private lawsuits brought by consumers in July 2020, the court of first instance gave its verdict that the defendants in both cases had infringed consumers' rights and interests regarding personal information.

Further, as confirmed by the decision in the *Sina/Maimai* case ruled by the Beijing Intellectual Property Court, user data/information is an important operating resource and confers competitive advantages to network operators. If a network operator "steals" data from its competitor by accessing the data of such competitor without authorisation, the aggrieved party could sue the infringing party for unfair competition on the basis of the *Anti-unfair Competition Law of the People's Republic of China*.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

Qunar, a major online ticket-booking platform in China, and China Eastern Airlines were sued by one of its users for tort before the First Intermediate People's Court of Beijing in March 2017, as the user's personal information, including name and telephone number, was disclosed by Qunar and China Eastern Airlines to a third party who sent phishing messages to such user, claiming that the flight booked was cancelled. The court ordered Qunar and China Eastern Airlines to apologise to the plaintiff.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Please refer to the answer to question 6.1.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations may take out insurance against Incidents, provided that such insurance categories are within the permitted scope of insurance regulations and have been approved by or filed with the China Insurance Regulatory Commission ("*CIRC*"). Currently, in China, there are already several insurance agents providing insurance related to Incidents such as data leakage, hacking, etc.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

So far, we are not aware of any regulation that sets out limitations specifically on insurance against Incidents. Normally, the coverage of loss will be decided through private negotiation between the insurer and the applicant, as long as such coverage does not violate mandatory regulations in China.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In accordance with the *Cybersecurity Law* and other relevant regulations, generally there are several enforcement agencies that are entitled to have investigatory power regarding an Incident, such as:

(1) the CAC, which is responsible for the overall planning and coordination of cybersecurity work and the relevant supervision and administration; and

(2) the authority in charge of telecommunication, the public security authority and other relevant authorities of the State Council, which will take charge of protecting, supervising and administrating cybersecurity pursuant to the present regulations in China.

The specific investigatory power of the above enforcement agencies can be found in a number of laws and regulations. For example, as stated in Article 54 of the *Cybersecurity Law*, the relevant departments of the government at provincial level and above are entitled to take the following measures in case of an increasing risk of an Incident:

(1) require authorities, organs and personnel concerned to promptly collect and report necessary information;

(2) organise authorities, organs and professionals concerned to analyse and evaluate cybersecurity risks; and
(3) give warnings to the public about the cybersecurity risks and release prevention and mitigation measures.

Pursuant to Article 19 of the *Anti-Terrorism Law of the People's Republic of China* ("*Anti-Terrorism Law*"), where a risk of terrorism may arise in an Incident, the CAC, competent telecommunications department, public security department, as well as the national security department shall carry out the following actions in accordance with their respective duties:

(1) order the relevant entities to stop transmission and delete the information involving terrorism and extremism; and
(2) shut down the relevant sites and cease the related services.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

First, the *Cybersecurity Law* has made it clear that network operators shall provide technical support for the public security department and the national security department specifically on two matters: 1) safeguarding national security; and 2) investigation of crimes. Second, the *Anti-Terrorism Law* explicitly states that telecommunications operators and internet service providers shall facilitate the relevant departments in terrorism cases, such as providing technical interfaces and decryption services. Moreover, for entities and individuals which engage in international network connections, public security departments may also ask them to provide information, materials and digital files on security protection matters when investigating crimes committed through computer networks connected with international networks. In several business sectors, such as the financial sector, there are also applicable laws or regulations requiring entities to coordinate with relevant industrial regulators in their investigatory activities. For example, the *Anti-Money Laundering Law* requires financial institutions to promptly report transactions of large amounts and suspicious transactions to the anti-money laundering information centre.

Susan Ning is a senior partner and the head of the Commercial and Regulatory Group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the *Journal of Cyber Affairs*. Her articles include "New Trends of the US Personal Data Protection – Key Points of the New FCC Rules", "Big Data: Success Comes Down to Solid Compliance", "Does Your Data Need a "VISA" to Travel Abroad?", and "A Brief Analysis on the Impact of Data on Competition in the Big Data Era", among others. Susan is recognised as a "Tier 1 Lawyer" for Cybersecurity and Data Compliance in 2019 *LEGALBAND* China.
Susan's practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, compliance of cross-border data transmissions, etc. Susan has assisted companies in sectors such as IT, transportation, online payments, consumer goods, finance, Internet of Vehicles in dealing with network security and data compliance issues.

King & Wood Mallesons
18th Floor, East Tower
World Financial Center
1 Dongsanhuan Zhonglu
Chaoyang District
Beijing 100020
P. R. China

Tel: +86 10 5878 5010
Email: susan.ning@cn.kwm.com
URL: www.kwm.com

Han Wu practises in the areas of cybersecurity, data compliance and antitrust. He excels in providing cybersecurity and data compliance advice to multinational companies' branches in China from the perspective of data compliance in China. Han also has expertise in establishing network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the European Union (GDPR), the United States and other cross-jurisdictions. Han was elected as one of "40-under-40 Data Lawyers" by *Global Data Review* in 2018. In the areas of cybersecurity and data compliance, Han provides legal services including: assisting clients to establish a cybersecurity compliance system; assisting clients in self-investigation on cybersecurity and data protection; assisting clients to conduct internal training on cybersecurity and data compliance; assisting clients in due diligence in data transactions; assisting clients to design plans for cross-border data transfers; and assisting clients in network security investigations and cybersecurity Incidents, among others.

King & Wood Mallesons
18th Floor, East Tower
World Financial Center
1 Dongsanhuan Zhonglu
Chaoyang District
Beijing 100020
P. R. China

Tel: +86 10 5878 5749
Email: wuhan@cn.kwm.com
URL: www.kwm.com

King & Wood Mallesons is an international law firm headquartered in Asia that advises Chinese and overseas clients on a full range of domestic and cross-border transactions, providing comprehensive legal services. Around the world, the firm has over 2,000 lawyers with an extensive global network of 27 international offices spanning Singapore, Japan, the US, Australia, the UK, Germany, Spain, Italy and other key cities in Europe as well as presences in the Middle East. With a large legal talent pool equipped with local in-depth and legal practice, it provides legal services in multiple languages. King & Wood Mallesons, with its strong foundation and ever-progressive practice capacity, has been a leader in the industry. It has received more than 300 international and regional awards from internationally authoritative legal rating agencies, businesses and legal media, including Acritas, *The Financial Times*, *ALB*, *Who's Who Legal*, *Chambers Asia-Pacific* Awards, *Euromoney*, *LEGALBAND*, *Legal Business*, *The Lawyer*, etc.

www.kwm.com

KING&WOOD MALLESONS
金杜律师事务所

England & Wales


Nigel Parker


Nathan Charnock

Allen & Overy LLP

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes. Under the Computer Misuse Act 1990, it is an offence to cause a computer to perform any function with the intent to secure unauthorised access to any program or data held in a computer (or enable such access to be secured). On indictment, the maximum penalty is two years' imprisonment. If a person commits this offence with the intent to commit or facilitate a more serious "further offence" (e.g. theft via the diversion of funds), the maximum penalty is five years' imprisonment. In 2019, a director of a CCTV provider and her employee were sentenced to 14 months' and five months' imprisonment (respectively) after they accessed CCTV footage of the post-mortem of footballer Emiliano Sala. In 2019, a disgruntled former IT contractor at Jet2 was sentenced to 10 months' imprisonment after he deleted user accounts and accessed the email account of the Jet2 CEO in a revenge attack.

Denial-of-service attacks
Yes. Under the Computer Misuse Act 1990, it is an offence to do any unauthorised act in relation to a computer that a person knows to be unauthorised, with the intent of impairing the operation of any computer, preventing or hindering access to any program or the data held in any computer, impairing the operation of any program or the reliability of any data, or enabling any of the above. On indictment, the maximum penalty is 10 years' imprisonment. In 2017 and 2019, two individuals were each sentenced to 16 months in youth offender institutions for separate denial-of-service attacks against various websites targeting websites of law enforcement and a number of companies including Amazon, Netflix and NatWest.

Phishing
Yes. See the answer in respect of hacking.

Under the Fraud Act 2006, phishing could also constitute fraud by false representation if (for example) an email was sent falsely representing that it was sent by a legitimate firm. On indictment, the maximum penalty is 10 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes. See the answer in respect of denial-of-service attacks.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Yes. Under the Computer Misuse Act 1990, it is an offence to make, adapt, supply or offer to supply any article intending it to be used to commit, or which may be likely to be used to commit, an offence under section 1 (see the answer in respect of hacking) or section 3 (see the answer in respect of denial-of-service attacks) of the Act. On indictment, the maximum penalty is two years' imprisonment.

Under the Fraud Act 2006, it is an offence to make or supply articles for use in the course of, or in connection with fraud, provided the individual either has (i) knowledge that the article is designed or adapted for use in the course of or in connection with fraud, or (ii) intends the article to be used to commit or assist in the commission of fraud. On indictment, the maximum penalty is 10 years' imprisonment.

In 2019, an individual was sentenced to nine years' imprisonment after he created website scripts designed to look like the websites of up to 53 UK-based companies to help criminals defraud victims out of approximately £41.6 million. He also supplied the criminals with software that disguised their phishing sites from being identified by web browsers.

Possession or use of hardware, software or other tools used to commit cybercrime
Yes. See the response relating to the distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime above.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes. Under the Fraud Act 2006, it is an offence to dishonestly make a false representation, knowing that the representation was or may be untrue or misleading, with the intent of making a gain for yourself or another or causing a loss or risk of loss to another (i.e. fraud by false representation). On indictment, the maximum penalty is 10 years' imprisonment. In 2019, an individual was convicted of offences under the Fraud Act 2006 and Computer Misuse Act 1990 (after accessing a barrister colleague's email account to copy his practising certificate in order to produce a faked copy in his own name before going on to practice as a barrister working on 18 cases) and was sentenced to a total of two years' and three months' imprisonment.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Yes. This may constitute an offence under the Computer Misuse Act 1990 (such as hacking) as well as a financial crime, such as theft (under the Theft Act 1990). A breach of confidence or

misuse of private information is actionable as a common law tort, but not as a criminal offence in itself. In 2020, a self-employed IT support specialist was sentenced to 20 months' imprisonment for offences under the Computer Misuse Act 1990 and the Theft Act 1990 after he stole over £31,000 in cryptocurrency from a client.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Yes. See "Hacking (i.e. unauthorised access)" above.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Please see above. In addition, certain terrorism offences may arise in relation to cybersecurity. For example, under the Terrorism Act 2000, it is an offence to take any action designed to seriously interfere with or seriously disrupt an electronic system if this is designed to influence the government or intimidate the public or a section of the public, or for the purpose of advancing a political, religious, racial or ideological cause.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes. For certain offences under the Computer Misuse Act 1990 (such as hacking, phishing or denial-of-service attacks), the offence will be committed where there is a "significant link to the domestic jurisdiction". This includes the person committing the offence being in the UK, the target computer being in the UK or a UK national committing the offence while outside the UK (provided in the latter instance that the act was still an offence in the country where it took place).

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

There is an exemption for certain offences under the Computer Misuse Act 1990 (such as hacking, phishing or denial-of-service attacks) in respect of an enforcement officer acting in accordance with legislation to facilitate inspection, search or seizure without a person's consent. There are no general defences under the Computer Misuse Act 1990. However, Crown Prosecutors will consider a number of public interest factors before charging an individual with an offence.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

England and Wales does not have a comprehensive cybersecurity law; instead, the legal framework for cybersecurity is dispersed across a number of different laws:

- **Data Protection Act 2018** – applies, alongside the EU General Data Protection Regulation insofar as it forms part of retained EU law in the UK following Brexit (**UK GDPR**), to Incidents to the extent that they involve Personal Data. The Data Protection Act 2018 also sets out data protection requirements for national security and immigration as well as other domestic areas of law.
- **Communications Act 2003** – includes cybersecurity obligations that apply in the telecommunications sector to public electronic communications network providers and public electronic communications service providers.
- **Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)** – includes security obligations in respect of personal data that apply to public electronic communications service providers.
- **The Network and Information Systems Regulations 2018 (NIS Regulations)** – implements the EU Network and Information Systems Directive into UK law, imposing obligations on operators of essential services (**OES**) and relevant digital service providers (**RDSPs**). OES are organisations that operate services deemed critical to the economy and wider society such as water, transport, energy, healthcare and digital infrastructure. RDSPs are anyone who provides online marketplaces, online search engines or cloud computing services and, is a medium or large-sized business with its head office, or a nominated representative in the UK. The NIS Regulations require OES and RDSPs to have sufficient security systems in place to prevent the data they hold or the services they provide being compromised and to report certain Incidents to a competent authority. The ICO is the competent authority for RDSPs. See question 2.2 for more information about OES.
- **The Regulation of Investigatory Powers Act 2000 (RIPA)** – governs the investigative powers of law enforcement, such as surveillance and interception of communications data. RIPA will ultimately be replaced by the Investigatory Powers Act 2016, the operative provisions of which are not yet all in force.
- **The Computer Misuse Act 1990** – sets out various cybercrime offences (see answers to question 1.1), which may be prosecuted in conjunction with offences under the **Theft Act 1968** or the **Fraud Act 2006**.
- **Official Secrets Act 1989** – may apply in respect of servants of the Crown or UK government contractors, and creates offences in relation to disclosure (or failure to secure) certain information which may be damaging to the UK's interests.
- Governance obligations, which can directly or indirectly relate to cybersecurity, apply to public companies under the **Companies Act 2006**, the Disclosure and Transparency Rules and the Listing Rules in the **Financial Conduct Authority (FCA) Handbook** and the risk management and control provisions in the **UK Corporate Governance Code**.
- Various common law doctrines may also apply in respect of civil actions (see question 5.1).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

- **Telecommunications sector** – cybersecurity requirements under the Communications Act 2003 require providers of

public electronic communications networks and public electronic communications services to, amongst other things, maintain the security and integrity of those networks and services, including by taking measures to prevent or minimise the impact of Incidents on end users and on the interconnection of networks.

- **Operators of essential services (OES)** – The NIS Regulations came into force in the UK on 10 May 2018, imposing certain security duties, on any "operator of essential services", including a duty to notify Incidents to the relevant competent authority. The NIS Regulations identify sector-based competent authorities (for sectors covering energy, transport, health, drinking water supply and distribution and digital infrastructure) with the National Cyber Security Centre (**NCSC**) as the UK's single point of contact for Incident reporting. The NIS Regulations also place obligations on digital service providers in relation to security and reporting of Incidents. The NCSC does not have a regulatory function but it will undertake the role of the Computer Security Incident Response Team responding to Incidents which arise as a result of a cyber-attack and which have been notified to it. The NIS Regulations introduce a range of penalties that can be imposed by the relevant competent authority. These range from £1 million for any contravention of the NIS Regulations which the relevant authority determines could not cause an Incident, up to £17 million for a material contravention of the NIS Regulations which the relevant authority determines has caused, or could cause, an Incident resulting in immediate threat to life or significant adverse impact on the United Kingdom economy.
- **Financial services sector** – The Senior Management Arrangements Systems and Controls (**SYSC**) part of the FCA Handbook (see answer to question 3.2) applies to financial services infrastructure providers who are regulated by the FCA – these organisations will be operators of essential services for the purposes of the NIS Regulations (see above).

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Data Protection Act 2018 (and the UK GDPR), if an organisation is a controller in respect of personal data (i.e. it determines how and why personal data is processed) it will be required to implement appropriate technical and organisational measures to ensure a level of security of that personal data appropriate to the risk, including the risk of accidental or unlawful disclosure of, or access to, that personal data. Controllers are also required to document any personal data breaches.

The NIS Regulations also require operators of essential services and digital service providers to take appropriate and proportionate technical and organisational risk management measures, including to prevent and minimise the impact of Incidents.

Under PECR, a public electronic communications service provider must take appropriate technical and organisational measures to safeguard the security of its service and maintain a record of all Incidents involving a personal data breach in an inventory or log. This must contain the facts surrounding the breach, the effects of the breach and the remedial action taken by the service provider.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Data Protection Act 2018 and UK GDPR

Under the Data Protection Act 2018 and the UK GDPR, a controller will be required to notify an Incident involving personal data to the ICO without undue delay and, where feasible, within 72 hours after becoming aware of it, unless it is unlikely to result in risks to individuals. This notification must include: (a) a description of the nature of the Incident; (b) the name and contact details of the organisation's data protection officer or contact point; (c) the likely consequences of the Incident; and (d) the measures taken, or proposed to be taken, to address the Incident and mitigate possible adverse effects.

Under the Data Protection Act 2018, the ICO is not permitted to publicise any information that has been disclosed to it (e.g. through notification of an Incident) if that information relates to an identified or identifiable individual or business and is not already in the public domain. However, this restriction on publication will not apply in certain cases, such as if the ICO determines that publication is in the public interest. The ICO's practice is not to publicise data breach notification information unless it has taken public enforcement action in relation to the breach, or publication is necessary in the public interest (e.g. to allay public concern).

NIS Regulations

The NIS Regulations also require OES and RDSPs to report Incidents to the relevant competent authority without undue delay. The relevant authority may inform the public where public awareness is needed either to prevent or resolve the Incident, or where this would otherwise be in the public interest, but the organisation will be consulted before disclosure to the public is made to preserve confidentiality and commercial interests.

The NCSC publishes a weekly threat report on its website, with content drawn from recent open source reporting, which details cyber threat information, known network and software vulnerabilities and other information organisations and individuals may find useful. However, there is no obligation for organisations to report threat information to the NCSC to compile these reports.

Communications Act 2003

The Communications Act 2003 requires public electronic communications network providers to notify Ofcom of any breach of security that has a significant impact on the network's operation. It also requires public electronic communications service providers to notify Ofcom of any breach of security that has a significant impact on the operation of the service.

PECR

PECR requires a public electronic communications service provider to notify the ICO of a data breach within 24 hours of becoming aware of the "essential facts" of the breach. The notification must include: (a) the service provider's name and contact

details; (b) the date and time of the breach (or an estimate) and the date and time of detection; (c) information about the nature of the breach; and (d) the nature and content of the personal data concerned and the security measures applied to it.

FCA and PRA Handbooks

An organisation regulated by the FCA are also required to notify the FCA of any significant failure in its systems and controls under Chapter 15.3 of the Supervision Manual of the FCA and PRA Handbooks, which may include Incidents that involve data loss. Similarly, the FCA expects payment service providers to comply with European Banking Authority guidelines on major Incident reporting under which those providers are expected to report major operational or security Incidents to the competent authority within four hours from the moment the Incident was first detected, with intermediate updates and a final report delivered within two weeks after business is deemed to have returned to normal.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under the Data Protection Act 2018 and the UK GDPR, a controller will be required to notify affected individuals of an Incident without undue delay if the Incident involves personal data and is likely to result in a high risk to the rights and freedoms of those individuals. This notification must include: (a) a description of the nature of the Incident; (b) contact details where more information can be found; (c) the likely consequences of the Incident; and (d) the measures taken, or proposed to be taken, by the organisation to address the Incident and mitigate possible adverse effects.

Under PECR, a public electronic communications service provider must notify its affected subscribers or users of an Incident without unnecessary delay if that Incident is likely to adversely affect their personal data or privacy. The service provider should provide a summary of the Incident, including the estimated date of the breach, the nature and content of personal data affected, the likely effect on the individual, any measures taken to address the Incident and information as to how the individual can mitigate any possible adverse impact. No notification is required if the service provider can demonstrate to the ICO's satisfaction that the personal data that has been breached was encrypted or was rendered unintelligible by similar security measures.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

- The **ICO** is the relevant regulator under data protection laws, including the Data Protection Act 2018, the UK GDPR and PECR (https://ico.org.uk/).
- **Ofcom** is the relevant regulator under the Communications Act 2003 (https://www.ofcom.org.uk/).
- The **FCA** is the relevant regulator under the FCA Handbook (https://www.fca.org.uk/). The **PRA** is also responsible for the regulation and supervision of financial services firms.
- **Sector-based competent authorities** are the relevant regulators in Schedule 1 to the NIS Regulations (https://www.legislation.gov.uk/uksi/2018/506/schedule/1/made).

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

- Data Protection Act 2018 and the UK GDPR – failure to report an Incident involving a personal data breach, or to implement appropriate security measures, can incur a fine of up to the higher of 2% of annual worldwide turnover or €10 million.
- PECR – failure by a public electronic communications service provider to notify an Incident involving a personal data breach to the ICO can incur a £1,000 fixed fine. A failure by a public electronic communications service provider to take appropriate technical and organisational measures to safeguard the security of their service can incur a fine of up to £500,000 from the ICO.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In July 2019, in the first fine to be announced by the ICO under the UK GDPR, the ICO announced an intention to issue a fine of £183.39 million to British Airways following an Incident in September 2018. This Incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers was compromised in this Incident, which is believed to have begun in June 2018.

Also in July 2019, the day after the announcement of the British Airways fine, the ICO announced further plans to fine Marriott International £99.2 million following a data breach affecting Marriott subsidiary Starwood's guest reservation database. A variety of personal data contained in approximately 339 million guest records globally were exposed by the Incident, of which 7 million related to UK residents. It is believed the relevant vulnerability began in 2014, but was not discovered until 2018. The ICO found that Marriott failed to undertake sufficient due diligence when it bought the Starwood hotels group in 2016, and should have done more to secure its systems.

Both British Airways and Marriott had the opportunity to make further representations to the ICO. It is expected that the fines issued will ultimately be lower than those stated in 2019, but at the time of writing, no further update has been announced by the ICO.

In January 2020, the ICO issued a fine of £500,000 to DSG Retail Limited after security failings enabled malware to be installed by an attacker on 5,390 tills at DSG's Currys, PC World and Dixons Travel stores between July 2017 and April 2018 resulting in unauthorised access to the personal information of approximately 14 million people – this incident occurred prior to the introduction of the UK GDPR and the fine represents the maximum penalty available under the Data Protection Act 1998.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There are no specific laws prohibiting the use of web beacons in the UK. However, where use of a web beacon involves processing personal data, the organisation's use of the web beacon must be in accordance with the requirements of data protection laws.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are no specific laws prohibiting the use of honeypots in the UK.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are no specific laws prohibiting the use of sinkholes in the UK.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Monitoring of employees, e.g. monitoring use of email and internet access, involves processing of personal data and so the Data Protection Act 2018 (and the UK GDPR) will apply. The ICO's Employment Practices Code (the **Code**) contains guidance on monitoring employees at work. The Code states that employees still have an expectation of privacy, and so monitoring should be justified, proportionate, secured and that organisations should undertake an impact assessment and ensure that the employees are notified that monitoring will take place. A failure to comply with the Code will not automatically result in a breach of the UK GDPR or the Data Protection Act 2018. However, an organisation should be able to justify any departure from the Code, and the ICO can take this into account in consideration of any enforcement action.

Under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, an organisation may lawfully monitor and record communications without consent to: (a) ascertain compliance with regulatory practices or procedures relevant to the business; (b) ascertain or demonstrate standards which ought to be achieved by employees using the telecommunications system; (c) prevent or detect crime; (d) investigate or detect unauthorised use of the telecommunications system (such as detecting a potential Incident); and (e) ensure the effective operation of the telecommunications system.

The Investigatory Powers Act 2016 amends some of the legislation relating to a business's ability to record telephone calls with its employees, but the operative provisions are not yet in force.

The Human Rights Act 1998 and, in particular, the right to respect for private and family life, home and correspondence, must also be considered and balanced against obligations on the organisation to implement appropriate security measures in respect of potential Incidents.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There are no specific restrictions on the import or export of technology designed to prevent or mitigate the impact of cyber-attacks.

However, export authorisation is required for the export of certain technology or software (e.g. decryption technology) that is used for or in connection with, or required for the development, production, or use of, certain explosives, aircraft, firearms, chemicals and vessels.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Certain sectors, such as financial services and telecommunications, are more incentivised to avoid the cost and reputational impact of Incidents. In some organisations, cybersecurity practice is driven not only by compliance with Applicable Laws but also the desire to promote good "cyber hygiene" culture. For example, although there is no legal requirement to train employees in cyber risks, many organisations do and may carry out simulations (such as phishing simulations and "war games") as a matter of good practice.

Public sector organisations (such as the National Health Service) and government authorities are subject to additional reporting guidelines issued by the central government, in addition to disclosure obligations under Applicable Laws.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Under SYSC 3.2.6R, regulated financial services organisations are required to take reasonable care to establish and maintain effective systems and controls for compliance with regulatory requirements and standards and for countering risk that the organisation may be used to further financial crime. Further, under SYSC 3.1.1R, the organisation is required to maintain adequate policies and procedures to ensure compliance with those obligations and countering those risks. These requirements extend to cybersecurity issues. For example, the FCA has previously fined Tesco Bank (£16.4 million) and three HSBC firms (£3 million) for failure to have adequate systems and controls in place to protect customer confidential information and manage financial crime risk.

In the telecommunications sector, public electronic communications network providers and public electronic communications service providers must take appropriate technical and organisational measures to manage risks to the security of the networks and services, including to minimise the impact of Incidents. Public electronic communications network providers must also take all appropriate steps to protect, so far as possible, the availability of that provider's network.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

A failure to prevent, mitigate, manage or respond to an Incident may be a breach of directors' duties if, for example, the failure resulted from a lack of skill, care and diligence on the part of the relevant director. Directors are required, under the Companies Act 2006, to promote the success of the company for the benefit of its members as a whole and exercise reasonable skill, care and diligence in performing their role. It is up to the board of directors of each company to ensure that the board has the relevant competence and integrity to exercise these duties in view of the risk to the company as a whole, including the risk of Incidents.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

No, there are no specific requirements in this respect. However, listed companies are required, under the UK Corporate Governance Code, to set up certain committees with responsibility for specific areas, such as audit. Financial services companies may also be required to have a risk committee. These committees may, as part of their functions, conduct risk assessments that cover cyber risk. The UK Corporate Governance Code, as applicable from 1 January 2019, emphasises the board's responsibility to determine and assess the principal risks facing the company. This responsibility extends to a robust assessment of the company's emerging risks, which would cover cyber risk.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Under the Disclosure and Transparency Rules set out in the FCA Handbook, listed companies are required to disclose an Incident if the Incident amounts to inside information that may affect the company's share price. For example, theft of business-critical intellectual property is likely to be price-sensitive information.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

There are a number of potential civil actions that may be brought in relation to any Incident, for example:

- **Breach of confidence.** Where there is unauthorised disclosure or use of information and: (i) the information itself had a necessary quality of confidence about it; (ii) that information was imparted in circumstances importing an obligation of confidence; and (iii) there was an unauthorised use of that information to the detriment of the party communicating it.
- **Breach of contract.** This could take any form, including a breach of a commercial contract or breach of an employee's terms and conditions of employment. For example, if a party has contractually agreed or warranted that it complies with an ISO standard, a failure to do so will be a breach of contract.
- **Breach of trust.** A person who owes a fiduciary duty to another may not place him or herself in a situation where they have a personal interest that may conflict with the interest of the person to whom the fiduciary duty is owed. If an Incident is caused by an employee or a director, a breach of trust/fiduciary duty may be claimed. Dishonest assistance may be claimed where there is a fiduciary relationship and dishonest assistance has been given by a third party to the breach of trust.
- **Causing loss by unlawful means.** A defendant will be liable for causing loss by unlawful means where they intentionally cause loss to the claimant by unlawfully interfering in the freedom of a third party to deal with the claimant.
- **Compensation for breach of the Data Protection Act 2018 (and UK GDPR).** Individuals who suffer "material or non-material damage" by reason of any contravention, by a data controller, of any requirements of the Data Protection Act 2018 (including the UK GDPR) are entitled to compensation for that damage. "Non-material damage" includes distress. This does not require the claimant to prove pecuniary loss.
- **Conspiracy.** The economic tort of conspiracy requires there to be two or more perpetrators who are legal persons who conspire to do an unlawful act, or to a lawful act but by unlawful means.
- **Conversion** is a tort that may cover unauthorised interference with personal information and other property.
- **Deceit.** There are four elements: (i) the defendant makes a false representation to the claimant; (ii) the defendant knows that the representation is false or is reckless as to whether it is true of false; (iii) the defendant intends that the claimant should act in reliance on it; and (iv) the claimant does act in reliance of the representation and suffers loss as a consequence.
- **Directors' duties.** See answer to question 4.1.
- **Infringement of copyright and/or database rights.** Copyright is infringed when a person, without authority, carries out an infringing act under the Copyright, Designs and Patents Act 1988, such as copying the work or communicating the work to the public. Database rights are infringed if a person extracts or re-utilises all or a substantial part of a database without the owner's permission.
- **Misuse of private information.** Similar to a breach of confidence, but removing the need for the claimant to establish a relationship of confidence. The cause of action may be better described as a right to informational privacy and to control dissemination of information about one's private life.
- **Negligence** may be claimed where the defendant owed a duty of care to the claimant, breached that duty of care and that breach caused the claimant to suffer a recoverable loss.
- **Trespass** is the intentional or negligent interference with personal goods. A deliberate attempt through the internet unlawfully to manipulate data on a computer may amount to trespass to that computer.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

The following are illustrations of cases that have been brought that can be said to relate to Incidents.

Breach of confidence and various economic torts

Ashton Investments Ltd v OJSC Russian Aluminium (Rusal) [2006] EWHC 2545 (Comm): there was a good arguable case justifying service out of the jurisdiction, in respect of claims for breach of confidence, unlawful interference with business, and conspiracy where a computer server in London had allegedly been improperly accessed from Russia and confidential information and privileged information had been viewed and downloaded.

Contract

Bristol Groundschool Ltd v Intelligent Data Capture Ltd [2014] EWHC 2145 (Ch): a contract relating to the development of computer-based pilot training materials was a "relational" contract containing an implied duty of good faith. One party had behaved in a commercially unacceptable manner in accessing the other party's computer and downloading information, but its conduct was not repudiatory.

Frontier Systems Ltd (t/a Voiceflex) v Frip Finishing Ltd [2014] EWHC 1907 (TCC): an internet telephony provider's customer whose computer network had been hacked was not liable to pay the bill incurred by unauthorised third parties.

Trespass

Arqiva Ltd & Ors v Everything Everywhere Ltd & Ors [2011] EWHC 1411 (TCC): obiter reference to Clerk & Lindsell on Torts (20th Edition) at paragraphs 19-02 and 17-131. At paragraph 19-02, the authors state the proposition that "one who has the right of entry upon another's land and acts in excess of his right or after his right has expired, is a trespasser". At paragraph 17-131, the authors refer to "Cyber-trespass" and say that "[w]hile the definition of corporeal personal property may normally be straightforward, questions may nevertheless arise in a number of borderline cases, in particular in respect of electronic technology. For example, it is hard to see why a deliberate attempt through the internet unlawfully to manipulate data on a computer should not amount to trespass to that computer".

Compensation for breach of the Data Protection Act 2018 (and UK GDPR)

Wm Morrisons Supermarket PLC v Various Claimants [2020] UKSC 12: although determined under the previous legislation, in the first group litigation data breach case to come before the courts, Morrisons Supermarket was, following an appeal, found not to be vicariously liable for a deliberate data breach carried out by a rogue employee, out of working hours and at home on a personal computer. The ICO had, separately, concluded an investigation into the data breach and found that Morrisons had discharged its own obligations as required under the Data Protection Act 1998 and common law. At first instance, the court concluded that Morrisons had no primary liability in respect of the breach, but there was nonetheless a sufficient connection (as the rogue employee accessed the data in question in the course of his employment) for Morrisons to have vicarious liability. However, this position was overturned on appeal to the Supreme Court.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Please see the list in response to question 6.1.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement authorities have various surveillance powers under UK laws. For example, the Police Act 1997 authorises covert entry into and interference with communications systems by the police, and similar powers are available to the security services under the Security Service Act 1989 and the Intelligence Services Act 1994.

Other powers of surveillance and interception of communications data are subject to RIPA. Under RIPA, the Secretary of State can issue an interception warrant if this is necessary for the prevention or detection of serious crime (amongst others), provided this is proportionate and the information could not reasonably be obtained by other means. Under the Investigatory Powers Act 2016, new warrants are available for targeted equipment interference and targeted examination, as well as bulk warrants to enable law enforcement to obtain the communications data of multiple individuals using one warrant.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Under RIPA, telecommunications service providers are required to give effect to an interception warrant to assist law enforcement. The Secretary of State may issue a notice to a specified service provider detailing the measures that the service provider must implement to establish an interception capability.

The Investigatory Powers Act 2016 includes provision for the Secretary of State to require some telecommunications operators to install permanent interception capabilities through "technical capability notices". These notices will require approval by a Judicial Commissioner, but may include equipment interference, interception capability (such as removal of electronic protection applied to data) and disclosure of data. These provisions of the Investigatory Powers Act 2016 are not yet fully in force (at the time of writing), but there is some uncertainty over whether these notices could prevent a telecommunications operator from providing end-to-end encryption capabilities to end users.

Nigel Parker is a partner specialising in intellectual property, data protection and privacy, commercial contracts and IT law. He is a member of the firm's Cyber Security Group and has advised clients on strategies for managing legal risk in relation to cybersecurity, including the deployment of a variety of risk management tools, on the response to attacks and dealing with regulatory authorities, and on taking pro-active steps in response to attacks.
Nigel is recognised in *Chambers* and *The Legal 500*. He was named one of the "Top 40 under 40" data lawyers by *Global Data Review*.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3136
Email: nigel.parker@allenovery.com
URL: www.allenovery.com

Nathan Charnock is an associate specialising in commercial contracts, data protection and privacy, intellectual property and information technology law. He advises clients on their response to cybersecurity attacks, including their interactions with regulators and implementation of remediation steps. Nathan also advises on complex commercial arrangements for a range of clients in the technology, retail, telecommunication, life sciences and financial services sector, including IP licensing, outsourcing and service provision arrangements.

Allen & Overy LLP
One Bishops Square
London E1 6AD
United Kingdom

Tel: +44 203 088 3899
Email: nathan.charnock@allenovery.com
URL: www.allenovery.com

Allen & Overy is a full-service global elite law firm headquartered in London. Our commitment to help our clients deliver their global strategies has seen us build a truly global network now spanning over 40 offices. We have also developed strong ties with relationship law firms in more than 100 countries where we do not have a presence.
We have a strong cybersecurity practice comprising a core team of 19 partners with diverse backgrounds in data protection, bank regulation, anti-trust, securities laws, technology, IT, litigation, employment, IP and corporate. This spread is crucial because cybersecurity Incidents frequently span a wide range of traditional legal practice areas. There is an important legal component to cybersecurity and our integrated team of diverse practitioners reflects this requirement. As a full-service global elite law firm, we are able to advise clients on all legal issues concerning cybersecurity.

www.allenovery.com

ALLEN & OVERY

France

Stehlin & Associés

Frédéric Lecomte

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking is a criminal offence pursuant to article 323-1 of the French Criminal Code ("**FCC**") relating to unauthorised access to an automated data processing system. The punishment for fraudulent access into an automated data processing system is imprisonment and a fine of up to €60,000. When data is modified or suppressed as a result of the unauthorised access, the sanction is three years of imprisonment and a fine of up to €100,000. When the offence is committed in a public or governmental system, the sanction is raised to five years of imprisonment and a fine of up to €150,000.

Denial-of-service attacks
Article 323-2 of the FCC sanctions the impeding or slowing down of an information system. Any kind of obstruction falling within the perimeter of article 323-2 is punishable by five years of imprisonment and a fine of up to €150,000. When the offence involves a public or governmental system, the sanctions are raised to seven years of imprisonment and a fine of up to €300,000.

Phishing
Phishing is sanctioned by the following articles of the FCC and of the Intellectual Property Code: (i) the collection of data by fraudulent, unfair or unlawful methods is sanctioned by article 226-18 of the FCC with five years of imprisonment and a fine of up to €300,000; (ii) the theft and use of a third-party identity is sanctioned by article 226-4-1 of the FCC by one year of imprisonment and a fine of up to €15,000 – the applied sanction is cumulative with the sanctions applied pursuant to (i) above; (iii) the fraud or swindle is sanctioned by article 313-1 of the FCC with five years of imprisonment and a fine up to €375,000; (iv) unauthorised introduction of data in a system, the extraction, reproduction, transmission and use of data stored in this system is sanctioned by article 323-3 of the FCC with five years of imprisonment and a fine of up to €150,000; and (v) phishing can result in an infringement of intellectual property rights, in particular on the basis of articles L.335-2, L.713-2 and L.713-3 of the French Intellectual Property Code. The owner of the reproduced or imitated website or trademark can sue the phisher for the use of his trademark on the basis of infringement. This offence is sanctioned with three years of imprisonment and a fine of up to €300,000.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
This offence can by sentenced pursuant to article 323-1 of the FCC (*see Hacking*) but also pursuant to article 323-2 of the FCC (*see Denial-of-service attacks*) and pursuant to article 323-3 of the FCC (*see Phishing*).

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
(*See Possession or use of hardware.*)

Possession or use of hardware, software or other tools used to commit cybercrime
Pursuant to article 323-3-1 of the FCC, the act consisting of, without a legitimate motive (in particular for research or computer security), importing, holding, offering, transferring or making available equipment, instruments, computer programs or any data designed or specially adapted to commit one or more offences mentioned in articles 323-1 to 323-3 of the FCC (*see Hacking, Denial-of-service attacks and Phishing*) is punished with the most severe sanctions.

Identity theft or identity fraud (e.g. in connection with access devices)
Pursuant to article 226-4-1 of the FCC, the act of usurping the identity of a third party is punishable by one year of imprisonment and a fine of up to €15,000.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
The offence of theft pursuant to the FCC (article 311-1) has been extended to computer theft by French courts. French judges now consider computer data (i.e. dematerialised information), as constituting goods likely to be stolen.

Under French law, theft is punishable by three years of imprisonment and a fine of up to €45,000.

Article 226-18 of the FCC as well as articles L.335-2, L.713-2 and L.713-3 of the French Intellectual Property Code (*see Phishing*) could also be used in some circumstances.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Insofar as the owner of the IT is not aware of or has not authorised the penetration testing, this could be punished as hacking or a denial-of-service attack (*see Hacking, Denial-of-service attacks*).

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Article L.66 of the French Post and Electronic Communications Code imposes sanctions of two years of imprisonment and a fine of up to €3,750 for any person who, by breaking wires, damaging equipment or by any other means, deliberately interrupts electronic communications.

Attacks on the fundamental interests of the nation committed by means of information technologies are punished by numerous provisions of the FCC. For example, pursuant to article L.413-10 of the FCC, the destruction, misappropriation, subtraction, reproduction of the defence secrecy or the giving of access to an unauthorised person or making it available to the public, is sentenced to seven years of imprisonment and a fine of up to €100,000.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Pursuant to article 113-2-1 to the FCC, any crime or offence committed by means of an electronic communication network is deemed to have been committed on the territory of the Republic when it is attempted or committed to the detriment of a natural person residing in the territory of the Republic or a legal person whose registered office is in France.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Article L. 2321-4 of the Defence Code provides protection to any "ethical hacker" who informs the French National Cybersecurity Agency ("**ANSSI**") are informed of the existence of a vulnerability concerning the security of an automated data processing security. The ANSSI notifies the relevant organisation while protecting the confidentiality of the identity of the person who reported the vulnerability. Moreover, an offence will only be sanctioned by a court pursuant to the FCC if the intentional nature of the offence results from the facts or is demonstrated by the prosecutor. Pursuant to the GDPR as applied under French law, the lack of intentional motivation, all measures taken by the controller or the processor to mitigate the damage suffered by the data subjects, and/or the degree of cooperation to remedy the breach are considered positive behaviour and may reduce the level of administrative sanctions.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The most important laws in the cybersecurity domain are (without being exhaustive):

- The Godfrain Law (*n°88-19 of January 15, 1988*).
- The FDPA (*Loi Informatique et Libertés n°78-17 of January 6, 1978*) successively amended by two laws: Law *n° 2004-575 of June 21, 2004* and finally amended by the *Law n°2018-793 of June 20, 2018* transposing the GDPR and the ordinance 2018-1125 of December 12, 2018.
- The Law for a Digital Republic *n°2016-1321 of October 7, 2016* and recently amended by the law transposing the GDPR (*Law n°2018-493 of June 20, 2018*).
- The Network and Information Systems Security Act ("**NIS Act**") transposing the NIS Directive *n°2018-133 of February 26, 2018* completed by the Decree *n°2018-384 of May 23, 2018* which details the application of the NIS Act and lists the sectors, types of operators and critical infrastructures concerned, and the Decree of September 14, 2018 defining the security rules (together the "**NIS Rules**").

In addition to the above-mentioned law, the following texts have adapted the criminal law to certain forms of cybercrime and creating specific investigative means such as:

- The Law on Daily Security (known as LSQ *n°2001-1062 of November 15, 2001*), the Law on Internal Security (*n°2003-239 of March 18, 2003*).
- The law adapting the judiciary to developments in crime (*n°2004-204 of March 9, 2004*), the Law on Copyright in the Information Society (known as *David's Law of August 1, 2006, n°2006-961*).
- The Law OPSI II (*n°2011-267 of March 14, 2011*).
- The Law strengthening the provisions on the fight against terrorism (*n°2014-1353, of November 13, 2014*).
- The Law strengthening the fight against organised crime and terrorism (*n°2016-731, of June 3, 2016*).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

In France, critical infrastructures identified as such by the law (*Law n°2013-1168 of December 18, 2013, Law n°2016-41 of January 26, 2016, NIS Act*) must comply with specific legal requirements. This is mostly the case for the following infrastructures:

- Professionals subject to the obligation of professional secrecy. For instance, pursuant to article 1111-8-2 of the French Public Health Code, healthcare institutions as well as bodies and services carrying out prevention, diagnosis or care activities shall report without delay serious information system security Incidents to the Regional Health Agency.
- Operators for essential services ("**OES**") which, pursuant to the NIS Rules are designated by the Prime Minister in various sectors, such as Energy, Transportation, Banking, Financial Markets Infrastructures, Health and Digital Infrastructures. In that regard, the French NIS Rules added specific sectors to the list defined in the Directive such as: insurance; pharmaceutical retailing; and collective catering. The OES shall be designated by an order of the Prime Minister. The OES shall appoint a representative that will be the point of contact of the ANSSI. By November 2018, France had already identified 122 EOS.
- Digital service providers ("**DSP**"). Pursuant to the NIS Rules, these infrastructures must appoint a representative established on the national territory of the ANSSI if it is established outside the European Union and does not have any representative within the European Union.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Pursuant to the GDPR, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the identified risk.

Pursuant to article 57 of the FDPA, the controller (and processor) are required to take all necessary precautions, having regard to the nature of the data and the risks associated with the processing, to preserve the security of the data and, in particular, to prevent it from being distorted, damaged or accessed by unauthorised third parties.

The NIS Rules also require OES and DSP to:

- carry out and maintain a list of networks and information systems necessary for the provision of the essential/digital services;
- identify the risks threatening the security of the information systems;
- guarantee an appropriate level of security according to the existing risks and implement technical and organisational measures necessary and proportionate to prevent, manage and reduce these risks;
- avoid Incidents and minimise their impact so as to guarantee the continuity of their services; and
- identify the IT security risks that may affect their activities.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

The GDPR (article 33) provides for an obligation for all data controllers to notify any Incidents to the competent data controlling body unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. This notification to the data protection authority ("**CNIL**") must take place within 72 hours of the discovery breach and must contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects, a detailed description of the measures taken to remedy or mitigate negative effects, the name and contact details of the data protection officer, and describe possible harmful consequences of the unlawful access and measures taken by the controller.

The FDPA (article 83) specifically concerns DSP and provides for an obligation to notify any data breach to the CNIL immediately and without conditions. The information to be communicated is rather similar to the above mentioned.

The NIS Rules also require OES and DSP to notify the ANSSI "without undue delay" any Incident when it has or is *likely to have* a significant impact on the continuity of services.

As regards the reporting procedures, organisations must provide the ANSSI by electronic means or by mail, with an Incident reporting form available on its website. This form includes information on the reporter, the network information system affected by the Incident, the consequences of the Incident on the services concerned, the type of Incident, its causes and the measures taken to respond to it.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Pursuant to the GDPR and the FDPA, a controller must inform each affected individual of an Incident if the breach may create a high risk to the rights and freedoms of affected individuals (article 58 of the FDPA and 34 GDPR).

The information must detail the name and contact details of the data protection officer ("**DPO**") and describe in clear and plain language (i) the nature of the Incident, (ii) the likely consequences of the Incident, and (iii) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Pursuant to NSI Rules, OES and DSP only are required to report Incidents to the ANSSI.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The CNIL controls the proper application of the FDPA and the GDPR by data controllers and processors. It also gives opinions on legislative drafts or regulatory texts. The CNIL has important powers of control and investigation.

Finally, the CNIL has significant administrative and financial penalty powers and can take decisions such as the temporary or permanent suspension of data processing.

For application of the NIS Rules, the ANSSI is the national authority responsible for replying to cybersecurity Incidents targeting strategically important institutions (https://www.ssi.gouv.fr).

The Ministry of Defence and the Ministry of the Interior also assume functions of prevention of all forms of cybercrime.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Depending on the nature of the offence, the penalty may vary between €10 million or 2% of the worldwide turnover, and €20 million or 4% of the worldwide turnover.

OES and DSP may be subject to the following fines:

- €100,000 (€75,000 for DSP) in case of non-compliance with security rules.
- €75,000 (€50,000 for DSP) in case of failure to communicate a cybersecurity Incident.
- €125,000 (€100,000 for DSP) in case of obstruction of inspection operations.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Since the entry into force of the GDPR, the CNIL has sanctioned several companies. The CNIL fined Google LLC €50 million for lack of transparency, unsatisfactory information and lack of valid consent for the customisation of advertising.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Insofar as beacons have the same purposes, and are deemed to be cookies, their use is legal provided such use complies with cookie legislation.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Under French law, loyalty of evidence production is material to the fairness of trial. Therefore, the law distinguishes between active and passive provocation to commit an offence. Honeypots should be considered legal if used as passive traps to detect cyber threats. The French Cour de Cassation in a decision of 30 April 2014 stated that there had been no provocation to commit the offence in a case where the FBI had created a surveillance site to gather evidence of the commission of credit card fraud.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Operating a sinkhole may not be compliant with the GDPR obligations insofar as some personal data could be collected without the consent of the computer's user and sent to the sinkhole. There is also a risk of collateral damage.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

The CNIL considers the monitoring of employees is possible. The employer can control and limit the use of the internet (site filtering devices, virus detection, etc.) and email (tools for measuring the frequency of messages sent and/or the size of messages, "anti-spam" filters, etc.) provided that (i) prior information and consultation of the employee representative committee has been carried out, and (ii) employees have been individually informed. The monitoring must be proportionate, i.e. respect the balance between the employee's privacy and the employer's power of control.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

In France, encryption mediums are subject to specific regulations. The use of a means of cryptology is free. However, the sale, supply, import, intra-community transfer and export of an encryption medium are subject, except in listed cases, to a declaration or a request for authorisation depending on the technical functionalities of the means and the planned commercial operation. Decree n° 2007-663 of 2 May 2007 lists which technology is subject to the declaration or authorisation process. The supplier is responsible for carrying out the declaration or request for authorisation with the ANSSI.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The measures to be implemented are stronger in some business areas. This is particularly the case for critical infrastructures which must comply with the NIS Rules (see question 2.2), or for infrastructures that process sensitive data (for example, health data or data relating to criminal sentences, offences or security measures). Also, as mentioned above (see question 2.2), companies who host personal health data must be accredited for this purpose.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

The legal requirements related to cybersecurity in the following two sectors are as follows:

(a) The financial services sector must comply with several requirements such as auditing IT systems, strengthening resistance to cyber risks, developing defences adapted to the complexity of cyber-attacks, and making several declarations to the ANSSI (ministerial orders of November 28, 2016).

(b) Pursuant to article L.33-1 of the French Post and Electronic Communications Code, companies in the telecommunication sector must comply with rules relating to the conditions of permanence, quality, availability, security and integrity of the network and service, which include obligations to notify to the competent authority breaches to the security or integrity of networks and services.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Beyond the company's responsibility in case of failure of the IT system (see question 2.10), the company manager (i.e. in France, it is the representative of the company who has the power to bind the company, e.g.: president; CEO; and general manager) is

liable under civil law towards the company and its shareholders of (i) breach of the laws and regulations or of the bylaws, and (ii) mismanagement (article 1850 of the Civil Code). Moreover, the company manager can be liable because of the behaviour of his employees if such behaviour results in damage to a third party (article 1242 paragraph 5 of the French Civil Code). Finally, pursuant to the FCC and the French Commercial Code, numerous French provisions specifically make the company manager subject to personal criminal liability.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Please see below the Applicable Law requirements:

(a) There are no general obligations, so far, to designate a CISO. However, the GDPR sets out the obligation to appoint a DPO when (i) the data processing is carried out by a public authority or public body, (ii) the data processing requires regular and systematic monitoring on a large scale, and (iii) in cases of large-scale processing of sensitive data.

(b) For critical infrastructures, the NIS Rules set out the obligation to establish, maintain and implement a network and information system security policy ("**ISSP**"). The ISSP describes all procedures and organisational and technical means implemented by the operator to ensure the security of its essential information systems. The operator shall also maintain a crisis management procedure in the event of major cyber-attacks. For other companies, there are no general obligations to establish a written Incident response plan or policy.

(c) For critical infrastructures, the NIS Rules imposes on the OES to carry out and maintain a risk analysis of its essential information systems. Pursuant to the FDPA, the controller and the processor must carry out a risk assessment in order to implement measures to protect data processing systems. Moreover, pursuant to article 1110-4-1 of the French Public Health Code, health professionals, healthcare institutions and services must use information systems for the processing of health data, their storage on electronic media and their transmission by electronic means, in accordance with interoperability and security standards in order to guarantee the quality and confidentiality of personal health data and their protection.

(d) For critical infrastructures, the NIS Rules impose audits to assess the level of security of information systems with regard to known threats and vulnerabilities. For other companies, French law strictly applies the GDPR according to which the controller and the processor must implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (article 32.1.d).

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Pursuant to article L.225-100-1 of the French Commercial Code and article 222-3 of the General Regulations of the French Financial Markets Authority, listed and private companies must draw up an annual management report which contains a description of the main risks and uncertainties the company had to face or is facing (which implicitly includes cyber risks). Pursuant to article L.451-1-2 of the French Commercial Code, listed companies are required to submit this report to the French Financial Markets Authority and to publish it on their website.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Under French law, the general rule of civil liability is set forth under article 1240 of the French Civil Code, pursuant to which any act which causes damage to another shall oblige the person by whose fault it occurred to repair it (i.e. three elements are necessary to engage liability: (i) a fault; (ii) a damage; and (iii) a causal link between the two). Moreover, under the GDPR (article 79), a civil action may be brought in the event of an Incident if the controller or the processor have not complied with the GDPR requirements. Finally, under the FDPA, the data subject shall have the right to mandate a not-for-profit body, organisation or association to stop the breach and to obtain compensation (article 37).

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

For example, a woman was penalised in civil and criminal terms by the Chambéry Court of Appeal on November 16, 2016 for the possession of hacking data.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

See the answers to questions 6.1 and 6.2 above

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Cyber risk is partially covered by traditional insurance contracts which cover certain foreseeable consequences of certain computer threats (e.g. insurance contracts covering damage to property and civil liability). The emergence of new risks from the evolution of technologies and the increase in their uses requires the implementation of appropriate legal frameworks. To cope with these new risks, insurers have developed a new contract: the cyber contracts; which is a multi-risk contract cover for damage (costs and losses incurred); liability (non-material damage to third parties); and management services of crises.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Pursuant to article L.113-1 of the French Insurance Code, the insurer does not cover loss or damage resulting from the insured's intentional or wilful misconduct. In addition, criminal sanctions are not insurable because they are regarded as personal sanctions. Moreover, there is still a debate about the possibility to insure administrative or financial sanctions to the extent they are not the result of intentional misconducts. The authors opine that this risk should be insurable.

On the subject of terrorism and cyberterrorism, the French Public Purse stated that "insurance contracts whose purpose is to guarantee the payment of a ransom to Daech, as to any terrorist entity, are prohibited".

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In France, there are many police services specialising in cybersecurity. For example: the PICyAN (cybercrime investigation platform and digital analysis), which analyses IT equipment seized during police searches and internet surveillance thanks to special software; the C3N (Digital Crime Centre) whose mission includes judicial investigations and criminal intelligence; the BEFTI (Information Technology Fraud Investigation Brigade), which operates only in Paris and the surrounding suburbs and which is responsible for managing any breaches of the data processing system, software counterfeiting and classic offences such as fraud; and the OCLCTIC (Central Office for the Fight against Information and Communication Technologies Crime), which ensures the legality of published content on Internet and ordering providers to remove illegal content.

The police services mentioned above may carry out investigations, searches, interceptions, data collection, geolocation, wiretapping, infiltration, and arrest and detain suspects in police custody.

In addition, in order to ensure the effective application of the FDPA, the CNIL has the power to carry out extensive controls on all data controllers and processors. The ANSSI can also carry out controls on OES's facilities.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There is no obligation to set up backdoors. However, the administrative and judicial authorities may require the submission of encryption keys. Pursuant to article L.871-1 of the French Internal Security Code, natural or legal persons who provide encryption services aimed at ensuring a confidentiality function are required to submit within 72 hours to authorised agents (i.e. administrative and judicial authorities), at their request, agreements enabling the decryption of data transformed by means of the services they have provided.

Frédéric Lecomte has been a member of the Paris Bar since 1989. Frédéric joined Stehlin & Associés in 1993 after having spent five years at Coudert Brothers in Paris. He became a partner in 1998.
Frédéric is the author of numerous articles in relation to technology law and is the author of a book about the GDPR *Nouvelle Donne Pour les Données* (Fauve Editions, 2018).
Practice areas: new technologies and data law; intellectual property; contract law and trade; and distribution law.

Stehlin & Associés
48 avenue Victor Hugo
Paris, 75116
France

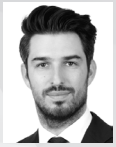
Tel: +33 1 44 17 07 70
Fax: +33 1 44 17 07 77
Email: f.lecomte@stehlin-legal.com
URL: www.stehlin-legal.com

The firm's attorneys work together in a pragmatic way to implement their projected operations and solve problems encountered by clients, both in their day-to-day business as well as in specific transactions. With an international outlook from the beginning of its existence, the firm has numerous contacts with firms throughout the world. Since 2012, the firm has been the French member of the Mackrell International network, which is ranked among the top law firm networks in *Chambers* 2020, having a presence in 60 countries and 170 cities, and providing access to more than 4,500 attorneys. Our team assists its clients in the new technologies and intellectual property fields, which include copyright and neighbouring rights, industrial property rights, the internet and new technologies rights and privacy law.

www.stehlin-legal.com

Germany


Dr. Alexander Niethammer


Constantin Herfurth


Dr. David Rieks


Stefan Saerbeck

Eversheds Sutherland (Germany) LLP

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking constitutes a criminal offence according to Sec. 202a and Sec. 202b of the German Criminal Code (so-called "data espionage", Sec 202a, and "phishing" Sec. 202b). According to Sec. 202a, whosoever unlawfully obtains data for himself, or another, that was not intended for him and was especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine. According to Sec. 202b, whoever, without being authorised to do so, intercepts data which are not intended for them, either for themselves or another, by technical means from non-public data transmission or from an electromagnetic broadcast from a data-processing facility, incurs a penalty of imprisonment for a term not exceeding two years or a fine, unless the offence is subject to a more severe penalty under other provisions. Depending on the facts of the case, "hacking" could possibly come under the definition of both of the offences set out above, depending on the level of protection applied to the data in question.

Denial-of-service attacks
Denial-of-service attacks constitute a criminal offence according to Sec. 303b of the German Criminal Code (so-called "computer sabotage"). According to this provision, whosoever interferes with data-processing operations which are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, or by entering or transmitting data with the intention of causing damage to another, shall be liable to imprisonment for up to three years or a fine. The same applies to destroying, damaging, rendering unusable, removing or altering a data-processing system or data carrier. Also, it is important to note that the sole attempt is punishable and if the data-processing operation is of substantial importance for another's business or enterprise, or a public authority, the penalty can be imprisonment for up to five years or a fine.

Phishing
Phishing can constitute two different criminal offences. The unlawful interception of data by technical means from a non-public data-processing facility constitutes a criminal offence according to Sec. 202b of the German Criminal Code and is punishable with imprisonment for up to two years or a fine. The *use* of such data with the intent of obtaining an unlawful material benefit would constitute a criminal offence under Sec. 263a of the German Criminal Code (so-called "computer fraud") and is punishable with imprisonment for up to five years or a fine. In especially serious cases of computer fraud, the penalty is imprisonment for a term not exceeding five years or a fine. Furthermore, *storing or modifying* such data in a way that a counterfeit or falsified document would be created, may constitute a criminal offence under Sec. 269 of the German Criminal Code (so-called "forgery of technical records").

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware constitutes a criminal offence according to Sec. 303b of the German Criminal Code (so-called "computer sabotage"). According to this provision, whosoever interferes with data-processing operations which are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, or by entering or transmitting data with the intention of causing damage to another, shall be liable to imprisonment for up to three years or a fine. The same applies to destroying, damaging, rendering unusable, removing or altering a data-processing system or data carrier. Also, it is important to note that the sole attempt to commit such an offence is punishable. Moreover, if the data-processing operation is of substantial importance to another's business or enterprise, or a public authority, the penalty can be imprisonment for up to five years or a fine.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
According to Sec. 27 of the German Criminal Code, anyone who assists another person in committing an intentional, unlawful act is liable for prosecution (so-called "aiding"). In this context, aiding is provided by the person who physically or psychologically assists another in the intentional commission of an unlawful act.

If someone distributes or sells hardware, software or other instruments being used to commit cybercrime and this use is covered by the seller's intent, then he is liable for the respective completed offence (e.g. see above) in connection with Sec. 27 of the German Criminal Code. The penalty for the aider is based on punishment for the offender. However, the penalty must be mitigated pursuant to Sec. 49 (1) of the German Criminal Code.

Depending on the individual circumstances of the case, assisting an offender could also fall under the definition of abetting (Sec. 26 of the German Criminal Code) if the assistant intentionally induces another to intentionally commit an unlawful act.

In this case, the abettor faces the same threat of punishment as the offender. However, individual punishment may differ from the sentence the offender will receive.

Whenever there is preparatory conduct to data espionage and phishing, Sec. 202c of the German Criminal Code must be considered in particular. This criminal offence was expressly created with a view to the increasing danger of cybercrime and it is supposed to closing gaps in criminal liability prior to actual cyber-attacks. The criminal offence includes the manufacture, sale and procurement for the purpose of using, distributing or otherwise making available a device, including computer programs, which were primarily designed or prepared for the purpose of committing certain cyberattacks. Further, Sec. 202c of the German Criminal Code will be especially applicable for such conduct in which prosecution is not able to prove that the offender or another has committed the criminal offences of data espionage or phishing, but has taken preparatory measures to commit such offences.

Possession or use of hardware, software or other tools used to commit cybercrime

The sole possession of hardware, software or other tools which can be used to commit cybercrime can constitute a criminal offence according to Sec. 202c of the German Criminal Code. According to this provision, the preparation of the commission of data espionage or phishing by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible software for the purpose of the commission of such an offence shall be liable to imprisonment for up to one year or a fine. In case of a use of such instruments, the same principles as set forth above with respect to "Hacking" apply.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft can constitute various criminal offences, depending on how the offender obtains access to the identity data. This can either be done by phishing methods, which would constitute a criminal offence under Sec. 202b of the German Criminal Code, as set forth above with respect to "Phishing", or by use of such identity data for fraudulent purposes, which could constitute a criminal offence under Sec. 263 of the German Criminal Code (fraud) or Sec. 263a of the German Criminal Code (computer fraud), both offences being subjected to imprisonment for up to five years, or even up to 10 years in especially serious cases. Depending on the individual facts of the case, the use of such identity of another may further constitute a criminal offence under Sec. 267 (forgery of documents) or Sec. 269 (forgery of data of probative value) of the German Criminal Code, with both offences being punishable by imprisonment for up to five years, or even up to 10 years in especially serious cases.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft constitutes a criminal offence under the preconditions of Sec. 202a of the German Criminal Code. Therefore, the affected data must be especially protected against unauthorised access and the offender must gain access to the data by circumventing access protection. Usually, this is not the case when a current or former employee breaches confidence, as the employee has authorised access to the data. However, such conduct may constitute a criminal offence according to Sec. 23 of the German Trade Secret Protection Act (so-called "betrayal of business and corporate secrets") or Sec. 142 of the German Patent Act. Furthermore, such conduct may constitute the criminal offence of "phishing". The above-mentioned principles apply.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Penetration tests are a comprehensive security check of IT infrastructure. It involves taking measures that even a hostile hacker would use to penetrate networks without authorisation.

In Germany, penetration tests may only be carried out with the prior consent of the owner of the IT infrastructure to be tested. Also, with regard to Sec. 202a of the German Criminal Code, a criminal liability is only excluded here if the penetration test is authorised by the owner of the IT infrastructure to be tested.

In addition, even in the case of legal penetration tests, the data protection regulations must be guaranteed at all times, as the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – "*BSI*") has expressly determined.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Under German criminal law, some other activities in connection with the above-mentioned conduct constitute criminal offences. These are: (i) preparing of an unauthorised obtaining or interception of data, Sec. 202c of the German Criminal Code; (ii) handling of stolen data, Sec. 202d of the German Criminal Code; (iii) violation of postal and telecommunications secrets, Sec. 206 of the German Criminal Code; (iv) computer sabotage, Sec. 303b of the German Criminal Code; (v) certain types of violation of the EU General Data Protection Regulation with the intention of enrichment or to harm someone, Art. 84 of the General Data Protection Regulation and Sec. 42 of the German Federal Data Protection Act; and (vi) falsification of digital evidence, Sec. 269 *et seq.* of the German Criminal Code.

1.2 Do any of the above-mentioned offences have extraterritorial application?

In general, the application of the German Criminal Code depends on the "place of commission of the offence". According to Sec. 9 of the German Criminal Code, an offence is deemed to have been committed in every place where the offender acted or in which the result occurs, or should have occurred, according to the intention of the offender. Therefore, the above-mentioned offences will be applicable both if the offender acted in the territory of Germany and in case the offence affects IT systems which are situated or used for services provided in Germany where the offender acted from outside Germany. With regard to Sec. 23 of the German Trade Secret Protection Act (so-called "betrayal of business and corporate secrets"), Sec. 5 of the German Criminal Code stipulates extraterritorial application. According to Sec. 5 no. 7 of the German Criminal Code, German criminal law applies *regardless of which law is applicable at the place where the offence was committed* to a violation of the business or trade secrets of a business which is physically located within the territorial scope of this statute or of an enterprise which has its seat therein, or of an enterprise which has its seat abroad and which is dependent on an enterprise which has its seat within the territorial scope of this statute and which forms a corporate group with the latter.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Even "ethical hacking" remains a violation of Sec. 202a of the German Criminal Code, as long as unauthorised action is taken and no prior consent of the IT system owner has been obtained.

In general, under German law, a penalty for criminal or administrative wrongdoing is determined by the degree of individual guilt. There is a margin of discretion for the judge to impose penalties. Positive behaviour after a violation of a statutory provision, as well as compensation for the occurred damage, affect the level of penalties. Therefore, the circumstances of each individual case must be considered. In particular, the subjective circumstances and attitudes as well as the objectives of the offender are also decisive.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity is governed by several Acts in Germany. The main legal act relating to cybersecurity is the German IT Security Act (*IT-Sicherheitsgesetz*) of 25 July 2015, which amended a number of laws, in particular the Telemedia Act (*Telemediengesetz*), the Telecommunications Act (*Telekommunikationsgesetz*), the EU General Data Protection Regulation (*Datenschutz-Grundverordnung*), the Federal Data Protection Act (*Bundesdatenschutzgesetz*) and the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*). Further, sector-specific parts of cybersecurity are governed for example by the Banking Act (*Kreditwesengesetz*) and Securities Trading Act (*Wertpapierhandelsgesetz*). Besides this formal legislation, there are a few important informal provisions with respect to IT security in Germany. These are the BSI IT Baseline Protection Manual which are developed by the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – "*BSI*"), the Common Criteria for Information Technology Security Evaluation, standardised as ISO/IEC 15408, and the Control Objectives for Information and Related Technology ("COBIT"). Furthermore, the European Cybersecurity Act provides the necessary authority to the European Union Agency for Cybersecurity ("ENISA") in order to establish a cybersecurity certification. Companies may voluntarily obtain such certification which is meant to inform the public about IT security provisions and general compliance with relevant IT security regulations. ENISA will perform cybersecurity trainings during which companies may evaluate their processes when being subject to a cyber-attack. Generally, the ENISA will be a principal contact for any cybersecurity-related questions.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes, the Act on the Federal Office for Information Security provides for specific obligations for critical infrastructure. Critical Infrastructures shall mean facilities, equipment or parts thereof which:

1. are part of the energy, information technology and telecommunications, transportation and traffic, health, water, nutrition, finance and insurance industry sectors; and
2. are of high importance to the functioning of the community as their failure or impairment would result in material shortages of supply or dangers to public safety.

Operators of Critical Infrastructures must:

- take appropriate organisational and technical precautionary measures to avoid disruptions of the availability, integrity, authenticity and confidentiality of their information technology systems, or any components or processes that are integral to the functionality of the critical infrastructures;
- demonstrate compliance with the requirements of the Federal Office for Information Security by means of security audits, reviews or certifications at least every two years towards the Federal Office for Information Security;
- specify a contact point to the Federal Office for Information Security within six months who must be available 24/7; and
- immediately report the certain Incidents to the Federal Office for Information Security via the contact person.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes, German and European law provide for several obligations for organisations to take measures to monitor, detect, prevent and mitigate Incidents.

In detail:

- According to Sec. 13 (7) of the Telemedia Act, telemedia providers must ensure through technical and organisational measures that no unauthorised access to the technical equipment used for their telemedia services is possible and that they are protected against personal data breaches and against disturbances, even if they are caused by external attacks.
- According to Sec. 109 (1) of the Telecommunications Act, providers of telecommunications services must implement technical safeguards to protect telecommunications privacy and personal data and to protect telecommunications and data-processing systems against unauthorised access (further obligations in Sec. 109 (2) to (5) Telecommunications Act).
- Providers of several financial products are obliged to develop an IT-specific risk management (Sec. 25a of the Banking Act (*Kreditwesengesetz*) and Sec. 80 of the Securities Trading Act (*Wertpapierhandelsgesetz*)).
- According to Art. 5 (1) (f) and Art. 32 of the General Data Protection Regulation, controllers are obliged to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, there are specific reporting obligations with respect to Incidents under German and European law.

In detail:

- Controllers must notify personal data breaches to the competent data protection authority under Art. 33 of the General Data Protection Regulation. An exception applies where the security breach is unlikely to result in a high risk to the rights and freedoms of the data subject. The report must be made without undue delay and not later than 72 hours after having become aware of the breach, and has to contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects and a detailed description of the measures taken to remedy or mitigate negative effects. The notification to the competent data protection authority must also describe possible harmful consequences of the unlawful access and measures taken by the body. The name and contact details of the data protection officer have to be provided as well.
- Operators of critical infrastructures must notify certain Incidents regarding the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes immediately to the Federal Office for Information Security under Sec. 8b of the Act on the Federal Office for Information Security. The notification shall include information on the interference, possible cross-border effects and the technical framework, in particular the assumed or actual cause, the information technology concerned, the type of facility or equipment concerned, as well as the critical provided service and the effects of the Incident on this service.
- Providers of public telecommunications networks or services must notify any impairments of telecommunications networks and services which lead or may lead to significant security breaches immediately to the Federal Network Agency and the Federal Office for Information Security under Sec. 109 of the Telecommunications Act. The notification must contain information on the impairment, as well as the technical conditions, in particular the presumed or actual cause and the information technology affected.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons (see above under question 2.4), controllers must communicate the personal data breach to the data subject without undue delay under Art. 34 of the General Data Protection Regulation. The communication to the data subject must describe in clear and plain language the nature of the personal data breach and at least contain the information and measures referred to in Art. 33 of the General Data Protection Regulation.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The requirements identified for the above-mentioned requirements are enforced by the Federal Office for Information Security, competent Data Protection Authorities and the Federal Network Agency.

In detail:

- The Federal Office for Information Security is the main authority with respect to cybersecurity in Germany. This authority should be the main contact regarding questions about preventive security measures and is primarily responsible for receiving notifications about security breaches with respect to critical infrastructures.
- Data Protection Authorities enforce all relevant data protection laws. In Germany, each federal state has a separate Data Protection Authority.
- The Federal Network Agency enforces the telecommunications-related laws and is responsible for receiving notifications about security breaches with respect to telecommunications networks and services.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Under Sec. 14 of the Act on the Federal Office for Information Security, non-compliance with the above-mentioned requirements may be subject to administrative fines of up to 100,000 EUR. Under Art. 83 of the General Data Protection Regulation, non-compliance with the aforementioned requirements is subject to fines up to 10 million EUR or 2% of the worldwide annual turnover, whichever is higher.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

German data protection authorities have started imposing administrative fines on companies who have not complied with their obligations under Art. 32 of the General Data Protection Regulation. A German social network ("Knuddels") had to pay a fine of 20,000 EUR because it failed to properly secure users' data. Hackers managed to obtain 808,000 email addresses and almost 2 million usernames and passwords. These were stored unencrypted on the company's servers. Furthermore, the hackers obtained specific data as to the age and addresses of some users. As the social network immediately reported the security Incident, cooperated with the relevant data protection authority and made a high investment in new data security measures, the fine of 20,000 EUR was rather low. This Incident was the first fine in Germany under the General Data Protection Regulation.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Yes, beacons are permitted.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Yes, honeypots are permitted.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Yes, sinkholes are permitted.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Generally, organisations are permitted to monitor or intercept electronic communications on their networks in order to prevent or mitigate the impact of cyber-attacks. However, at the same time they must comply with applicable data protection laws with regard to the monitoring of electronic communications of its employees which may lead to certain restrictions.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Germany follows EU regulations and the Wassenaar Arrangement. The export of data encryption products is regulated in Germany by the directly applicable EC Dual-Use Regulation, the Foreign Trade Act ("AWG") and the Foreign Trade Regulation ("AWV"). In the recent years, the threat potential of cyber-attacks has grown rapidly. Among other things, the European Union has reacted to this by adapting Annex I of Regulation EC No. 428/2009 ("Dual-Use Regulation") in 2018. The so-called Waassenaar Agreement treats strong cryptography as a weapon of war. Germany has signed this agreement and must therefore monitor the export of certain cryptographic products. Exports of such products are, in principle, subject to a licensing requirement; however, all products that are available in the mass market can be exported without a licence.

There are no import restrictions on data encryption products in Germany, regardless of whether they are hardware or software.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice with respect to information security in Germany mainly depends on the security relevance of the individual business; in particular, whether the sector is considered a sector which is related to critical infrastructures and whether the business processes sensitive personal data or not. However, there are no known sector-specific deviations from the strict legal requirements.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes, in detail:

- Providers of certain financial products are obliged to develop an IT-specific risk management (Sec. 25a of the Banking Act (*Kreditwesengesetz*) and Sec. 80 of the Securities Trading Act (*Wertpapierhandelsgesetz*)).
- According to Sec. 109 (1) of the Telecommunications Act, providers of telecommunications services must implement technical safeguards to protect telecommunications privacy and personal data and to protect telecommunications and data-processing systems against unauthorised access (further obligations in Sec. 109 (2) to (5) of the Telecommunications Act).

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Yes, such failure may lead to a breach of directors' or officers' duties.

According to Sec. 130 of the German Administrative Offences Act (*Ordnungswidrigkeitengesetz* – "*OWiG*"), the owner or management of a company commits a misdemeanour if:

- it omits purposefully or negligently to appropriately control the company; and
- if a crime or misdemeanour was committed that could have been avoided or significantly impeded by exercising such control.

The obligation to control also includes the obligation to diligently select and monitor supervising personnel, active monitoring of the development of legal and technical standards, random inspections, enforcement of implementation measures, etc. The owner or management of a company is obligated to organise the company in a manner that allows the company to comply with the law. Consequently, failures to prevent, mitigate, manage or respond to an Incident can constitute a breach of directors' duties if the directors failed to implement the appropriate measures to avoid such occurrences.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There are no general obligations, so far, to either designate a CISO or an equivalent, establish a written Incident response plan or policy or conduct periodic cyber risk assessments. However, according to Art. 32 of the General Data Protection Regulation, such measures can be required in order to ensure appropriate IT security measures. Companies shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In particular, companies shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing. This must therefore be assessed on a case-by-case basis. Furthermore, operators of public telecommunications networks or providers of publicly available telecommunications services must appoint a security commissioner under Sec. 109 of the Telecommunications Act.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no further obligations beyond the above-mentioned disclosure requirements in the event of data breaches. However, with respect to publicly listed companies, sole cybersecurity risks without an Incident having occurred may trigger the obligation to disclose the cybersecurity risk in an *ad hoc* notification if the risk is likely to have an impact on the company's stock market price.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

If the entity in charge of the attacked IT systems is not reacting appropriately, it is – depending on the kind of Incident – possible to file for an interim injunction of a German court in order to compel such entity to comply with its contractual and statutory obligations. This would require an ongoing Incident, as well as the violation of a statutory or contractual obligation.

Furthermore, it is possible to file for damage payments if the Incident has been enabled by the lack of an appropriate IT security model. In this case, any individual or other company which suffered material damage can take civil actions against the company which is responsible for the Incident. This liability is basically not limited but can be covered by insurance.

Additionally, in terms of private actions, damaging events can often be interrupted or even reversed through close cooperation with law enforcement and compliance departments.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

The case law on Incidents in Germany is very rare due to the lack of the possibility of class actions in Germany. Private actions are usually not published in Germany.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes, civil liability in tort depends on the damage which occurred due to the organisation's failure and is basically not limited.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents in Germany.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations to insurance coverage against any type of loss.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Depending on the type of authority (e.g. Public Prosecutor, Federal Office for Information Security and Data Protection Authority), the enforcement powers vary. If the conduct being investigated might qualify as a criminal offence, it will be the public prosecution office leading the investigations most commonly using the aid of other authorities. All aforementioned authorities have the power to carry out on-site investigations including accessing IT systems. Furthermore, under certain preconditions according to Sec. 100a of the German Code of Criminal Procedure, telecommunications may be intercepted and recorded without the knowledge of the persons concerned and Sec. 100b of the German Code of Criminal Procedure provides the possibility to gain covert access to information technology systems used by persons concerned.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No; so far, there is no such obligation. However, the German legislator is currently debating such an obligation with respect to social media and instant messaging accounts.

Dr. Alexander Niethammer is the Managing Partner of Eversheds Sutherland in Germany. He specialises in cybersecurity, data protection as well as technology transfer and outsourcings, with additional experience in advising on complex IT transactions. With more than 17 years of experience, Alexander has advised many Fortune 100 companies from the IT, industrials, consumer and financial sectors on global projects. He is admitted as an attorney (*Rechtsanwalt*) in Germany and as an attorney-at-law in the State of New York (USA). Alexander is recommended for data protection by *Best Lawyers* and *The Legal 500* and has been recognised as a leading data protection and IT lawyer in Germany by the business magazine *Wirtschaftswoche*.

Eversheds Sutherland (Germany) LLP
Brienner Str. 12
80333 Munich
Germany

Tel: +49 89 54565 318
Email: alexanderniethammer@eversheds-sutherland.com
URL: www.eversheds-sutherland.com

Constantin Herfurth is an Associate in the Data Protection & Cybersecurity practice at Eversheds Sutherland in Munich. His area of advice covers all aspects of data protection, IT law and cybersecurity. In particular, he has strong expertise in the management of data breaches. He mainly advises international and national clients from the industrial and health sectors. Constantin frequently publishes in the specialist journals *Zeitschrift für Datenschutz* (journal for data protection) and *MultiMedia und Recht* (multimedia and law), and is a contributor to the EU chapter of ILO's *Tech, Data, Telecoms & Media* newsletter.

Eversheds Sutherland (Germany) LLP
Brienner Str. 12
80333 Munich
Germany

Tel: +49 89 54565 295
Email: constantinherfurth@eversheds-sutherland.com
URL: www.eversheds-sutherland.com

Dr. David Rieks is a Counsel in the area of compliance and criminal law in the Hamburg office of Eversheds Sutherland. As a certified specialist in criminal law, David advises and represents national and international companies regarding all questions of commercial and tax criminal law. He regularly advises clients with regard to cybercrime and other data breach-related compliance matters. David also helps companies investigate and enforce damage claims resulting from criminal offences or other misconduct by business partners and employees. David is recognised as one of the leading lawyers for white-collar crime in Germany by German business magazine *Wirtschaftswoche*.

Eversheds Sutherland (Germany) LLP
Stadthausbrücke 8
20355 Hamburg
Germany

Tel: +49 40 808094 260
Email: davidrieks@eversheds-sutherland.com
URL: www.eversheds-sutherland.com

Stefan Saerbeck is a Principal Associate in the Litigation & Dispute Management practice at Eversheds Sutherland in Munich. Stefan has more than 10 years of experience as a trial lawyer in German courts. He focuses especially on injunction proceedings, as well as regular court proceedings in commercial, corporate and cyber-related disputes. Stefan is a member of the American Bar Association and the German Institution of Arbitration ("DIS"), and a lecturer at the University of the German Armed Forces in Munich. He is recommended as a corporate litigator by *Global Law Experts*.

Eversheds Sutherland (Germany) LLP
Brienner Str. 12
80333 Munich
Germany

Tel: +49 89 54565 167
Email: stefansaerbeck@eversheds-sutherland.com
URL: www.eversheds-sutherland.com

As a global top 40 law practice, Eversheds Sutherland provides legal services to a global client base ranging from small and mid-sized businesses to the largest multinationals, acting for 66 of the FTSE 100, 73 of the Fortune 100 and 119 of the Fortune 200.

With more than 3,000 lawyers, Eversheds Sutherland operates in 68 offices in 32 jurisdictions across Africa, Asia, Europe, the Middle East and the United States. In addition, a network of more than 200 related law firms, including formalised alliances in Latin America, Asia Pacific and Africa, provide support around the globe.

In Germany, more than 160 lawyers, tax advisors and notaries in Berlin, Dusseldorf, Hamburg and Munich provide advice to multinational groups, listed and medium-sized companies, investors, financial service providers, as well as family businesses in all relevant areas of commercial law.

In the fields of data protection and cybersecurity, the German team in particular provides advice on data security, the reform of the European data protection law, the transfer of data abroad, data protection management, as well as with regard to employee data protection and digitalisation issues such as Big Data, artificial intelligence and the internet of things. The team, which is part of the global Data Privacy & Cybersecurity Group of Eversheds Sutherland, furthermore advises on data protection management and provides support with regard to crisis management in case of data breaches and cyberattacks.

www.eversheds-sutherland.com

EVERSHEDS SUTHERLAND

Greece


Dr. Nikos Th. Nikolinakos


Dina Th. Kouvelou

Nikolinakos & Partners Law Firm

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking (i.e. unauthorised access to information systems or electronic data, according to the Greek Criminal Code (GCC)) is a criminal offence pursuant to Art. 370C par. 2 GCC. Under Art. 370C par. 2 GCC, hacking carries the penalty of imprisonment. If the action targets international relations or state security, other Articles of the GCC shall apply (Art. 148 GCC on espionage), bearing a penalty of up to 10 years of imprisonment if the data was used to damage the state. If hacking causes a severe hindrance to the operation of an information system or when data is modified or suppressed as a result of hacking, the penalty ranges from one to five years of imprisonment depending on the severity of the outcome (Art. 292B).

Pursuant to Art. 15 of Law 3471/2006, which regulates privacy in the field of electronic communications, an administrative penalty of €10,000 to €100,000 may be imposed if the offender gained access to personal data of subscribers or users of the system in an unauthorised manner.

Furthermore, according to Art. 4 part II of Law 4411/2016: a) a recommendation for compliance; b) an administrative fee from €20,000 to €1,000,000; c) a revocation or suspension of their operating licence; or d) an exclusion from public services may be imposed on the offender if the hacking was carried out by a legal person. For the cumulative or selective application of the above administrative sanctions, the imposing authority takes into account the gravity of the offence, the degree of intent, the economic status of the legal entity and any existing offending history.

Denial-of-service attacks
Denial-of-service attacks constitute a criminal offence under Art. 292B GCC, which sanctions the impeding of an information system's operation, with a minimum of one year of imprisonment. If a certain tool was used for the attacks, the penalty varies from one to five years of imprisonment, while if the attack caused severe damage or targeted critical infrastructure, a penalty of at least two years of imprisonment for each case applies (Art. 292B GCC par. 2 sec. a, and secs b and c, respectively).

Phishing
If phishing is defined as the use of technical equipment to proceed with unauthorised monitoring, extraction or reproduction of a system's data, with the purpose of knowing its content, then it falls under Art. 370D GCC and bears a penalty of 10 days to five years of imprisonment. If the data is diplomatic or military, whoever uses it faces the penalties of Art. 146 GCC, which imposes imprisonment of up to 10 years. Phishing can also be punished as a preparatory action (Art. 292C sec. b GCC; Art. 370E sec. b GCC, etc.).

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware is a criminal offence and can be sanctioned pursuant to Arts 292B, 292C, 370C par. 2, 370E, 381A and 381B GCC, depending on the type of infection of the IT system.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
These acts constitute criminal offences under Art. 292C GCC, bearing a penalty of imprisonment of up to two years or a fine under the condition that the hardware, software or other tools were used to commit the cybercrimes described in Art. 292B GCC.

Possession or use of hardware, software or other tools used to commit cybercrime
This offence can be sanctioned pursuant to Arts 282C sec. a, 370E sec. a, 381 A and 381B sec. a GCC depending on the act of cybercrime for which the hardware, software or tools have been used.

Identity theft or identity fraud (e.g. in connection with access devices)
Pursuant to Art. 386A GCC, whoever, with the purpose of gaining illegal profit, damages foreign property by influencing by any means of data processing, faces a penalty of up to 10 years' imprisonment. Apart from the abovementioned case, identity theft can constitute several criminal offences under GCC, depending on the manner and reason for which the offender obtains access to the identity data.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Given that electronic theft is not a specific criminal offence in the GCC, Greek courts have considered such offences: a) under Art. 386A GCC, as fraud with the use of information systems, with the respective penalties; b) under Art. 370B GCC (state and non-state secrets violation excluding diplomatic and military), with a penalty of at least one year of imprisonment; and c) under Art. 370C GCC, according to which if the offender is offering its

services to the information system owner, the offence is punishable only if it is expressly stated in the bylaws or in a written decision of the owner.

Law 2121/1993 on intellectual property, in its Art. 66, provides for criminal penalties of at least one year's imprisonment and a €2,900 to €15,000 fine for illegal unauthorised copies, reproductions and sale of material that are protected under its provisions. Art. 65 of the same law provides for civil liabilities in case of copyright infringement and Art. 65A for administrative penalties up to €1,000 per copy if someone reproduces or sells illegal copies.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Any unfair – including without permission – violation of elements or programs of computers – such as a software or system intervention in order to determine its vulnerabilities – shall be considered a crime independently pursuant to Art. 370G GCC, or as a preparatory action on the occasion of which the above crimes may be committed.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Within the framework of Law 4624/2019, if anyone who commits the above acts simultaneously intervenes in any way in a system for personal data archiving, and by doing so becomes aware of the data, and a) copies, removes, changes, damages, collects, adds, organises, saves, adapts, recovers, seeks, correlates, combines, limits, erases, destroys them, or b) transmits, diffuses, or communicates them to non-eligible persons, is sanctioned with imprisonment for up to one or up to five years, respectively. In case any of the above acts concern special categories of personal data (Art. 9 (1) GDPR) or data relating to criminal convictions and offences (Art. 10 GDPR), the sanction consists of imprisonment for one to five years and a fine of up to €100,000. In case penalties are provided by both the Penal Code and Law 4624/2019, the more severe penalties apply.

Administrative sanctions

In Art. 4 of Law 4411/2016, administrative sanctions are defined against legal entities in favour of which the acts of Arts 292B, 370C, 370D, 370E, 381A και 386A GCC as described above are committed. The sanctions include a) recommendations for compliance, b) an administrative fee from €20,000 to €1,000,000, c) a revocation or suspension of their operating licence, or d) an exclusion from public services, if the hacking has been committed by a legal person. For the cumulative or selective application of the above administrative sanctions, the imposing authority takes into account the gravity of the offence, the level of intent, the economic status of the legal entity and any existing offending history.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The GCC applies for all criminal offences with their "place of the offence" within Greece (Art. 5 par. 1 GCC). According to Art. 5 par. 3 GCC, when the offence is committed via a network or other means of communication, Greece is also considered the place of offence if, in that territory, specific means for the offence are accessible. The "place of the offence" is defined under Art. 16 par. 1 GCC as the place where the offender actually committed the offence, in whole or in part, as well as the place where the result of the offence took or would have taken place.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Most of the crimes described above contain the condition of purpose for their sanctions to apply. For example, in the subjective element of identity theft or identity fraud, the perpetrator of an act is punished when there is the intention of personal (or in favour of a third party) financial gain. As a similar condition, hacking is sanctioned when the perpetrator acts unfairly – a condition which obviously cannot include cases of ethical hacking.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The following laws are the most significant instruments with regard to cybersecurity:

- Law 4727/2020 regarding "Digital Governance (Transposition into Greek Legislation of Directive (EU) 2016/2102 and Directive (EU) 2019/1024) – Electronic Communications (Transposition into Greek Legislation of Directive (EU) 2018/1972) and other provisions".
- Law 4577/2018, which transposed NIS Directive 2016/1148/EU into Greek law, regarding measures for a high common level of security of network and information systems.
- Ministerial Decision No. 1027/2019, issued by the Minister of Digital Governance, which specifies the implementation and the procedures provided under Law 4577/2018.
- The General Data Protection Regulation and the relevant Greek Law 4624/2019.
- Law 4411/2016, which transposed Directive 2013/40/EU into Greek law, on attacks against information systems.
- Law 4070/2012, in relation to the operation of electronic communications networks and the provision of electronic communications services.
- Act 205/2013 of the Hellenic Authority for Communication Security and Privacy (ADAE), which is a Regulation for the Security and Integrity of Networks and Electronic Communication Services.
- Art. 12 of Law 3471/2006, regarding the protection of personal data and privacy in the electronic telecommunications sector and the operators' obligation to take the necessary safety measures.
- Draft Law of the Greek Code of Electronic Communications, which is a transposition of the Directive (EU) 2018/1972 into Greek law.
- Art. 386A of the Greek Penal Code, regarding fraud committed via a computer.
- Law 2121/1993, i.e. the Greek Copyright Act, recently amended and replaced by Art. 25 of Law 4708/2020.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Law 4577/2018 and the subsequent Decree 1027/08.10.2019 on the implementation of the said Law outline the responsibilities of essential service operators, i.e. critical infrastructure operators in the fields of energy, transportation, banking and finance, health, drinking water and IT infrastructures, which are the following:

- adopting technical and organisational measures to identify potential security risks and to prevent and minimise the impact of cybersecurity Incidents;
- notifying all Incidents that might severely impact the operational continuity of the essential services they are providing to the Hellenic Cybersecurity Authority (HCA) and the Hellenic Cyber Security Incident Response Team (CSIRT) without undue delay;
- collaborating with the competent authorities;
- ensuring that the operator's Security Policy is in line with the Comprehensive Security Policy issued by the Hellenic Cybersecurity Authority and that the "Basic Security Requirements", as outlined by the Hellenic Cybersecurity Authority are adhered to; and
- designating a CISO.

According to Law 4577/2018, the Hellenic Cybersecurity Authority, in cooperation with the competent regulatory and oversight authorities, is responsible for identifying the essential service operators in Greece and compiling a list of the essential services and their operators, which is updated regularly – every two years at the minimum. It also supervises operator compliance with the provisions of the said Law and, in case of severe violation, may impose fines ranging from €15,000 to €200,000.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

There are several legal provisions for organisations to take measures for monitoring, detecting, preventing or mitigating Incidents:

- Law 4577/2018 establishes significant obligations for organisations in regard to security measures on their behalf. In particular, operators of essential services and digital service providers shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in their operations and to prevent and minimise the impact of Incidents affecting the security of the network and information systems used for the provision of their services (Arts 9 and 11).
- According to the GDPR, personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Art. 5(f)). Under Art. 32, the Controller and the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, *inter alia*, as appropriate: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical Incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- Art. 37 of Law 4070/2012 establishes the obligations for undertakings providing public communications networks or publicly available electronic communications services to take the appropriate technical and organisational measures to properly manage network and service security risk. These measures, taking into account the latest technical capabilities, must ensure a certain level of safety commensurate with the existing dangers. These undertakings shall in particular take measures to prevent and minimise the effects of security Incidents affecting users and interconnected networks.
- Act 205/2013 of ADAE sets similar obligations for undertakings providing public communications networks or publicly available electronic communications services to take the appropriate technical and organisational measures.
- Art. 12 of Law 3471/2006 regarding the protection of personal data and privacy in the field of electronic communications also sets obligations for providers of electronic communications services, as they must take appropriate technical and organisational measures in order to protect the security of the services provided.
- According to Art. 148 of the Draft Law of the Greek Code of Electronic Communications (Transposition of Directive (EU) 2018/1972 into Greek law), to the extent that is absolutely necessary to ensure interoperability of the services, operators must comply with standards published in the Official Journal of the EU. In case such standards have not been published, they should comply with standards of European standardisation bodies and, in the absence of those, by international standardisation bodies. Operators take measures, including encryption, where appropriate, to prevent and minimise the impact of security Incidents affecting users and other networks and services.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Several instruments within the Greek and European legal frameworks require organisations to report information related to Incidents and potential Incidents to the competent authorities.

Art. 33 GDPR provides that "in case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority", which in this case is the Hellenic Data Protection Authority (HDPA), unless the personal data breach is unlikely to result in a

risk to the rights and freedoms of natural persons. The notification shall contain the information provided in Art. 33 par. 3 (a–d).

Law 4577/2018 provides that in case of an Incident related to essential service operators (Art. 9(1)(c)) or to digital service providers (Art. 11(1)(c)), the operators and providers are required to notify the Hellenic Cybersecurity Authority and the Hellenic CSIRT without undue delay, and their notification must include all information necessary for the Authorities to assess the critical nature of the Incident and its potential cross-border impacts.

Pursuant to Art. 17(2)(d) of Act 205/2013 of the Hellenic Authority for Communication Security and Privacy titled "Regulation for the Security and Integrity of Networks and Electronic Communications Services", on the mitigation of Security Incidents, the provider shall, without undue delay, notify all Incidents jeopardising the security and integrity of networks and services to its the Security and Network Integrity Manager, its competent executives as well as to the Hellenic Authority for Communication Security and Privacy, which is the competent authority.

Pursuant to Art. 37(4) of Law 4070/2012 on the organisation and operation of the electronic communications sector in Greece, in the event that security breaches or Incidents of loss of integrity occur which may significantly impact the operation of the networks or services, organisations providing access to public communications networks or publicly available electronic communications services shall notify the Hellenic Telecommunications and Post Commission (EETT). The Commission shall in turn notify the Hellenic Authority for Communication Security and Privacy.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Pursuant to Art. 34 GDPR, "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall communicate the personal data breach to the data subject without undue delay" and shall "describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)". The communication to the data subject is not required if any of the conditions of Art. 34 par. 3 (a–c) are met.

Law 4577/2018 provides that in case of an Incident related to "operators of essential services" (Art. 9 par. 4) or to "digital service providers" (Art. 11 par. 5), the Hellenic Cybersecurity Authority, after consultation with the relevant provider, may inform the public of individual Incidents or require the relevant provider to do it so, as far as this is required to prevent a future Incident or to handle an ongoing Incident.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The competent authorities for the enforcement of the above-mentioned requirements are:

- The Hellenic Data Protection Authority, a constitutionally consolidated independent authority, serves as the watchdog of the personal data and privacy of individuals in accordance with the provisions of Law 4624/2019 and Law 3471/2006. An additional mission of the HDPA is the support and guidance to Controllers in their compliance with the obligations set by the law.
- The Hellenic Telecommunications and Post Commission, an independent authority granted with specific rights under the Hellenic Constitution, acts as the national regulator of the telecommunications and postal market. It was established in 1992 by virtue of Law 2075/1992; however, several new laws and amendments have expanded its competence. The Laws in force are 4070/2012 (for electronic communications) and 4053/2012 (for postal services market and electronic communication matters).
- The Hellenic Authority for Communication Security and Privacy has been established under Law 3115/2003 and Art. 19 par. 2 of the Hellenic Constitution, having, *inter alia*, the competence to: issue regulations regarding the assurance of the confidentiality of communications; perform audits on communications network/service providers, public entities as well the Hellenic National Intelligence Service; and hold hearings of the aforementioned entities, to investigate relevant complaints from members of the public and to collect relevant information using special investigative powers.
- The Hellenic Cybersecurity Authority, as designated by Law 4577/2018 implementing the NIS Directive, consists of the Directorate of Cyber Security of the General Secretariat of the Ministry of Digital Policy, Telecommunications and Media (as established by Art. 15 of Decree 82/2017). The HCA monitors, *inter alia*, the implementation of the NIS Directive, cooperates with the Hellenic CSIRT and is designated as the single point of contact to ensure cross-border cooperation with competent authorities of other EU Member States.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Under Art. 64(1) of the Copyright Act, the competent court may order the precautionary seizure of the items lying in the possession of the alleged infringer that consist of (and are respectively qualified as) either the means of commission, the products deriving from or the evidence of the infringement. In addition, an injunction may be imposed for the purpose of either preventing any imminent copyright and/or related rights infringement or to temporarily forbid the continuation of the violation as accompanied, where appropriate, by the ordering of a penalty payment under the Greek Civil Procedure Code (Art. 64(3)). Moreover, the respective rightsholders may apply for an injunction against intermediaries whose services are used by third parties to infringe copyright or a related right or the *sui generis* right granted to database makers. In cases of intent or negligence, the law provides for the payment of the moral damage caused to the right-holder, further dictating that such a remuneration shall not be less than double the amount that is usually or under the law payable for the unlicensed form of exploitation. Instead of seeking compensation and without the requirement of liability, copyright and related rightsholders may ask for either the payment of the amount that the infringer obtained as a result of the unlawful exploitation of the work and/or subject-matter of protection or of the profit that had been respectively conferred to the latter. On the grounds of omission of acts and for each infringement, the court may impose a penalty payment ranging from €880 to €2,900, as well as up to one year's imprisonment. Furthermore, administrative sanctions are firstly aligned to the unlawful reproduction,

distribution or possession for the purpose of distributing to the public computer programmes; the court in this case may order the payment of a fine of €1,000 for each illegal copy. Last, Art. 66 on criminal sanctions provides for a penalty payment ranging from €2,900 to €15,000 and for a *de minimis* one-year imprisonment for a number of specifically designated Incidents, while the aforementioned sanctions may be doubled when the profit pursued or the damage threatened are particularly extensive.

With regard to the penalties that may be imposed by the Committee for the Notification of Copyright and Related Rights Infringement on the Internet (EDPPI), it is entitled to impose a fine ranging from €500 to €1,000 for each day of non-compliance with the dictum of the decision issued on the grounds of which either the removal of the unlawful content or the blocking of access had been respectively ordered.

In respect of the GDPR, an administrative fine of up to €10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year – whichever is higher – may be imposed in cases of non-compliance with the obligations of: a) Controllers and Processors; b) the certification body; and c) the monitoring body as specified under this legal instrument. The aforementioned penalties are doubled in case of infringements of: a) the basic principles for processing, including conditions for consent; b) the data subjects' rights; c) the personal data being transferred to a recipient in a third country or an international organisation; d) the obligations established under national law under Chapter IX of the Regulation; and e) in the case of non-compliance with an order, a temporary or definitive limitation on processing, the suspension of data flows by the supervisory authority or a failure to provide access in violation as all respectively defined. The same penalties may also be imposed in the case of non-compliance with an order issued by the supervisory authority. Art. 39 of Law 4624/2019 enables the HDPA to impose an administrative fine of up to €10,000,000 against the public authorities defined under Law 4270/2014 for a number of specifically designated infringements on the grounds of a relevant specially detailed decision following a prior call for explanations of the interested party for each case at issue. In addition, the HDPA is entitled (Art. 82 of Law 4624/2019) to impose to competent authorities administrative fines of up to one or €2,000,000 in the specifically designated circumstances where the latter fail to comply with their obligations as personal Data Controllers. Moreover, the national legislator provides criminal sanctions (under Art. 38 of Law 4624/2019) of both imprisonment and penalty payments of €100,000, €200,000 and €300,000 for the offences defined therefor.

Furthermore, the ADAE is entitled to address a recommendation for compliance with a certain provision of the law (being complemented by a warning for the imposition of sanctions in the case where a recurrence of the violation of the law governing the confidentiality of communication or the prerequisites and the procedure related to its declassification is substantiated), while it may also impose an administrative fine ranging from €15,000 to €1,500,000 (Art. 11 of Law 3115/2003).

Lastly, Law 4577/2018 provides for the competence of the Minister of Digital Governance to impose on a) essential service operators, b) digital service providers, and c) any natural and legal person a number of penalty payments ranging from €15,000 to €200,000 following a relevant recommendation issued by the HCA (Art. 15). These fines are applicable when the aforementioned persons do not notify Incidents entailing a serious impact on the operation of their services or they do so but with undue delay, or in the case where they do not undertake both appropriate and proportionate, technical and organisation measures on a provisional basis to manage the risks related to the security of the networks and information systems used for such services ((a) and (b)). In respect of natural/legal persons in general, the imposition of a fine is related to the non-provision or the provision with undue delay of any relevant information that is required within the context of inspections or Incident investigation.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In 2020, the HDPA had imposed on the grounds of Art. 83 par. 5 GDPR administrative fines of €5,000 (Decision No. 4/2020), €8,000 (Decision No. 8, 30/2020), €15,000 (Decision No. 43/2019) and €150,000 (Decision No. 26, 44/2019). Within the context of Art. 83, the HDPA has also imposed a fine of €5,000 (Decision No. 2/2020).

On the basis of the violation of Art. 12(3) GDPR, the HDPA imposed a penalty sanction of €3,000 on a candidate member of Parliament (Decision No. 28/2020). In addition, fines of €1,000, €2,500, €3,000 and €4,000 were imposed for the violation of Art. 11 of Law 3471/2006; these fines were charged to a candidate MEP, a candidate municipal councillor and to candidate members of the Parliament (Decisions No. 10, 11, 12, 13, 17 and 19/2020). Lastly, on the basis of Art. 83 par. 2 GDPR, the HDPA imposed a pecuniary sanction of €5,000 (Decision No. 18/2020).

It is noteworthy that the imposition of the above fines was determined on an *ad hoc* basis being further qualified as an additional and effective, proportionate and preventive pecuniary sanction, aiming at both bringing into conformity and penalising the unlawful conduct.

With regard to copyright and related rights infringements on the Internet, the EDPPI recently had its role enhanced under the recent amendment of Art. 66E of the Greek Copyright Act (intended to extend and foster its competency with the aim of rapidly dealing with online infringements), which provides for a supplementary total 15 days' timeframe within which access blocking may be ordered, provided that the circumvention of a decision already issued by the Committee is substantiated. Since the issuing of the first decision under the revised provision is currently pending, it is noteworthy to cite the enforcement actions already taken by the Committee; in all cases, EDPPI ordered for the blocking of access to the infringing content for a time period of three years. In relation to the fines imposed on ISPs, the administrative pecuniary sanctions ordered (on the grounds of the respective assessment of the severity of the infringement) are listed as follows: €850 (Decision No. 3/2018); and €700 (Decisions No. 5/2019, 7/2019, 9/2019, 11/2019 and 15/2020) for each day of non-compliance with the operative part of the said decisions.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Greek law does not prohibit the use of beacons for cybersecurity purposes; however, such use would have to be assessed under e-privacy and data protection legislation. Insofar as beacons are regarded as cookies due to the similarity of the purpose for which they are used, their use is legal if it complies with cookie

legislation, namely the ePrivacy Directive 2002/58/EC as it was amended in 2009 and transposed into Greek law by Law 3471/2006.

If the use of web beacons results in the processing of personal data (e.g. users' personal account information or their IP addresses, which qualify as personal data if the entity collecting the IP address has the means to identify the person using it), it ought to be in compliance with the provisions of the GDPR.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
The use of honeypots is not prohibited under Greek law.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The use of sinkholes is not prohibited under Greek law.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Organisations are responsible for preventing and responding to cyberattacks. However, monitoring or intercepting electronic communications on their networks may only be permitted under specific and strict circumstances. Particularly, interception of communications (e.g. calls) falls under the scope of privacy of communications and may not be performed without a prosecutor's order. However, stored communications (e.g. emails) or monitoring of logs in real time to prevent cyberthreats is not considered to fall under the scope of communications privacy, but rather under the provisions of the personal data protection framework. In such case, organisations are required to adhere to the requirements of the GDPR and Law 4624/2019. Such processing of personal data will be considered lawful if it is grounded on the purposes outlined in Art. 6 GDPR, in particular on whether it is deemed necessary for the purposes of the legitimate interests pursued by the organisation acting as a Data Controller. Safeguarding the security of its network system, protecting its property from severe threats and verifying or preventing illegal activity, constitute legitimate interests in order for the organisation to process personal data, on the condition that the measures adopted are appropriate to the risks and organisations have documented detailed and specific justifications with regard to their nature and necessity.

The lawfulness of monitoring network communications also crucially hinges on whether employees are provided with prior, clear and concise information on the collection and processing of their data. In addition, it should be stressed that in accordance with the principle of purpose limitation, if the processing of personal data is conducted specifically in order to ensure the safety of the system or network, such data may not be further processed for other purposes (e.g. to monitor employee performance), while the use of any monitoring system needs to take into account the principles of proportionality and accountability with regard to the collection and storage of employees' personal data.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

On an EU level, Regulation No. 428/2009 governs the EU's export control regime on "dual-use" items, which are broadly defined as items, including software and technology, which can be used for both civil and military purposes. Dual-use items are listed on a common and regularly updated annex, which includes products that use cryptography, such as encryption software and hardware. The Regulation provides that dual-use items, with some exceptions, may be traded freely within the EU, and it imposes common export control rules on Member States, including a common set of assessment criteria and common types of authorisations. Export authorisations are required in order for dual-use items to be exported from an EU Member State to third countries. Decision 121837/E3/21837 of the Ministry of Finance was published in 2009, to implement the provisions of Regulation 428/2009.

Greece is also member of the Wassenaar Arrangement, which is an agreement between states on the import and export of conventional arms and "dual-use" goods and technologies, including internet-based surveillance systems and software designed to defeat a computer or network's protective measures so as to extract data or information, as well as IP network surveillance systems.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

ISO Certifications, such as ISO/IEC 27001, are a very common market practice in the context of information security in various business sectors, e.g. the telecommunications sector. There are not any known sector-specific deviations from the strict legal requirements.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Organisations both in the financial services and in telecommunications fall under Laws 4577/2018 and 4411/2016. There are some additional provisions related to the telecommunications sector. More specifically, as mentioned in question 2.3, Art. 37 of Law 4070/2012 regarding security and integrity of networks and services, Act 205/2013 of ADAE and Art. 12 of Law 3471/2006 emphasise the need for organisations in the telecommunications sector to take the appropriate technical and organisational measures in order to protect the security of the services they provide. Also, a relevant provision is established in Art. 148 of the Draft Law of the Greek Code of Electronic Communications.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

There is no specific provision stipulating that a failure a by a company to prevent, mitigate, manage or respond to an Incident amounts to a breach of directors' or officers' duties, within the meaning of duty as it is set out in Art. 102 of Law 4548/2019 (S.A. Companies' Law).

However, Law 4577/2012 provides that operators of both essential and of digital services are subject to administrative fines – both at a company and at an individual level (Art. 15) – should they violate their notification obligation to the competent authority of the Incidents having a significant impact on the continuity of services they provide. The same fines are also applicable in case the above companies do not take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations as well as in cases where it is confirmed that a natural or legal person does not provide (or provides with undue delay) information requested in the context of an investigation of an Incident.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

According to Decree 1027/8.10.2019, specifying the provisions of Law 4577/2018, operators of essential services and providers of digital services (Operators hereinafter) are required to designate a CISO. The Decree requires that the above operators take efficient, effective and proportional measures to address cybersecurity risks but does not delineate how those measures shall be concretised. In that regard, while the law does not explicitly lay out the obligation to establish an Incident response plan, to conduct periodic cyber risk assessment and to perform penetration tests or vulnerability tests, it nonetheless indirectly requires that these measures should be adopted by the Operators for the latter to comply with the Law.

In relation to providers of public communication networks or publicly available electronic communications services, the obligation to establish an Incident response plan is explicitly laid out in Art. 17 of Act 205/2013 of the Hellenic Authority for Communication Security and Privacy.

The GDPR, being applicable to all businesses, requires in its Art. 32 that Data Controllers and Data Processors take the appropriate technical measures to comply with the obligation of secure data processing. According to the interpretation of the Article, the Incident response plan/policy, the vulnerability assessment and the periodic penetration tests, while also not explicitly laid out within the text of the Regulation and Law 4624/2019, they are nonetheless implicitly included among the necessary measures that Data Controllers or Processors need to take. Finally, as regards the designation of a Data Protection Officer (DPO), Law 4624/2019 requires only public entities to appoint a DPO. While a DPO and a CISO should be in close collaboration, their role is distinct and as such an operational independence must be maintained between these two positions within an entity.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No further disclosure obligations are stipulated within the Greek legislation, aside from those mentioned in section 2 above.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Arts 79 and 82 GDPR (and Art. 40 of Law 4624/2019) provide for the right to an effective judicial remedy and the right of compensation respectively against a Controller or Processor of any data subject whose rights under the GDPR have been infringed as a result of the processing of his/her data in non-compliance with the GDPR. The infringement of a data subject's rights (Incident) may refer to a hack, or a violation or threat to the confidentiality, integrity and availability of the data subject's personal data that resulted in a material or non-material damage to the data subject. A critical element for the action to be established is the proof by the data subject of his/her harm as a result of the Incident.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

While there have been a few cases where administrative fines were imposed by the HDPA to companies for illegal processing of personal data (HELLENIC PETROLEUM GROUP) and for not taking adequate measures to safeguard the security of information systems that resulted in data breach (OLYMPION HOTEL, AEGEAN MARINE), there is not still any published case of a private action in relation to Incidents in the Greek jurisdiction in accordance with the GDPR. There is a number of civil dicta in relation to unlawful processing of personal data in accordance with the old personal data law, Law 2472/1997, which is still in force in complementarity with Law 4624/2019.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

According to Art. 40 of Law 4624/2019, transposing Art. 79 GDPR into Greek legislation, there may be tort liability for a Data Controller or a Data Processor in case a data subject suffers material or non-material damage from acts or omissions of the above persons violating the Regulation. More in particular, the negligence to prevent an Incident which results in a data breach, falls within the scope of the tort liability by giving rise to the right of compensation of the affected data subject. Civil liability arising from torts – both material and moral – is regulated by the Greek Civil Code under Arts 914 and 932, respectively.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, it is permitted for organisations to take out cyber insurance against Incidents in Greece. Such an insurance package could indicatively include insurance coverage for cybercrime, reputational harm, dependent business interruption and telephone hacking.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration. The offered insurance package is formed after negotiation of the concerned party with the competent insurance agent, taking into account the provisions of the Greek Insurance Contract Act (2496/1997).

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The HDPA, the ADAE, the Cyber Crime Unit of the Hellenic Police, as well as the Hellenic Cybersecurity Authority (established in 2018) are the competent authorities in Greece for the investigation of an Incident. It should be noted that the Hellenic Cybersecurity Authority, which reports to the Ministry of Digital Governance, consults and cooperates with the other competent national law enforcement authorities. The above-mentioned authorities, as law enforcement authorities, have the right to conduct audits and impose administrative fines or criminal sanctions in case they find that the existing institutional framework has been violated. Especially in the public sector, the competent authority for dealing with/protecting against cyber-attacks and threats to the public body and the critical infrastructure of the country is the National Cyber Attack Authority – National CERT.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no provisions of national applicable laws that require organisations to implement backdoors in their IT systems for law enforcement authorities. Nevertheless, as part of inspections or audits, the competent authorities may inspect the technological infrastructure and other means, whether automated or not, by requesting access to all data and information required for the purposes of the relevant inspection and the performance of their duties, without the audited entity being able to oppose such due to any kind of secrecy.

Dr. Nikos Th. Nikolinakos is the Managing Partner of Nikolinakos & Partners LLP and co-head of the TMT, Digital Business and Competition Law practices. He features prominently in the TMT, data protection/cybersecurity, competition law and IP rankings of leading bar publications such as *Chambers and Partners* and *The Legal 500*.

Nikos divides his specialised practice between regulatory and policy advice in the TMT sector, and in EU/national competition law, data protection & cybersecurity, IP rights advocacy and compliance. Prior to founding the firm, Nikos held the post of general counsel – legal and regulatory affairs director for a major telecoms operator and internet provider in Greece. He also held the position of senior in-house adviser to the Telecommunications & Post Commission of Greece (EETT), responsible for competition law and regulatory policy/compliance. He has filled senior consulting roles in various international projects for governments, national regulatory authorities, market players and the European Commission.

Nikos has been a Visiting Lecturer on electronic communications law, data protection/cybersecurity, intellectual property and competition law at the AIT Center and at NTUA (the National Technical University of Athens). Nikos is the author of numerous contributions in books and refereed journals in the fields of TMT and competition law. He is also the author of *EU Competition Law and Regulation in the Converging Telecommunications, Media & IT Sectors* (2006, Kluwer Law International/Aspen Publishers).

Nikolinakos & Partners Law Firm
182, Mesogeion Avenue
15561, Athens
Greece

Tel: +30 213 002 0020
Email: nikolinakos@nllaw.gr
URL: www.nllaw.gr

Dina Th. Kouvelou is a Partner, head of the Data Protection & Cybersecurity practice and co-head of the TMT and Digital Business practice of Nikolinakos & Partners LLP. Dina is recommended as a leading TMT, data privacy and competition legal counsel by *Chambers and Partners* ("a true TMT expert", "a competition law expert who is extremely business oriented, proactive, and an effective strategist") and *The Legal 500* ("an outstanding regulatory counsel" who "provides a hard-to-find combination of technical and practical legal advice").

During the last 20 years, Dina's professional career has spanned TMT, data protection, betting & gaming, competition law and corporate/commercial law experience in, amongst others, the following roles: general counsel and head of legal & regulatory affairs in a leading alternative fixed telecoms operator and in a mobile operator in Greece; senior competition law and regulatory policy advisor in the Legal Department of the EETT; and legal consultant in regulatory, competition law and commercial law projects with Greek and international law firms and consultancies.

Nikolinakos & Partners Law Firm
182, Mesogeion Avenue
15561, Athens
Greece

Tel: +30 213 002 0020
Email: kouvelou@nllaw.gr
URL: www.nllaw.gr

Nikolinakos & Partners is an Athens-based law firm built upon a strong regulatory, transactional and litigation foundation. Our specialisation covers, *inter alia*, the following areas: Telecommunications, Media & Technology (TMT); Digital Business; Data Privacy & Cybersecurity; Competition Law; Intellectual Property; Administrative Law; and Agency Litigation.

Ranked #1 in Greece by the most prestigious international legal directories (for the ninth consecutive year) in TMT, Digital Business, and Data Protection & Cybersecurity.

The firm is highly recommended by *Chambers and Partners* and *The Legal 500*. Indicatively: "Nikolinakos & Partners LLP has a top-notch practice for data privacy and cybersecurity matters"; "the practice excels on the dispute resolution, GDPR, licensing and data protection fronts"; "considerable expertise in GDPR compliance matters"; "at the forefront of the telecoms, data protection and technology sectors/areas"; and "lawyers at Nikolinakos & Partners Law Firm are hailed as leaders in regulatory litigation and are also strongly recommended for TMT, antitrust and data protection disputes".

www.nllaw.gr

NIKOLINAKOS & PARTNERS
LAW FIRM

Ireland


Claire Morrissey


Kevin Harnett

Maples Group

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking is an offence under section 2 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 (the "**2017 Act**"). A person who, without lawful authority or reasonable excuse, intentionally accesses an information system by infringing a security measure, commits an offence.

Denial-of-service attacks
Denial-of-service attacks are an offence under section 3 of the 2017 Act. A person who, without lawful authority: intentionally hinders or interrupts the functioning of an information system by inputting data on the system; transmits, damages, deletes, alters or suppresses, or causes the deterioration of, data on the system; or renders data on the system inaccessible, commits an offence.

Phishing
Phishing does not, *per se*, constitute a specific offence in Ireland. However, it is possible that the activity would be caught by certain other, more general criminal legislation, depending on the circumstances (for instance, relating to identity theft or identity fraud). In this regard, see below.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware is an offence under section 4 of the 2017 Act. A person who, without lawful authority, intentionally deletes, damages, alters or suppresses, or renders inaccessible, or causes the deterioration of data on an information system commits an offence.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Distribution, sale or offering for sale hardware, software or other tools used to commit cybercrime also constitutes an offence under the 2017 Act (section 6). It occurs when a person who, without lawful authority, intentionally produces, sells, procures for use, imports, distributes, or otherwise makes available, for the purpose of the commission of an offence under the 2017 Act, certain hacking tools.

Possession or use of hardware, software or other tools used to commit cybercrime
As above, possession or use of hardware, software or other tools used to commit cybercrime constitutes an offence under the 2017 Act (section 6).

Identity theft or identity fraud (e.g. in connection with access devices)
Although there is no precise, standalone offence of identity theft or identity fraud in this jurisdiction, it can nonetheless potentially be captured by the more general offence referred to as "making a gain or causing a loss by deception" (as contained in section 6 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (the "**2001 Act**")). This occurs where a person who dishonestly, with the intention of: making a gain for himself, herself or another; or causing loss to another, by any deception induces another to do or refrain from doing an act. In addition, sections 25, 26 and 27 of the 2001 Act cover specific forgery offences.

Separately, under section 8 of the 2017 Act, identity theft or fraud is an aggravating factor when it comes to sentencing, in relation to "denial-of-service attack" or "infection of IT systems" offences.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft is covered by the relatively broad offence of "unlawful use of a computer", as provided for in section 9 of the 2001 Act. This occurs where a person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself, herself or another, or of causing loss to another.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Unsolicited penetration testing is an offence under the 2017 Act (section 2) where it involves intentionally accessing an IT system by infringing a security measure without lawful authority (i.e. permission of the system owner/right holder or where otherwise permitted by law) or "reasonable excuse". This term is not defined under the 2017 Act, and its application will depend on future judicial interpretation.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Section 5 of the 2017 Act creates the offence of "intercepting the transmission of data without lawful authority". This occurs when a person who, without lawful authority, intentionally intercepts any

transmission (other than a public transmission) of data to, from or within an information system (including any electromagnetic emission from such an information system carrying such data).

With regard to penalties, in relation to offences under the 2017 Act, the penalties range from maximum imprisonment of one year and a maximum fine of €5,000 for charges brought "summarily" (i.e. for less serious offences), to a maximum of five years' imprisonment (10 years in the case of denial-of-service attacks) and an unlimited fine for more serious offences. The above offences under the 2001 Act are only tried in the Circuit Court, with "making a gain or causing a loss by deception" carrying a maximum penalty of five years' imprisonment and an unlimited fine, and forgery and "unlawful use of a computer" offences carrying a maximum of 10 years and an unlimited fine.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the above offences under the 2017 Act have certain extra-territorial application, and so offenders may therefore be tried in Ireland, so long as they have not already been convicted or acquitted abroad in respect of the same act.

Although broader concepts such as, for instance, the "European arrest warrant" may be of relevance for Irish prosecutors, none of the above-mentioned offences under the 2001 Act carry, in and of themselves, extraterritorial application.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Each of the above offences under the 2017 Act contain the ingredient that it was committed without "lawful authority" (i.e. permission of the system owner/right holder or where otherwise permitted by law). Accordingly, prosecution of these offences will require, necessarily, that such authority or lawful permission was absent.

In addition, the offence relating to "hacking" carries a further qualification, i.e., where the person or company had a "reasonable excuse". This term is not defined under the 2017 Act, and so its application will depend on future judicial interpretation.

If a company is charged with any of the above 2017 Act offences where the offence was committed by an employee for the benefit of that company, it will be a defence for that company that it took "all reasonable steps and exercised all due diligence" to avoid the offence taking place.

It can be expected that judges will continue to take established factors into account when considering the appropriate penalty on foot of a conviction of a cybersecurity-related crime (e.g. remorse, amends, cooperation with investigators, criminal history, and extent of damage).

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Apart from the above-referenced statutes in respect of criminal activity, Applicable Laws include the following:

- **Data Protection**: The General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**") and the Data Protection Acts 1988 to 2018 ("**DPA**") govern the manner in which personal data is collected and processed in Ireland. Data controllers are required to take "appropriate security measures" against unauthorised access, alteration, disclosure or destruction of data, in particular where the processing involves transmission of data over a network, and comply with strict reporting obligations in relation to Incidents. The DPA also provides for offences related to disclosure and/or sale of personal data obtained without prior authority.
- **e-Privacy**: The e-Privacy Regulations 2011 (S.I. 336 of 2011), which implemented the e-Privacy Directive 2002/58/EC (as amended by Directives 2006/24/EC and 2009/136/EC) (the "**e-Privacy Regulations**"), regulate the manner in which providers of publicly available telecommunications networks or services handle personal data and require providers to take appropriate technical and organisational measures to safeguard the security of its services and report Incidents. It also prohibits interception or surveillance of communications and the related traffic data over a publicly available electronic communications service without users' consent. It was intended that a revised EU e-Privacy Regulation be introduced in May 2018 to replace the existing e-Privacy Directive and e-Privacy Regulations, expanding the current regime to cover all businesses which provide online communication services. That new regulation is still in draft form.
- **Payments Services**: The Payments Services Directive II (Directive 2015/2366/EU or "**PSD2**"), was transposed by the European Union (Payment Services) Regulations 2018 (S.I. 6 of 2018) (the "**Payment Services Regulations**"), and introduced regulatory technical standards (which were published by the European Banking Authority) to ensure "strong customer authentication" and payment service providers will be required to inform the national competent authority in the case of major operational or security Incidents. Providers must also notify customers if any Incident impacts the financial interests of its payment service users.

  The Security of Network and Information Systems Directive 2016/1148/EU (the "**NISD**") was transposed into Irish law under S.I. 360/2018 European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 ("**NISD Regulations**").
- **Other**: If there is a security breach which results in the dissemination of inaccurate information, persons about whom the inaccurate data relates may seek a remedy under the Defamation Act 2009 or at common law for breach of confidence or negligence.

See also sections 1 and 5.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The NISD Regulations and Commission Implementing Regulation (EU) 2018/151, which specifies further elements to be taken into account when identifying measures to ensure security of network and information systems, will apply.

The National Cyber Security Strategy 2019–2024 provides a mandate for the National Cyber Security Centre ("**NCSC**") to engage in activities to protect critical information infrastructure.

Enforcement powers under the NISD Regulations also allow NCSC-authorised officers to conduct security assessments and audits, require the provision of information and issue binding instructions to remedy any deficiencies.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the GDPR and DPA, controllers are required to take appropriate measures, as outlined in questions 1.1 and 2.1 above. The GDPR and DPA do not detail specific security measures to be undertaken but, in determining appropriate measures, a controller may have regard to the state of technological development and the cost of implementing the measures. Controllers must ensure that the measures provide a level of security appropriate to the harm that might result from a breach and the nature of the data concerned. The Data Protection Commission ("**DPC**") has issued guidance for controllers on data security recommending access controls, automatic screen-savers, encryption, anti-virus software, firewalls, software patching, secure remote access, logs and audit trails, back-up systems and Incident response plans. The DPC has also issued guidance on phishing and social engineering attacks, securing cloud-based environments and engaging cloud service providers.

Under the e-Privacy Regulations, providers of publicly available telecommunications networks or services are required to take appropriate technical and organisational measures and ensure the level of security appropriate to the risk presented, having regard to the state of the art and cost of implementation. Such measures shall at least ensure that personal data can only be accessed by authorised personnel for legally authorised purposes, protect personal data against accidental or unlawful destruction, loss, alteration, processing, etc., and ensure the implementation of a security policy.

The NISD Regulations require that operators of essential services ("**OES**") and digital services take appropriate measures to prevent and minimise the impact of Incidents affecting the security of the network and information systems used for the provision of essential and digital services with a view to ensuring continuity.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Where a personal data breach occurs, the controller shall without undue delay and, where feasible, within 72 hours of becoming aware of the breach, notify the DPC of the breach. This notification shall include a description of the breach, the number or approximate number of data subjects concerned and personal data records concerned. It must also contain a list of likely consequences of the breach and measures taken or proposed to be taken to address the breach.

Where a data breach occurs that is likely to result in a high risk to the rights and freedoms of a data subject, the controller must notify the data subject to whom the breach relates. The requirement is waived where the controller has implemented appropriate measures to protect the data; in particular where the measures render the data unintelligible through encryption or otherwise to any person not authorised to access it. This notification must contain at least the same information provided to the DPC as described above. The DPC and European Data Protection Board guidelines on data breach notification have been published.

Providers of publicly available telecommunications networks or services are required to report information relating to Incidents or potential Incidents to the DPC (to the extent that such Incidents relate to personal data breaches). In the case of a particular risk of a breach to the security of a network, providers of publicly available telecommunications networks or services are required to inform their subscribers concerning such risk without delay and, where the risk lies outside the scope of the measures to be taken by the relevant service provider, any possible remedies including an indication of the likely costs involved. In case of a personal data breach, such providers must notify the DPC without delay and, where the said breach is likely to affect the personal data of a subscriber or individual, notify them also. If the provider can satisfy the DPC that the data would have been unintelligible to unauthorised persons, there may be no requirement to notify the individual or subscriber of the breach.

The NISD Regulations require OES and digital providers to notify the NCSC without delay of any Incident having a substantial impact on the provision of a service. The notification must provide sufficient information so that the NCSC can assess the significance of same and any cross-border impact. The NISD Regulations stipulate that notification shall not make the notifying party subject to increased liability.

Section 19 of the Criminal Justice Act 2011 mandates reporting certain cybercrimes to the Irish police force, An Garda Síochána. Failure to make such a report, without reasonable excuse, is an offence.

The Central Bank of Ireland's ("**CBI**") *Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks* ("**Cross Industry Guidance**") requires firms to notify the Bank when they become aware of a cybersecurity Incident that could have a significant and adverse effect on the firm's ability to provide adequate services to its customers, its reputation or financial condition.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

See question 2.4 above.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

See question 2.4 above.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Failure to have appropriate security measures in place and/or report a data security breach in accordance with the GDPR can result in one of a number of administrative sanctions, including a ban on processing and fines of up to €10 million or 2% of the global turnover as set out in Article 83 of the GDPR.

Failure by providers of publicly available telecommunications networks or services to comply with the above-mentioned requirements under the e-Privacy Regulations is an offence, liable to a fine of up to €250,000. If a person is convicted of an offence, the court may order any material or data that appears to it to be connected with the commission of the offence to be forfeited or destroyed and any relevant data to be erased.

Failure by an operator of essential services or a digital service provider to notify an Incident is an offence under the NISD Regulations liable to a fine of up to €500,000.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The DPC has a number of ongoing inquiries into multinational tech companies, including an investigation into Twitter's compliance with its obligations under the GDPR to implement technical and organisational measures to ensure the safety and safeguarding of the personal data it processes. It also submitted a draft decision in May 2020 to other concerned data supervisory authorities in relation to Twitter's compliance with its data breach notification obligations in connection with a breach reported in January 2019.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of beacons for such purposes.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of honeypots for such purposes.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of sinkholes for such purposes.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Monitoring or interception of electronic communications on private networks to prevent or mitigate the impact of cyber-attacks must comply with the GDPR's requirements including in relation to transparency, necessity and proportionality. The e-Privacy Regulations prohibit interception or surveillance of communications and the related traffic data over a publicly available electronic communications service without users' consent.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

The export of dual use technology (i.e. technology that can be used for both civil and military purposes) is restricted. Most dual-use items can move freely within the EU. However, a licence is required to export them to a third country (i.e. outside the EU). Very sensitive items, such as equipment or software designed or modified to perform "cryptanalytic functions", require a transfer licence for movement within the EU.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, market practice with respect to information security varies considerably in Ireland depending on the industry sector concerned. Businesses in industries that are recognised as being particularly vulnerable to Incidents, such as the financial services sector, are more likely to have adequate processes in place to effectively address cyber risk. With current and long-term trends, such as the continued expansion of cloud computing, mobile data and the internet of things further increasing exposure to cyber risk, financial services firms are expected to update and implement their processes accordingly. The CBI's Cross Industry Guidance provides valuable information on the practices that financial services firms are expected to apply in order to protect their organisations from cyber threats.

Other industries have previously been less cognisant of the need for adequate cybersecurity protections. However, advances in robotics, technology and the digital marketplace have increased awareness across other industries of the need for maintenance and protection of cyber infrastructure.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

(a) There is currently no specific legislation focused on cybersecurity applicable to organisations in the financial services sector, but the CBI's Cross Industry Guidance will apply. The publication makes a number of recommendations including (but not limited to): the preparation of a well-considered and documented strategy to address cyber risk; the implementation of security awareness training

programmes; the performance of cyber risk assessments on a regular basis; and the implementation of strong controls by firms over access to their IT systems. The NISD Regulations introduce security measures and Incident reporting obligations for credit institutions. See also reference to Payment Services Regulations in question 2.1 above.

(b) As noted above, electronic communications companies (such as telecoms companies and ISPs) are governed by the GDPR, the DPA, and also the e-Privacy Regulations. Certain operators (IXPs, DNS service providers and TLD name registries) also now fall within the ambit of the NISD Regulations together with essential operators in the energy, transport, health, drinking water and digital infrastructure sectors.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

While there are no express directors' duties specific to cybersecurity, directors owe fiduciary duties to their company under common law and under the Companies Act 2014 (the "**CA 2014**").

There are a number of key fiduciary duties of directors set out in the CA 2014. This list, however, is not exhaustive. Some examples of directors' duties which could be considered to extend to cybersecurity are to:

- exercise their powers in good faith in what the director considers to be the interests of the company;
- act honestly and responsibly in relation to the conduct of the affairs of the company;
- act in accordance with the company's constitution and exercise his or her powers only for the purposes allowed by law;
- exercise the care, skill and diligence which would be exercised in the same circumstances by a reasonable person having both the knowledge and experience that may reasonably be expected of a person in the same position as the director with the knowledge and experience which the director has; and
- have regard to the interests of its employees in general.

Directors have a general duty to identify, manage and mitigate risk, as well as fiduciary duties, such as those outlined above, which would extend to cybersecurity. Such duties could be interpreted to mean that directors should have appropriate policies and strategies in place with respect to cyber risk and security and that directors should review and monitor these on a regular basis. Regard may also be had to compliance by a company with all relevant legislative obligations imposed on that company in assessing compliance by directors with their duties. Appropriate insurance coverage should also be considered.

Directors should be fully briefed and aware of all of the key issues relating to cyber risk. Larger organisations may choose to delegate more specific cyber risk issues to a specific risk sub-committee.

In relation to company secretaries, this will depend on what duties are delegated to the company secretary by the board of directors.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

While there are no such express obligations from a company law perspective, general director fiduciary duties, best corporate governance practices, as well as the "appropriate security" requirements under the DPA, may dictate that such actions are performed. See question 5.1 above for more detail on directors' duties. For industry-specific requirements, see question 4.1 above.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

While there are no such express obligations from a company law perspective, general director fiduciary duties, as well as best corporate governance practices, may dictate that such actions are performed. See question 5.1 above for more detail on directors' duties.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

As discussed in response to question 6.3 below, an Incident may give rise to various claims under the law of tort. It is also conceivable that an Incident would, depending on the circumstances, give rise to a claim for breach of contract.

In order to be entitled to compensation in damages, whether under a tortious or contractual analysis, a plaintiff will be required to establish: that a duty or obligation was owed to him/her by the defendant; that an Incident has occurred as a result of the defendant acting in breach of that duty or obligation; and loss or damage has been sustained to the plaintiff which would not have been sustained, but for the defendant's conduct.

Many classes of Incident may also give rise to claims for damages for breach of the constitutional right to privacy.

Where an Incident is committed by a State actor, for example, during the course of an investigation, it may give rise to an action in judicial review to prevent misuse of any inappropriately obtained data and/or to quash any decision taken in relation to, and/or on foot of, the Incident or any improperly obtained data.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

CRH plc and Others v Competition and Consumer Protection Commission [2017] IECS 34 – The Supreme Court upheld the finding of the High Court that, in seizing material unrelated to an investigation, the Competition and Consumer Protection Commission

had acted outside the scope of its statutory powers and would be acting in breach of the applicants' rights to privacy were it to examine such material. In the exercise by the State of its powers of search, the Supreme Court held that interference with the right to privacy was inevitable but that such interference must be proportionate.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Depending on the specific type of Incident concerned, liability in tort may arise. Examples of such tortious liabilities are as follows:

- The DPA permits a data subject to take a data protection action against a controller or processor where they believe their rights have been infringed.
- A breach of a person's privacy rights may give rise to a claim in tort for breach of confidence or negligence, depending upon the circumstances.
- Incidents involving the theft of information or property may give rise to claims in the tort of conversion.
- Incidents involving the publication of intrusive personal information may, in some circumstances, constitute the tort of injurious or malicious falsehood.
- Incidents involving the misuse of private commercial information may give rise to claims for damages for tortious interference with economic relations.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

"Cyber insurance" products are being taken up by businesses with increasing frequency and are now seen as routine. Such products afford cover for various data- and privacy-related issues including: the financial consequences of losing or misappropriating customer or employee data; the management of a data breach and attendant consequences, including the costs associated with involvement in an investigation by the DPC; and the costs associated with restoring, recollecting or recreating data after an Incident.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limits placed on what an insurance policy can cover. However, GDPR and DPA administrative and criminal fines are not likely to be insurable in Ireland as a matter of public policy. Similarly, in the ordinary way, the consequences of intentional wrongdoing tend to be contractually excluded, as are the consequences of failure to remedy ascertained weaknesses or shortcomings in systems.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Under the 2017 Act, the Irish police force is given a relatively broad authority to investigate cybersecurity Incidents or suspected activity. Specifically, a warrant is obtainable so as to enter and search a premises, and examine and seize (demanding passwords, if necessary) anything believed to be evidence relating to an offence, or potential offence, under the 2017 Act, from a District Court Judge on foot of a suitable Garda statement, on oath.

The DPC has broad powers to investigate breaches under the DPA, including the power to enter business premises unannounced and without a court-ordered search warrant.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no requirements under Irish law for organisations to implement backdoors to their IT systems for law enforcement authorities, or to provide law enforcement authorities with encryption keys.

Claire Morrissey is a Partner and head of the Dublin Data, Commercial and Technology practice at Maples and Calder, the Maples Group's law firm. Claire advises on a broad range of data protection issues and commercial contracts with a particular focus on compliance with the GDPR, technology and IP. In addition, Claire regularly advises on the technology, IP and data aspects of joint ventures and mergers & acquisitions.

Maples Group
75 St. Stephen's Green
Dublin 2, D02 PR50
Ireland

Tel: +353 1 619 2000
Email: claire.morrissey@maples.com
URL: www.maples.com

Kevin Harnett is a Partner in the Dublin Dispute Resolution & Insolvency team at Maples and Calder, the Maples Group's law firm. Kevin has extensive experience advising both domestic and multinational clients from diverse backgrounds on large and complex commercial disputes, including proceedings before the Commercial Court, as well as all forms of alternative dispute resolution. He has a particular focus on the financial services, technology, construction and property sectors.

Maples Group
75 St. Stephen's Green
Dublin 2, D02 PR50
Ireland

Tel: +353 1 619 2036
Email: kevin.harnett@maples.com
URL: www.maples.com

Israel


Haim Ravia


Dotan Hammer

Pearl Cohen Zedek Latzer Baratz

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Section 4 of the Israeli Computers Law, 5755-1995 criminalises unlawful intrusion into computer material. The term "intrusion into computerised material" is defined in the statute as "intrusion by communicating with or connecting to a computer, or by operating it, but excluding intrusion that constitutes wiretapping" under the Israeli Wiretap Law, 5739-1979. This offence carries a maximum penalty of three years' imprisonment.

Section 5 of the Computers Law penalises intrusion into computer material committed in furtherance of another predicate felony. The maximum penalty for this offence is five years' imprisonment.

A 2015 landmark Supreme Court judgment broadly interpreted the boundaries of the term "intrusion into computerised material" to cover any access to a computer absent of the owner's permission or some other legal authority. Prosecutions of this offence are becoming more abundant, such as with disgruntled former employees hacking into their former employer's systems, hackers hacking into web-connected cameras, terrorism-oriented hacking and bank account hacking.

Denial-of-service attacks
Denial of service attacks fall within the scope of Section 2 of the Israeli Computers Law, which penalises any obstructions to the ordinary operation of a computer or interference with its use. The maximum penalty for this offence is three years' imprisonment.

Phishing
Phishing falls within the scope of two traditional offences codified in the Israeli Penal Law, 5737-1977, the first being receipt of something by fraud (Section 415 of the Penal Law). This offence is punishable by a maximum term of three years in prison, but if the offence is committed in aggravating circumstances, the maximum punishment is five years in prison. The second offence is receipt of something by ploy or by intentional exploitation of another person's mistake (Section 416 of the Penal Law), punishable by two years' imprisonment. These offences have been the subject of indictments such as online bank account phishing and Facebook account phishing.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Section 6 of the Israeli Computers Law criminalises the programming or adaptation of a computer program for the purpose of unlawfully performing any one of six enumerated acts. Among the enumerated acts is interfering with the ordinary operation of a computer, impacting the integrity of computerised content, facilitating unlawful intrusion into computers or invading a person's privacy. This offence is punishable by up to three years' imprisonment. The act of trafficking in or installing such computer programs is punishable by up to five years in prison. Developers and distributers of spyware, worms, trojans and viruses have been prosecuted under these provisions.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Section 6 of the Israeli Computers Law criminalises the distribution, sale or offering of any tool used to commit a cybercrime. Among the enumerated acts is distributing, offering to the public, or transmitting to another person, tools used to commit a cybercrime, as well as penetrating another person's computer or installing computer software or hardware on another person's computer for the purpose of committing a cybercrime enumerated under this section. This offence is punishable by up to five years' imprisonment.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The installation of software or other tools used to commit cybercrime is an offence under Section 6 of the Israeli Computers Law. This also applies to hardware with a firmware component. While mere possession is likely not an offence, it may amount to an attempt to commit the offence. An attempt is punishable by the same prison term prescribed for the completed offence.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft or identity fraud can give rise to two traditional offences codified in the Israeli Penal Law, 5737-1977 – receipt of something by fraud and receipt of something by ploy, both discussed above. In addition, using the identity credentials of another person can give rise to the offence of impersonating another person with intent to defraud, codified in Section 441 of the Israeli Penal Law and punishable by up to three years in prison.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft can give rise to the traditional offence of larceny codified in the Israeli Penal Law, punishable by up to three years

in prison, or up to seven years if the stolen property is valued at ILS 500,000 or more. Theft by an employee is a more egregious offence, punishable by up to seven years' imprisonment. If the theft involves data whose confidentiality was compromised by the theft, and the confidentiality arises from an obligation under law, the theft amounts to a criminal invasion of privacy punishable by up to five years' imprisonment.

Copying, importing, renting out or distributing infringing copies of copyrighted material, as well as possession of such copies for the purpose of trafficking are offences under the Israeli Copyright Law, 5768-2007 if they are committed in a commercial scope. These are punishable by up to five years' imprisonment.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine vulnerabilities and weak points)

Unsolicited penetration testing, in certain circumstances, may fall within the scope of the prohibitions under Section 4 of the Israeli Computers Law, 5755-1995, which criminalises unlawful penetration into computer material.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Other activities that adversely affect or threaten the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data are likely captured by the above offences.

Failure by an organisation to implement cybersecurity measures

Under the Israeli Protection of Privacy Law, 5741-1981, certain organisations are required to appoint an information security officer. Details can be found in the answer to question 4.2 below. Under Section 31A(a)(6) of the Israeli Protection of Privacy Law, failure to appoint an information security officer where such is mandated by the law is a strict lability offence punishable by up to one year in prison.

According to the first Schedule of the Administrative Offenses Regulations (Administrative Fine – Protection of Privacy), 2004 (the "Administrative Offenses Regulations"), failure to appoint an information security officer where such is mandated by the law can give rise to an administrative offence. The fine set for this offence is 3,000 NIS for an individual and 15,000 NIS for an organisation.

Under the Protection of Privacy Regulations (Data Security), 5777-2017, most organisations that own, manage or maintain a database containing personal data are required to implement prescriptive security measures, whose main objective is the prevention of Incidents. Details can be found in the answer to question 2.3 below. Failure to comply with the regulations may result in the imposition of sanctions by the Privacy Protection Authority, including the revocation of the regulatory authorisation to use the database and the public disclosure of the details of the Incident (the data breach) by the Privacy Protection Authority, which in turn may lead to a class action lawsuit filed against the database owner.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The above offences have extraterritorial application in three main scenarios. First, if the offence was only partially committed outside Israel, the conduct will be fully captured by the above offences.

Second, if preparations to commit the offence, an attempt to commit it, inducement of another to commit the offence, or conspiracy to commit the offence were performed outside Israel, but the completed offence would have been committed in whole or in part in Israel, then the conduct will be fully captured by the above offences.

Finally, where an offence was committed outside Israel but was targeted against the State of Israel in the broad sense of the phrase (e.g., against national security, the State's regime, the State's property or economy), or was committed by an Israeli resident or citizen, then the conduct will be fully captured by the above offences.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The traditional affirmative defences to criminal culpability also apply to these offences. These defences include necessity, duress and self-defence, yet the bar is rather high to meet. Additionally, both prosecutorial discretion and sentencing guidelines would take into account mitigating factors such as the severity of the conduct, the degree of wilfulness, the scope of harm or affected victims, the motives, etc.

Courts have repeatedly ruled that unauthorised intrusion into a computer material is prohibited regardless of its motives, and the 2015 landmark Supreme Court judgment reinforces this approach. Yet, in 2004, the District Court of Jerusalem upheld a Magistrate's Court's ruling that unsolicited penetration testing may be permissible in some circumstances. The court stated that the unlawfulness of the penetration depends on the circumstances and the intentions of the defendant.

A person who tests the vulnerability of websites with good intentions, to some extent, acts for the benefit of the public and may create incentives for database owners to better secure their databases. In terms of public policy, the 2004 court decision ruled that website owners should not be allowed to penalise anyone who penetrates their server in order to test security measures.

2 Cybersecurity Laws

2.1 *Applicable Law:* Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Laws applicable to cybersecurity include the Israeli Computers Law, the Protection of Privacy Law, the Copyright Law, the Penal Law, the Defense Export Control Law, the Regulation of Security in Public Bodies Law, and the recently proposed Cyber Defense and National Cyber Directorate Bill.

2.2 *Critical or essential infrastructure and services:* Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Regulation of Security in Public Bodies Law authorises

the Israeli Security Agency and the National Cyber-defense Authority to issue binding directives to organisations operating critical infrastructures or essential services on matters related to information security and cybersecurity, and inspect such organisations' compliance with those directives. Organisations subject to this regime include telecom and internet providers, transportation carriers, the Tel Aviv Stock Exchange, the Israeli Internet Association, utility companies and others.

2.3 *Security measures:* Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Aside from the cybersecurity requirements applicable to critical infrastructures as explained in the preceding question, the Protection of Privacy Regulations (Data Security), 5777-2017, is an omnibus set of rules. It requires any Israeli organisation that owns, manages or maintains a database containing personal data, to implement prescriptive security measures whose main objective is the prevention of Incidents. These include, for example, physical security measures, access control measures, risk assessment and penetration tests. The regulations classify databases into four categories (basic, intermediate, high and those held by individuals), with each subject to an escalating set of information security requirements.

The regulations also require organisations to monitor and document any event that raises suspicion of compromised data integrity or unauthorised use of data.

Additionally, organisations that hold certain sensitive information are required under the data security regulations to implement an automated audit mechanism to monitor any attempt to access information systems that contain personal data. Sensitive information covers information regarding an individual's private affairs, including: individuals' behaviour in the private domain; health or mental condition; political opinions or religious beliefs; criminal history; telecommunication meta data; biometric data; financial information regarding individuals' assets, debts and economic liabilities; and consumption habits of an individual which may be indicative of the above-mentioned types of data.

In addition, financial institutions and insurance companies are required to operate a security operation centre tasked with monitoring, detecting and mitigating cybersecurity risks.

2.4 *Reporting to authorities:* Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There are several provisions according to which certain organisations are required to report Incidents.

First, under the Israeli data security regulations, any organisation that is subject to the intermediate security level or the high security level is required to notify the Privacy Protection Authority (the Israeli privacy regulator) of the Incident. The notification must state the measures taken to mitigate the Incident. The Privacy Protection Authority is vested with investigative powers and can request and obtain additional information accessible to the organisation about the Incident, including malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology.

The intermediate security level applies to public agencies, organisations that hold sensitive information and data brokers. The high security level applies to organisations that hold sensitive information and to data brokers; in each case this is applicable where there are at least 100,000 data subjects or more than 100 persons with access credentials.

Second, financial institutions and insurance companies are required to report Incidents pursuant to regulatory guidelines by the Israeli Banking Supervisor. Insurance companies are required to report to the Israel's Capital Market, Insurance and Savings Authority within the Ministry of Finance.

Third, under the Cyber Defense and National Cyber Organization Draft Bill, the National Cyber Organization and the Israeli Security Agency (colloquially known as the Shin Bet) can approach any organisation in Israel and demand any document and information it has relating to an Incident, instruct the organisation on how to operate its IT system and seize computers, communication systems and drives containing data. To date, this draft bill was not enacted.

There are no formally specified defences or exemptions by which an organisation might prevent publication of information relating to an Incident.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

In certain circumstances, the Privacy Protection Authority, upon consultation with the Head of the National Cybersecurity Authority, may instruct an organisation to report the Incident to all affected data subjects. A policy document published in this regard clarifies that, as part of the considerations in deciding whether or not to instruct the organisation to notify data subjects, the Israeli Privacy Protection Authority will examine whether the personal information was in fact compromised and will consider the severity of the risk to data subjects. To date, no known case has prompted the Israeli Privacy Protection to instruct the issuance of data subject notifications, and thus the particulars of this issue have not yet played out.

Additionally, in June 2020, a member of the Israeli parliament proposed a bill to impose a broad obligation to notify data subjects and the regulator in case of a data breach. However, private bills initiated by members of parliament without governmental support usually do not successfully pass the legislative process in the Knesset (the Israeli parliament). Therefore, it is not certain that the bill will ultimately be enacted.

2.6 *Responsible authority(ies):* Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The Privacy Protection Authority is responsible for enforcing the data security regulations. The Banking Supervisor at the

Bank of Israel is responsible for enforcing the data breach rules relating to Incidents in banks and credit card companies. The Supervisor of Capital Markets, Insurance and Savings within the Israeli Ministry of Finance is responsible for enforcing the data breach rules relating to Incidents at insurance companies.

2.7 *Penalties:* What are the penalties for not complying with the above-mentioned requirements?

There are currently no penalties imposable by the Israeli privacy regulator for failing to comply with the data breach notification requirement. However, in such cases, the Privacy Protection Authority is authorised to publicly disclose the details of the Incident which may lead to a class action lawsuit files against the database owner.

2.8 *Enforcement:* Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In February 2020, during the Israeli elections, the State of Israel's voter register was leaked in its entirety and was allegedly available on the Internet. The leak occurred following a security breach discovered in the "Elector" app, which was used by the "Likud" party in the election campaign. Following the leak, the Privacy Protection Authority conducted an investigation at Elector's offices to determine whether it had violated the data security regulations and its obligations under the Protection of Privacy Law. The Likud party continued to use the app.

In 2017, the Israeli privacy regulator investigated a data breach revealed in an Israeli company in the business of vehicle location monitoring. The data breach was revealed by an anonymous hacker, who exploited a security vulnerability in the company's website. The regulator launched enforcement action against the company and concluded that it had violated the Israeli data security regulations by not providing a timely notice to the regulator about the Incident.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
The use of beacons could arguably amount to unlawful intrusion into computer material but could be defensible under the affirmative defences of necessity or self-defence.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
The use of honeypots for detection purposes is likely permissible so long as it does not involve unlawful intrusion into the cyber threat actors' computers or invasion of their privacy (although these may in turn be defensible under the affirmative defences of necessity or self-defence). Use of honeypots for counter-attacks would amount to unlawful intrusion into the cyber threat actors' computers and other correlative offences.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The use of sinkholes for deflection purposes is likely permissible so long as it does not involve unlawful intrusion into the another person's computer, invasion of their privacy or interference with the ordinary functioning of their computer (although these may in turn be defensible under the affirmative defences of necessity or self-defence).

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Israeli legislation does not specifically address the issue of monitoring and accessing employees' communications and files. This legislative gap has been filled by case law, the most notable being a judgment delivered by the Israeli National Labor Court in 2011, known as the "Isakov case". The judgment expounded Israeli privacy law as applied to employers monitoring and accessing employees' communications and files. The decision sets forth the boundaries of permissible access to employee's email communications. The ruling also sets forth a stringent set of pre-requisites and conditions for permissible access.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

The importation and exportation of encryption technology is regulated under the Israeli Order and Declaration on Oversight of Goods and Services (Dealings in Means of Encryption). Generally, the importation and exportation of encryption or decryption technology is prohibited absent a permit from the Israeli Ministry of Defense. There are various encryption technologies whose use is exempt from the need for a permit if they are not used by way of integrating them into another technology or modifying them. A violation of these rules is punishable by a fine and up to three years' imprisonment.

Other than encryption technology, defensive technology against cyber-attacks (distinguishable from offensive and counter-attack technology) is generally not restricted for import or export.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Among those considered to be investing the most resources in cybersecurity are banks and credit card companies. This is likely due to them operating in a heavily regulated environment with a highly risk-averse regulator. At the other end of the spectrum are many small and medium businesses that often lack the resources for or awareness of cybersecurity and compliance with the Israeli data security regulations.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Banks and credit card companies are subject to the cybersecurity requirements laid down by the Supervisor of Banks at the Israeli Central Bank. One of the operative requirements for banking corporations and credit card companies is to appoint a cyber-defence manager and define the board of directors' responsibilities in this realm. They are required to continuously examine the effectiveness of the various cyber-defence controls that they have established – using tools such as vulnerability reviews and controlled-intrusion tests.

Insurance companies and investment firms are subject to the cybersecurity requirements laid down by the Supervisor of Capital Markets, Insurance and Savings. They are required, for instance, to approve, at least once a year, a corporate policy on cybersecurity risk management. They must appoint a chief cybersecurity officer and conduct an annual assessment of the suitability of defensive measures to the organisation's overall cybersecurity risks.

The Regulation of Security in Public Bodies Law authorises the Israeli Security Agency and the National Cyber-defense Authority to issue binding directives to telecom organisations operating critical infrastructures on matters related to information security and cybersecurity. These directives are not published.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

There has yet to develop any Israeli case law on the issue of directors' or officers' liabilities relating to cybersecurity, but directors' or officers' negligence on cybersecurity governance could amount to a breach of the directors' or officers' duty of care in turn. Additionally, cybersecurity guidelines issued by the Supervisor of Banks and the Supervisor of Capital Markets, Insurance and Savings, do specifically impose duties of oversight on the board of directors of these covered entities. Failure to do so may amount to the directors breaching their duty of care.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the Israeli Protection of Privacy Law, certain organisations are required to appoint an information security officer. These organisations include public agencies, service providers who process five or more databases of personal data by commission for other organisations and organisations that are engaged in banking, insurance and credit evaluation.

Organisations that are subject to the Israel data security regulations must establish and maintain procedures for Incident response.

Organisations that are subject to the intermediate or high security levels under the data security regulations are required to perform cyber risk assessments. Organisations that are subject to the high security level are also required to conduct assessments to identify cybersecurity risks.

Any organisation that is subject to the data security regulations is required to oversee and supervise its vendors' data security compliance on an annual basis.

Finally, organisations that are subject to the high level of security are required to perform penetration tests once every 18 months.

In addition, a legislative bill introduced by a member of the Knesset (the Israeli parliament), seeks to establish an obligation to appoint an official representative responsible for complying with privacy regulations in Israel when place of residence of the owner of a database is established outside of Israel. However, private bills initiated by members of parliament without governmental support usually do not successfully pass the legislative process in the Knesset (the Israeli parliament). Therefore, it is not certain that the bill will ultimately be enacted.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

All publicly traded companies are required to include in their periodic reports details of all types of risks that the company is exposed to in light of their line of business, the environment in which they operate and the characteristics unique to their operations. The Israeli Securities Authority published a circular emphasising a public company's duties of disclosure both of general cybersecurity risks that a company faces as well as of specific Incidents having material adverse effects on the company. Research conducted couple of years ago found that nearly half of the top 125 companies trading on the Tel Aviv Stock Exchange did not report cybersecurity as a risk.

5.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

We are not aware of any other requirements.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The most prominent civil action that may be brought against a legal entity in relation to an Incident is class action lawsuit in accordance with the Israeli Class Action Law, 5766-2006.

In order for the court to certify a class action suit, the representative plaintiff must prove that: (1) the action raises substantive questions of fact or in law common to all members of the putative class that were affected by the Incident, and that it is reasonably possible that such questions will be resolved in the class's favour; (2) under the circumstances of the case, a class action is the efficient and fair method to dispose of the dispute; (3) there are reasonable grounds to assume that the interests of all members of the class will be appropriately represented and conducted; and (4) there are reasonable grounds to assume that the interest of all members of the group will be represented and conducted in good faith.

In addition, any person or legal entity that suffered damages related to an Incident may assert a personal civil action based on several applicable laws; for example – invasion of privacy in accordance with the Protection of Privacy Law or for negligence in accordance with the Israeli Torts Ordinance.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

The Incident involving the "Likud" Party during the election, described in the answer to question 2.8 above, prompted a petition against the use of the app as well as a lawsuit by 20 Israelis.

The petition for a provisional injunction banning the use of the app, alleged a violation of voter privacy. The petition was denied by the chairman of the Central Election Commission, explaining that the Central Election Commission has no legal authority to enjoin the Likud from using the "Elector" app. The other lawsuit is still pending.

In addition, the Incident involving the vehicle monitoring company described in the answer to question 2.11 above has led to at least two class action suits filed against the company, alleging that the company negligently failed to safeguard consumer information.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

A person or entity responsible for safeguarding data against an Incident may arguably be liable in tort for failing to take the security measures required under the Israeli data security regulations in negligence or the tort of breach of a legal duty.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents; this is in fact becoming more common.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no noteworthy regulatory limits.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Israeli Police is empowered with general authority to investigate crimes and to seize documents, objects and computer materials that can potentially serve as evidence relating to the commission of a crime. Seizure of computers and computer material used by a business for investigation purposes requires a court order.

The Israeli Registrar of Databases has investigative powers relating to violations of the Israeli Protection of Privacy Law, including issues relating to the cybersecurity of databases containing personal data.

The Israeli Wiretap Law authorises investigative and security authorities to surreptitiously obtain the content of real time communications, for national security purposes or for the purpose of preventing and investigating serious crime. Wiretaps sought for preventing and investigating serious crime are subject to court approval, which in exceptional cases can be sought after the fact.

The Israeli Telecom Data Law provides police and various other investigative bodies with the authority to apply to the court of lowest instance in Israel to seek a comprehensive order to surreptitiously receive metadata (but not the content) of telecommunications, for the purpose of search and rescue, investigating or preventing crime, or seizing property. If metadata is required urgently and a court order cannot be obtained in time, such metadata may be obtained for a limited period of 24 hours, without a court order, subject to approval by a senior police officer.

The Israeli Privacy Protection Authority also has criminal investigatory powers as it can initiate an investigation of data breach and data crimes. Recently, the Privacy Protection Authority launched a criminal investigation against two suspects for data protection violations at an undisclosed airline.

Additionally, the Cyber Defense and National Cyber Directorate Bill granting far-reaching and unprecedented powers to the National Cyber Directorate, such as compelling organisations to produce any information or document required to handle cyber-attacks and authority to issue instructions to organisations, including instructions to carry out acts on the organisation's computerised material, for the purpose of handling cyber-attacks.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Section 11 of the General Security Service Law, 5762-2002 (the statute governing the operation of the Israeli Security Agency, colloquially known as "Shabak" or "Shin Bet"), grants the Prime Minister sweeping powers to order that metadata and non-real time telecommunications be retained by telecom providers and surreptitiously made available to the Shabak.

Section 13 of the Communications Law (Telecommunication and Broadcasts), 5742-1982, provides that the Prime Minister may order telecom service providers to render services to police, security agencies and intelligence agencies, and to have the providers install devices, take measures or adapt their facilities to assist the authorities.

Haim Ravia is a Senior Partner and Chair of the Internet, Cyber and Copyright Practice Group at Pearl Cohen Zedek Latzer Baratz. Haim deals extensively with data protection and privacy, cyber and internet law, IT contracts, copyright, electronic signatures, and open source software. Haim was a member of the Israeli public commission for the Protection of Privacy, and was part of a governmental team that re-examined the Israeli law pertaining to personal information databases. Haim received an acknowledgment award from the Israel Chamber of Information System Analysts for pioneering and innovation in the Israeli internet. Practising internet and cyber law for over 20 years, Haim has also written numerous columns on internet law for *Globes* (a major Israeli financial newspaper), the *Israel Bar Association Magazine* and other publications. Haim also operates Israel's first legal website (https://www.law.co.il) and publishes commentaries on Lexology.

Pearl Cohen Zedek Latzer Baratz
Azrieli Sarona Tower
121 Menachem Begin Rd.
Tel-Aviv, 6701203
Israel

Tel: +972 3 303 9058
Fax: +972 3 303 9001
Email: HRavia@PearlCohen.com
URL: www.pearlcohen.com / www.law.co.il

Dotan Hammer is a Partner and member of the Internet, Cyber and Copyright Group at Pearl Cohen Zedek Latzer Baratz. Dotan regularly advises on Israeli data protection and privacy laws. Having completed his academic degree in computer science at the age of 19, later working as a software developer and a technological project leader, Dotan also counsels clients on the privacy and data protections aspects of software and SaaS user agreements and licensing, as well as on other IT law matters such as digital (electronic) signatures, copyright issues and open source matters. Dotan regularly contributes to Israel's first legal website (https://www.law.co.il), Lexology and other online publications.

Pearl Cohen Zedek Latzer Baratz
Azrieli Sarona Tower
121 Menachem Begin Rd.
Tel-Aviv, 6701203
Israel

Tel: +972 3 303 9037
Fax: +972 3 303 9001
Email: DHammer@PearlCohen.com
URL: www.pearlcohen.com / www.law.co.il

Pearl Cohen Zedek Latzer Baratz ("Pearl Cohen") is an international law firm with offices in Israel, the United States and the United Kingdom, offering legal services across numerous practice areas.

Pearl Cohen's Data Protection and Privacy Practice Group in Israel comprises seasoned attorneys who leverage their nuanced understanding of new technologies and their experience in internet and cyber law to offer clients comprehensive legal services for the growing complexities of information and data privacy regulations.

At times, data protection and privacy matters entail court or administrative proceedings. Pearl Cohen's Data Protection and Privacy Practice Group has accumulated vast experience in representing clients before the Israeli Protection of Privacy Authority, and before Israeli courts in privacy and data protection litigation.

www.pearlcohen.com

PEARL COHEN

Italy


Alessandro Rubino


Gaetano Citro

Rubino Avvocati

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
The crime of abusive access to computer systems (Article 615-*ter* of the Italian Criminal Code).

Unlawful access to a computer system is the crime punishable under Article 615-*ter* of the Criminal Code, which states: "whoever unlawfully enters a computer or telematic system protected by security measures, or remains in it against the express or tacit will of the person who has the right to exclude him or her, shall be punished by imprisonment of up to three years". This applies where:

1. the act is committed by a public official or a person in charge of a public service, with abuse of powers;
2. the perpetrator uses violence against things or persons in order to commit the act, or if he is clearly armed; and
3. the act results in the destruction or damage to the system or the total or partial interruption of its operation.

Denial-of-service attacks
Damage to information, data or software (Article 635-*ter* of the Criminal Code).

This offence is committed when someone intentionally damages, destroys, deletes or disables any type of digital information, data or software owned by someone else. The penalty is imprisonment from six months to three years.

Phishing
Digital fraud (Article 640-*ter* of the Criminal Code). This offence is committed when a person – knowingly and with the intent to defraud – tampers with one or more digital devices, in violation of the law, using information, data or software for financial gain or in order to cause damage to someone else. The penalty is imprisonment from six months to three years.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Unauthorised access to a computer or telematic system (Article 615-*ter* of the Criminal Code). This offence requires a person to obtain access to a protected information system against the explicit or implicit consent of the person entitled to exclude third parties from obtaining such access. The penalty is imprisonment of up to three years.

Damage to information, data or software (Article 635-*bis* of the Criminal Code). The offence is committed when someone intentionally damages, destroys, deletes or disables any type of digital information, data or software owned by someone else. The penalty is imprisonment from six months to three years.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Under Article 615-*quinquies* of the Penal Code, whoever procures, produces, reproduces or simply makes available to others, equipment, devices or computer programs that have the objective of: unlawfully damaging a computer, telematic system, information, data or programs contained in it or relevant to it; or favouring the total or partial interruption or alteration of its functioning, can be imprisoned for up to two years or fined up to €10,329. This category includes malware, spyware, trojans, and the aforementioned diallers.

Possession or use of hardware, software or other tools used to commit cybercrime
The offence referred to can be included, as far as possible, in Article 615-*quater*, which provides that whoever, in order to procure a profit for himself or others or to cause damage to others, unlawfully procures, reproduces, disseminates, communicates or delivers codes, keywords or other means suitable for access to a computer or telematic system, protected by security measures, or in any case provides indications or instructions suitable for the aforesaid purpose, is punished with imprisonment of up to one year and a fine of up to €5,164.

Identity theft or identity fraud (e.g. in connection with access devices)
False identity (Article 494 of the Criminal Code). The article in question is applicable to real identities, as well as digital identities; the offence in question is committed when someone falsely and voluntarily takes the place of someone else. The penalty is imprisonment of up to one year.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
This crime is attributable to simple theft committed through hacking, punished as described under the point "Hacking" above, for which there will be the violation of two crimes: Articles 624 and 615-*ter* of the Penal Code.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
This type of crime falls within the case of abusive access to computer systems, Article 615-*ter* of the Criminal Code, when a penetration test is carried out by an individual, or by a group of persons, without any authorisation from the organisation subjected to such test, or any notification to the authorities.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Illegal interception and destruction of communications (Article 616 of the Penal Code). The offence is committed when a person opens, steals or destroys correspondence, including emails, not addressed to him or her. The penalty is imprisonment for up to one year.

Illegal interception, distortion, falsification and destruction of communications (Articles 617a to 617e of the Penal Code). These various offences, punishable under various articles of the Penal Code, are committed when a person opens, steals or destroys the correspondence of others, including emails, with software, malware or any type of digital tool having one of these purposes. The penalty is imprisonment from six months/one year to four years.

Illegal disclosure of emails (Article 618 of the Criminal Code). This offence is committed when a person intentionally discloses, or attempts to disclose, to any other person the content of any communication by cable, verbal or electronic means, knowing or having reason to know that the information has been obtained by interception by cable, verbal or electronic means in violation of this provision. The penalty is imprisonment for up to six months.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, where an IT crime is committed: in an Italian territory; or by subjects in connection with the Italian territory, has repercussions and is exclusively abroad.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Italian legislation provides justification for crimes that occur when said crime is committed:
- with the consent of the entitled person (Article 50 of the Criminal Code);
- in the exercise of a right and in the performance of a duty (Article 51 of the Criminal Code);
- in self-defence (Article 52 of the Criminal Code); and
- in a state of necessity (Article 54 of the Criminal Code).

However, it is at the discretion of the court to evaluate a reduction in punishment if the person responsible for the crime has compensated the damage.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

There are several rules and regulations that deal with cybersecurity and compliance.
1. First of all, since 25 May 2018, EU Regulation 2016/679, known as the General Data Protection Regulation (GDPR) – on the protection of individuals with regard to the processing and free movement of personal data – has become fully applicable in all Member States.
2. On 19 September 2018, Legislative Decree no. 101 of 10 August 2018 came into force, which introduced provisions for the adaptation of Italian national legislation (Legislative Decree no. 196/2003) to the provisions of the GDPR. In addition to transposing the provisions of the GDPR, Legislative Decree no. 101/2018 regulated certain aspects that have been left to the national legislative authority, including the provision of certain types of criminal offences, in addition to the financial penalties already provided for by the GDPR.
3. Then we have the EU Network and Information Systems Security Directive (NIS Directive 2016/1148), which aims to achieve a common high level of network and information system security throughout the EU.
   Italy also did so with Legislative Decree no. 65 of 18 May 2018.
4. Similar to the GDPR is Directive 680 of 2016.
5. With regard to the Copyright Law, Law 22/04/1941 no. 633, G.U. 16/07/1941.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes, there are for Essential Service Operators (ESOs) and Digital Service Providers (FSDs) according to the NIS Directive.

ESOs are public or private entities that provide "essential services to maintaining social activities and/or economic fundamentals, the supply of which depends on the network and the information systems and on which an incident would have negative effects significant".

The Directive considers the following sectors to be essential:
- Energy (electricity, oil, gas).
- Transport (air, rail, seafarers/fluvial, road).
- Banking (credit institutions).
- Market infrastructure financial (trading venues and central counterparties).
- Healthcare (healthcare providers).
- Water (suppliers and distributors of drinking water).
- Digital infrastructure (operators' Internet exchange points (IXP), service providers (DNS), top-level domain name registers (TLD)).

- FSDs are defined as "any legal entity providing a digital service", which include the following:
  - Search engines.
  - Online markets.
  - Computer services on "clouds".

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Directive requires ESOs and FSDs to adopt "a risk management culture that includes risk assessment and implementation of safety measures".

This should be appropriate to the possible risks, so as not to face "a disproportionate financial and administrative burden".

Article 14 of the Directive states that ESOs must:

- "Take technical measures and organisational and proportional to the management of risks posed to network security and of the information systems they use in their operations". These measures should "ensure a level of network security and information systems appropriate to existing risk."
- "Take appropriate measures to prevent and minimize the impact of safety incidents on network and information systems used for the supply of such essential services, in order to ensure the continuity of such services."
- "Notify without undue delay the competent authority or the CSIRT incidents having an impact relevant to the continuity of services essentials lent."

An ESO must also have "the information necessary to assess the safety of its own networks and information systems, including documented security policies, plus the 'evidence of effective implementation' of such policies, such as the results of the safety checks carried out by the competent authority or an auditor certified".

Article 16 further specifies the provisions for FSDs, which must:

- "Take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the network and information systems they use in the context of the provision of services." These security measures should "ensure a level of network and information system security that exists in the context of the provision of services".
- "Take appropriate measures to prevent and minimize the impact of safety incidents on network and information systems services [offered], with the aim of ensuring continuity."
- "Notify without undue delay the competent authority or the CSIRT of any incident that might have a major impact on provision of a service."

Pursuant to Article 16, information appropriate to the existing risk must take into account:

- the security of systems and installations;
- incidents management;
- business continuity management;
- monitoring, auditing and testing; and
- compliance with international standards.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, they are required under the law.

The GDPR regulates the data breach by expressly providing for an obligation of notification and communication on the part of the owner, in the presence of violations of personal data that may compromise the freedoms and rights of the persons concerned. The Regulation provides for the possibility to make a deferred notification, after the 72 hours provided for by Article 33. This is the case where, for example, a company suffers repeated, close and similar violations of a high number of subjects.

Article 33 provides that the notification must be made to the competent supervisory authority, in accordance with Article 55. In turn, Article 55 provides that each supervisory authority is competent to exercise the tasks and powers assigned to it in the territory of its Member State. Therefore, if the violation occurs in a given Member State, it will be to the Guarantor authority of that State that the appropriate notification must be submitted.

In addition to the obligations to notify the supervisory authority, Article 34 provides for an obligation on the part of the owners to notify the persons concerned so that they can take action to protect their interests.

To prevent, manage and resolve incidents of loss and/or destruction of personal data is necessary:

- adopt a response protocol;
- perform periodic tests to check the validity of the protocol;
- obtain insurance coverage for possible cases of data breach;
- keep a record of data breaches; and
- conduct investigation activities to identify the nature and extent of the breach.

The response protocol

The data controller must adopt a response protocol, i.e. procedures to be followed to manage and resolve any episodes of destruction and/or loss of data. The adoption of the protocol involves numerous corporate departments and public structures such as ministries, asps, etc. This protocol must indicate a consistent, systematic and proactive way to manage these incidents involving personal data. For the solution of these incidents the company/public body may be assisted by third-party service providers such as:

- call centres;
- user support services and public relations;
- monitoring systems; and
- identity theft resolution systems.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, the authorities must be held accountable if the violation has caused obvious damage to the rights and freedoms of citizens.

A data controller (public entity, company, association, party, professional, etc.) must, without undue delay and, where possible, within 72 hours of becoming aware of it, notify the Guarantor for the protection of personal data unless the violation of personal data is unlikely to pose a risk to the rights and freedoms of individuals.

A data controller who becomes aware of a possible violation is required to promptly inform the owner so that they can take action. Additionally, if the violation involves a high risk for the rights of persons, the owner must communicate it to all concerned, using the most appropriate channels, unless he or she has already taken measures to reduce its impact.

The data controller, regardless of the notification to the Guarantor, documents all violations of personal data, for example by preparing a special register. This documentation allows the authority to carry out any checks on compliance with the regulations. The notification must contain the information provided for in Article 33, par. 3 of Regulation (EU) 2016/679 and indicated in the attachment to the Guarantor's Order of 30 July 2019 on the notification of violations of personal data (web doc. no. 9126951).

The communication of the data breach to the persons concerned, due to the need to mitigate the risk of damage and in order to help the persons concerned to take the appropriate measures to avoid such risk, must be timely and, in any case, as soon as reasonably possible.

The scheme of communication of a personal data violation to the interested party must contain all the elements provided for by Article 34 of the GDPR:

- Describe, with a simple and clear message, the nature of the violation.
- Measures taken by the owner.
- Initiatives that should be taken by the person concerned.
- Contact details of the Data Protection Officer (DPO) or other point where information can be obtained.
- Always provide a reference to which the person concerned can turn for clarifications and suggestions regarding the initiatives to be taken.

With regard to ESOs and FSDs, the notification of incidents with significant impact on the services provided will be made to the Computer Security Incident Response Team (CSIRT) and to the competent NIS Authorities, i.e. the various Ministries. The latter are assigned the task of supervising the application of the Directive at the national level, and imposing administrative sanctions in case of failure to comply with the obligations.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The main regulatory authority of points referred to at questions 2.1 and 2.6 is the Guarantor for the protection of personal data, or the Privacy Guarantor, an independent administrative authority established by Law 675/1996 with the aim of protecting the rights, fundamental freedoms and proper processing of personal data in respect of the dignity of the person.

The new Italian Computer Security Incident Response Team (CSIRT) aims to optimise the effectiveness of the prevention and response of the country to cyber-attacks against public and private entities, monitoring and analysing incidents, disseminating information and intervening in case of emergency, the institution, created within the Department of Security Information (DIS), is part of the European framework of the NIS Directive issued by the European Parliament, which provides for the creation of national CSIRTs in all Member States.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

The GDPR, which provisions have been supplemented by Legislative Decree no. 101/2018, provides for effective, proportionate and dissuasive administrative sanctions in case of non-compliance. These sanctions can be up to €20 million or 4% of the "total worldwide turnover in the previous fiscal year", (whichever is greater) of the non-compliant organisation.

Article 21 of the NIS Directive provides that Member States shall lay down the rules on penalties applicable to infringements of the provisions of the Directive and shall take measures to ensure that they are implemented. These penalties must be "effective, proportionate and dissuasive".

It is to be expected that the penalties for breaching the NIS Directive will be similarly severe. For example, in Italy the government has decided that the competent authorities may apply administrative sanctions of up to €150,000.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The rules on privacy sanctions are governed by Articles 83 and 84 of the GPDR. Fines are applied according to the EU Regulation but the amount is determined according to the type of violation.

The consequences for companies and professionals who commit violations are different:

- criminal sanctions;
- administrative sanctions;
- compensation for damages in favour of the person concerned; and
- prohibition of the processing of personal data until the non-compliance situation is remedied.

Criminal sanctions for the protection of privacy are regulated on the basis of the rules established by each State. In the case of Italy, reference continues to be made to the 2003 Privacy Code that provides for imprisonment of up to six years and identifies five types of violations:

- unlawful processing of data;
- unlawful communication and dissemination of personal data subject to processing on a large scale;
- fraudulent acquisition of personal data subject to processing on a large scale;
- false statements to the Guarantor and interruption of the performance of the duties or exercise of the powers of the Guarantor; and
- non-compliance with the provisions of the Guarantor.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Yes, they are.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Yes, they are.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Yes, they are.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes, they are, under the Jobs Act.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

No, it does not.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Not at all, but the NIS Directive identifies critical infrastructures, such as ESOs and FSDs, which must take "adequate and proportionate" safety measures and inform the relevant national authorities in case of serious incidents. On the regulatory level, there are no differences.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes, more specifically recalling the answer given above at question 2.2.

The NIS Directive (EU Directive 2016/1148) aims to achieve a high common level of network and information systems security within the European Union for:

1. Operators of essential services.
2. Digital service providers.

It is up to them to adopt appropriate technical and organisational measures for risk management and prevention of cyber incidents.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

The defaulting conduct of the directors, whether active or omissive, which may result in their liability to the company for consequential damages, may consist of:

- the violation of the general duty of professional diligence, suitable to include all the measures necessary to perform the management role in the specific case;
- the non-fulfilment (i.e. the failure to perform or an execution that does not comply with the fee of diligence, as identified above) of obligations with specific intent, determined by law or the articles of association; and
- failure to prevent and mitigate incidents, constituting a breach of directors' duties, especially if directors fail to prove that they have implemented appropriate measures to prevent incidents.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Considering that the duties of the DPO, set forth in Articles 38 and 39 of the GDPR, refer, among other things, to information and assistance activities of the data controller or data processor, to supervisory tasks and dialogue between them and the Privacy Authority, there are cases in which the figure of the DPO is mandatory and others in which it is not necessary.

The cases of obligation are:

- data processing carried out by public administrations (e.g. municipalities, hospitals, schools, etc.);
- subjects whose core business (main activity) is the regular and systematic monitoring of people on a large scale;
- subjects whose core business (main activity) is the large-scale processing of particular data (e.g. state of health, union data, biometric data, etc.) or judicial data; and
- the Italian Guarantor in the published guidelines also suggests the appointment of public service concessionaires (i.e. of water, gas and energy management companies).

With regard to cybersecurity obligations, the NIS Directive requires ESOs and FSDs to adopt "a risk management culture that includes risk assessment and implementation of security measures appropriate to the possible risks 'so as not to face' a disproportionate financial and administrative burden".

An explanation of what this entails can be found in Recital 46: "Risk management measures include measures to identify possible incident risks, to prevent, detect and address incidents and to mitigate their impact. Network and information systems security includes the security of data stored, transmitted and processed."

However, cybersecurity compliance measures are covered by both the NIS Directive and the GDPR pursuant to Articles 32 and 33, where data controllers are required to implement all measures to adapt to the risk of violations.

In addition, companies must have a policy of response to incidents, regardless of the GDPR requirements, identifying vulnerabilities and critical points in the first step, in order to mitigate incidents.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

The explicit information obligations concern for the time being data breaches and incidents. However, companies must constantly monitor information infrastructure, especially critical infrastructure. The Implementation Regulation also outlines the parameters to be taken into account to define a "significant impact" according to which critical companies must notify the incident to the competent authority. The parameters are:

- Unavailability of the service for more than five million users/hour in the Union.
- Loss of confidentiality, integrity, availability or authenticity of accessible data on networks or information systems involving more than 100,000 users in the Union.
- The fact that the incident creates a risk to public security, public safety or human lives.
- The possibility that the material damage of at least one user in the Union exceeds €1 million.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The civil liability of organisations depends on the extent of the damage caused as a result of a non-compliance infrastructure, and the damage resulting from the violation of citizens' rights and freedoms. As regards civil law aspects, and, in particular, compensation for damages, it is the same Article 82(6) of the GDPR that provides that the only remedy available is recourse to the courts of the Member States.

Article 140-*bis* of the Data Protection Code (Privacy Code, Legislative Decree no. 196/2003) states that the person concerned, if he or she believes that his or her rights under data protection legislation have been violated, may alternatively choose to lodge a complaint with the Guarantor or to proceed through the classic judicial remedy.

In Italy, the lodging of the complaint excludes the possibility of appeal, and the *vice versa*.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In the 2019 annual report published on June 23, 2020, the Privacy Guarantor dedicates ample space to the issue of sanctions.

It is in fact to highlight the first period of application of the sanctions regime provided by EU Regulation 2016/679 (GDPR).

Among the highest penalties are the €8.5 million imposed on a company in the energy sector for unlawful treatment in telemarketing and teleselling activities and the €28 million imposed on a well-known telephone company. The latter, to date, is the highest sanction in the history of the Guarantor, even considering the period of first application of the sanctions provided by the GDPR.

There are also references to sanctions imposed on private companies in the healthcare sector, such as the sanction of €8,000 imposed on a healthcare company that had illegally communicated to a provider the personal and health data of its patients.

A fine of €16,000 was imposed on a doctor who had used the addresses of about 3,500 former patients to send letters in support of a candidate in the regional political elections, without the consent of those concerned.

Activities of public bodies can also the subject of a sanction, with a fine of €10,000 for the unlawful processing of judicial data.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes. Tort liability depends on the damage that occurred due to the organisation's failure to take security measures, specifically in the field of civil liability. Article 2050 lacks provisions in this respect and nothing is provided for by Legislative Decree no. 101/2018. The logical consequence is that, as far as this area is concerned, reference must necessarily be made to Article 82 of EU Regulation 679/2016.

This chapter establishes the right of anyone to obtain compensation for the damage suffered, whenever there has been a violation of the provisions of the GDPR by the owner or the data controller.

Under the GDPR, compensation may be claimed for both pecuniary and non-pecuniary damages and the action will be brought before the competent court; in this jurisdiction, before the civil courts.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, they are permitted. We are in the era of cyber 2.0 policies, especially for the world of SMEs, which are the richest and most dynamic fabric of our industrial economic reality but also the least prepared and most vulnerable to cyber-attacks.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations to insurance coverage against specific types of loss, but it is important to remember that new generation of cyber policies that are "GDPR-aware" can never cover any sanctions that may be imposed on the offender.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Depending on the type of investigation to be addressed, there are several authorities that can take part in forensic investigations,

such as the Ministry of Justice, the Ministry of Defence, the CSIRT Computer Security Incident Response Team, the judicial authority or the Privacy Guarantor.

The supervisory authority, the Privacy Guarantor, has powers of investigation, correction, authorisation and consultation, as well as the power to impose administrative fines.

These powers are dealt with in Article 58 of the Regulation by listing and dividing them into:

- Powers of investigation (Article 58, paragraph 1).
- Corrective powers (Article 58, paragraph 2).
- Authorisation and advisory powers (Article 58, paragraph 3). The power to impose administrative sanctions through the GDPR is instead provided by Article 83.

The following ministries are defined as NIS competent authorities: Economic Development, for the energy, digital infrastructure and FSD sectors; Infrastructure and Transport, for the transport sector; Economy and Finance, for the banking and financial market infrastructure sectors, in collaboration with the Bank of Italy and Consob; Health; and, Environment. For some areas – such as health and the supply and distribution of drinking water – the competent authorities are the Regions and Autonomous Provinces of Trento and Bolzano. They are assigned the tasks of supervising the application of the Directive at national levels and imposing administrative sanctions in the event of failure to comply with their obligations.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Nowadays, there is no such obligation. However, the NIS Directive invites organisations to adopt security policies, especially those related to the web.

Alessandro Rubino graduated in 2013 in Law from the University Carlo Cattaneo – LIUC, with a specialisation in "E-justice" (electronic justice). He obtained a Master's in Tech Law and Digital Transformation, AI and Blockchain, a Master's in Cybersecurity Specialism and a Master's in Cybersecurity Management, becoming an IT security specialist.
He mainly deals with Privacy, Data Protection and Cybersecurity.
Thanks to his contact with different business realities, after university he developed skills in the field of Privacy, Data Protection and Cybersecurity with particular focus on the drafting of privacy and GDPR compliance policies, connecting them to the cyber reality, implementation of incident response and business continuity procedures, and risk assessment in order to make organisations resilient to external vulnerabilities.
The vision of a market in continuous revolution denotes how the traditional methods integrated in the current market are cumbersome and no longer easy in respect of digital transformation. The figure of the lawyer must be renewed and integrated in new financial, tech, design and security scenarios.

Rubino Avvocati
Piazza dei Martiri, Palazzo Calabritto
Naples
Italy

Tel: +39 081 1844 0103
Email: a.rubino@rubinoavvocati.it
URL: www.rubinoavvocati.it

Gaetano Citro graduated with honours in Law from the University Carlo Cattaneo – LIUC. He is a Barrister at Law and a member of the Bar Association of Salerno.
At the same university, he carried out wide-ranging research and coordination activities on Civil Economy and Corporate Social Responsibility (CSR) with specific studies on Corporate Compliance. Important parts of his research have been considered and applied by the Faculty of Law at the Universities of Boston and Harvard and the Anti-Fraud Office (OLAF) at the European Commission in Brussels.
He currently collaborates with the Sant'Anna School of Advanced Studies University of Pisa for research projects in anti-corruption and legal and digital compliance. He collaborates with Transparency International for anti-corruption, anti-money laundering and whistleblowing projects.
He provides integrated consulting to companies on issues relating to corporate responsibility and privacy protection in relation to technological progress. He provides legal, judicial and extra-judicial assistance in matters of criminal law and white-collar crimes.

Rubino Avvocati
Piazza dei Martiri, Palazzo Calabritto
Naples
Italy

Tel: +39 081 1844 0103
Email: g.citro@rubinoavvocati.it
URL: www.rubinoavvocati.it

Rubino Avvocati is an independent legal boutique led by the lawyer Raffaele Rubino, founder of the Firm, which counts on a team of seven professionals joined by a network of experts and technicians, also in complementary areas, including accountants and notaries.
Raffaele Rubino directs the team, always involved in all matters, with an analytical and multidisciplinary approach.
For each individual client, with whom he establishes a relationship of trust, the Firm is committed to being a strategic partner able to intercept their real needs, finding tailor-made solutions.
Each member of the team provides his or her own specific expertise and subject matter, guaranteeing the best solution for the client with respect to his or her unique and unique needs.
Rubino Avvocati provides specialised assistance to companies and individuals located throughout Italy.

www.rubinoavvocati.it

RUBINO AVVOCATI

Japan


Hiromi Hayashi


Masaki Yukawa


Daisuke Tsuta

Mori Hamada & Matsumoto

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

As background, there are two main laws criminalising cyber-attacks, namely (A) the Act on the Prohibition of Unauthorised Computer Access (the "**UCAL**"), and (B) the Penal Code.

(A) The UCAL imposes criminal sanctions on any person who makes "**Unauthorised Access**" to a computer (an "**Access Controlled Computer**"), the access to and operation of which are under the control of an administrator (the "**Access Administrator**").

Unauthorised Access means any action which operates an Access Controlled Computer by either (i) inputting an identification code (*shikibetsu-fugou*) (e.g., password and ID) allocated to a user who is authorised to access the Access Controlled Computer (an "**Authorised User**"), without the permission of the Access Administrator or the Authorised User, or (ii) inputting any information (other than an identification code) or command which enables that person to evade control (e.g., cyber-attack of a security flaw), without the permission of the Access Administrator (UCAL, Article 2, Paragraph 4).

The UCAL prohibits the following actions:

(a) Unauthorised Access (Article 3);

(b) obtaining the identification code of an Authorised User to make an Unauthorised Access (Article 4);

(c) providing the identification code of an Authorised User to a third party other than the Access Administrator or the Authorised User (Article 5);

(d) keeping the identification code of an Authorised User which was obtained illegally to make Unauthorised Access (Article 6); and

(e) committing the following acts by impersonating the Access Administrator or causing a false impression of being the Access Administrator by: (a) setting up a website where the fake Access Administrator requests an Authorised User to input his/her identification code; or (b) sending an email where the fake Access Administrator requests an Authorised User to input his/her identification code (Article 7).

Any person who commits (a) above (Article 3) is subject to imprisonment of up to three years or a fine of up to JPY 1,000,000 (Article 11). Any person who commits (b) to (e) above (Articles 4 to 7) is subject to imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12). However, if the person committing (c) (Article 5) does not know that the recipient intends to use the identification code for Unauthorised Access, that person is subject to a fine of up to JPY 300,000 (Article 13).

(B) The Penal Code provides for criminal sanctions on the creation and provision of "**Improper Command Records**" which give improper commands, such as a computer virus, to a computer (*fusei shirei denji-teki kiroku*). Improper Command Records mean (i) electromagnetic records that give a computer an improper command which causes the computer to be operated against the operator's intention or fail to be operated in accordance with the operator's intention, and (ii) electromagnetic or other records which describe such improper commands.

Under the Penal Code, any person who creates or provides, without any justifiable reason, Improper Command Records, or who knowingly infects or attempts to infect a computer with Improper Command Records, is subject to imprisonment of up to three years or a fine of up to JPY 500,000 (Article 168-2). Any person who obtains or keeps Improper Command Records for the purpose of implementing such records is subject to imprisonment of up to two years or a fine of up to JPY 300,000 (Article 168-3).

In addition, the Penal Code provides for the following additional penalties:

(i) any person who obstructs the business of another by causing a computer used in the business to be operated against the operator's intention, or fail to be operated in accordance with the operator's intention, by (a) damaging that computer or any electromagnetic record used by that computer, or (b) giving false information or an improper command to the computer, is subject to imprisonment of up to five years or a fine of up to JPY 1,000,000 (Article 234-2);

(ii) any person who gains or attempts to gain, or causes or attempts to cause a third party to gain, illegal financial benefits by (a) creating false electromagnetic records by giving false information or an improper command to a computer, or (b) providing false electromagnetic records for processing by a third party, in either case, in connection with a gain, a loss or a change regarding financial benefits is subject to imprisonment of up to 10 years (Article 246-2); and

(iii) any person who creates, provides or attempts to provide electromagnetic records for the purpose of causing a third party to mistakenly administer matters which relate to rights, obligations or proofs of facts is subject to imprisonment of up to five years or a fine of up to JPY 500,000. However, if the act relates to records to be made by public authorities or public servants, the penalty is imprisonment of up to 10 years or a fine of up to JPY 1,000,000 (Article 161-2).

Hacking is Unauthorised Access under the UCAL, punishable by imprisonment of up to three years or a fine of up to JPY 1,000,000.

If the hacking is made through Improper Command Records, it is also punishable under the Penal Code (please see question 1.1(B) above). In addition, if a business is obstructed by such hacking, the crime is punishable by imprisonment of up to five years or a fine of up to JPY 1,000,000 (Penal Code, Article 234-2).

Denial-of-service attacks
This carries the same penalties as hacking.

Phishing
Article 7 of the UCAL prohibits phishing, while Article 4 of the UCAL prohibits obtaining any identification code through phishing. These actions are punishable by imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12).

In addition, any person who gains illegal benefits by using identification codes obtained by phishing is subject to imprisonment of up to 10 years under Article 246-2 of the Penal Code.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
This carries the same penalties as hacking.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Other than the crime of providing Improper Command Records (see above) without any justifiable reason to any third party, which is subject to imprisonment of up to three years or a fine of up to JPY 500,000 (Penal Code, Article 168-2), there is no general prohibition against the distribution, sale or offering of hardware, software or other tools which may be used to commit a cybercrime.

Generally, if a person provides hardware, software or other tools knowing that those tools will be used for Unauthorised Access (see above) or to infect a computer with Improper Command Records, that person will be an accessory to these crimes. However, the Supreme Court has taken a relatively modest approach in punishing providers of software which can be used either for legitimate or illegal purposes. The Supreme Court on 19 December 2011 acquitted a developer of a P2P software that could be and actually was used for copyright violation, saying that a software provider may be punished as an accessory only if he knew that the software will be used for a specific criminal act or mostly for criminal acts. In this case, the court found that since the developer constantly warned users not to use the software in violation of any copyright, it was difficult to attribute knowledge to the developer.

Possession or use of hardware, software or other tools used to commit cybercrime
Any person who obtains or keeps Improper Command Records for the purpose of using such records is subject to imprisonment of up to two years or a fine of up to JPY 300,000 (Penal Code, Article 168-3).

As an example, nine persons were prosecuted for uploading software which contained a computer virus to an online storage system, and which infected the computers of people who accessed the storage and downloaded the software from September to December 2016.

Identity theft or identity fraud (e.g. in connection with access devices)
This carries the same penalties as phishing.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
In addition to the criminal penalties applicable to phishing, electronic theft is penalised under the Unfair Competition Prevention Act. If a current or former employee (a) acquires a trade secret of the employer through theft, fraud, threat or other illegal actions (the "**Illegal Actions**"), including Unauthorised Access, or (b) uses or discloses a trade secret of the employer acquired through Illegal Actions, for the purpose of obtaining wrongful benefits or damaging the owner of the trade secret, that employee is subject to imprisonment of up to 10 years or a fine of up to JPY 20,000,000, or both (Article 21, Paragraph 1). In addition, if that employee commits any of the foregoing acts outside Japan, the fine is increased up to JPY 30,000,000 (Article 21, Paragraph 3).

Under the Copyright Act, any person who uploads electronic data of movies or music, without the permission of the copyright owner, to enable another person to download them is subject to imprisonment of up to 10 years or a fine of up to JPY 10,000,000, or both (Article 119, Paragraph 1). Furthermore, any person who downloads electronic data which is protected by another person's copyright, and who knows of such protection, is subject to imprisonment of up to two years or a fine of up to JPY 2,000,000, or both (Article 119, Paragraph 3). In addition, any person who sells, lends, manufactures, imports, holds or uploads any device or program which may remove, disable or change technology intended to protect copyright (e.g., copy protection code) is subject to imprisonment of up to three years or a fine of up to JPY 3,000,000, or both (Article 120-2).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Since there is no exemption for this type of testing, unsolicited penetration testing is punishable as Unauthorised Access.

Vulnerability testing without permission is generally not allowed. However, the National Institute of Information and Communications Technology (the "**NICT**") (and only the NICT) is allowed to conduct vulnerability testing without permission under the Law on the National Institute of Information and Communication Technology, which exempts the NICT from the prohibition against Unauthorised Access.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
This carries the same penalties as electronic theft.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The UCAL provides for the extraterritorial application of Articles 3, 4, 5 (except where the offender did not know the recipient's purpose) and 6 of the UCAL (Article 14).

The Penal Code also has extraterritorial application (Article 4-2).

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The above-mentioned offences are not subject to exceptions such as "ethical hacking" or lack of intention to cause damage or make financial gains.

As discussed above (please see question 1.1), vulnerability testing without permission may be conducted only by the NICT based on a special law, and there are no general exceptions to similar activities for other persons.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

In addition to the UCAL, the Penal Code and the Unfair Competition Prevention Act described above, the following laws are also applicable to cybersecurity.

(A) Basic Act on Cybersecurity (the "BAC")

This provides the basic framework for the responsibilities and policies of the national and local governments to enhance cybersecurity. In July 2018, pursuant to the BAC, the Japanese government issued the Cybersecurity Strategy (which was drafted by the Cybersecurity Strategy Headquarters (the "**CSHQ**")), established under Article 25 of the BAC to promote Japan's cybersecurity measures, and its secretariat, the National Center of Incident Readiness and Strategy for Cybersecurity (the "**NISC**").

Furthermore, the BAC obligates operators of critical infrastructure to make efforts to voluntarily and proactively enhance cybersecurity, and to cooperate with the national and local governments to promote measures to enhance cybersecurity. In December 2018, the BAC was amended to establish the cybersecurity council (the "**Cybersecurity Council**"). The Cybersecurity Council is intended to be the avenue to allow national and local governmental authorities and business operators to share information which may facilitate the proposal and implementation of cybersecurity measures. The Cybersecurity Council was established in April 2019 and 225 entities participate in the council as of July 2020.

(B) Telecommunication Business Act (the "TBA")

Article 4 of the TBA provides that (1) the secrecy of communications being handled by a telecommunications carrier shall not be violated, and (2) any person who is engaged in a telecommunications business shall not disclose secrets obtained while in office, with respect to communications being handled by the telecommunications carrier, even after he/she has left office.

The secrecy of communications protects not only the contents of communications but also any information that would enable someone to infer the meaning or the contents of communications. In this regard, data on access logs and IP addresses are protected under the secrecy of communications. If a telecommunications carrier intentionally obtains any information protected under the secrecy of communications, discloses protected information to third parties and uses protected information without the consent of the parties who communicated with each other, that telecommunications carrier is in breach of Article 4(1).

To prevent cyber-attacks, it would be useful for telecommunications carriers to collect and use information regarding cyber-attacks, e.g., access logs of infected devices, and share this information with other telecommunications carriers or public authorities. However, the TBA does not explicitly provide how a telecoms carrier may deal with cyber-attacks without breaching Article 4(1). The Ministry of Internal Affairs and Communications (the "**MIC**"), the governmental agency primarily responsible for implementing the TBA, issued reports in 2014, 2015 and 2018 which addressed whether a telecoms carrier may deal with cyber-attacks and the issues that may arise in connection with the secrecy of communications. The findings of the three reports are included in the guidelines on cyber-attacks and the secrecy of communications (the "**Guidelines**"), issued by the Council regarding the Stable Use of the Internet. This Council is composed of five associations which are the ICT Information Sharing And Analysis Center Japan (the "**ICT-ISAC Japan**"), the Telecommunications Carriers Association, the Telecom Services Association, the Japan Internet Providers Association and the Japan Cable and Telecommunications Association. The Guidelines include the contents of the MIC's three reports. The Guidelines, however, are not legally binding, although they carry a lot of weight because the MIC confirmed them before the Guidelines were issued.

Furthermore, in 2013, the MIC started a project called ACTIVE (Advanced Cyber Threats response InitiatiVE) that aims to protect internet users from cyber-attacks by collaborating with ISPs and vendors of IT systems. To prevent computer virus infections, warning users or blocking communications in accordance with the Guidelines may be done by ISPs which are members of ACTIVE.

In addition, in May 2018, the TBA was amended to introduce a new mechanism which enables a telecommunications carrier to share with other carriers information on transmission sources of cyber-attacks through an association which the MIC confirms is eligible to assist telecommunications carriers. After the amendments became effective in November 2018, the MIC designated the ICT-ISAC Japan to be that association in January 2019.

(C) Act on the Protection of Personal Information (the "APPI")

The APPI is the principal data protection legislation in Japan. It is the APPI's basic principle that the cautious handling of Personal Information under the principle of respect for individuals will promote the proper handling of "**Personal Information**". Personal Information means information about specific living individuals which can identify them by name, date of birth or other descriptions contained in the information (including information that will allow easy reference to other information, which may enable individual identification) (Article 2, Paragraph 1). A business operator handling Personal Information may not disclose or provide Personal Information without obtaining the subject's consent, unless certain conditions are met.

To prevent cyber-attacks, it would be useful for business operators to collect and use information regarding the cyber-attacks, e.g., access logs of infected devices, and share this information with other business operators or public authorities. However, if the information includes Personal Information, it would be subject to the restrictions on the use and disclosure of Personal Information under the APPI.

(D) the Japanese Foreign Exchange and Foreign Trade Act (the "FEFTA")

The FEFTA regulates the export of sensitive goods and technologies including encryption software and hardware (please see question 3.3) as well as inward direct investments such as acquisition of shares in Japanese companies by non-Japanese investors. From the viewpoint of national security, prior notification to the Ministry of Finance and other competent authorities will be required for an acquisition of 1% or more of shares in a Japanese company which engages in information technologies, software, and telecommunications businesses, unless an exemption is applicable, and the Ministry of Finance and other competent authorities may order the cessation of the acquisition.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The UCAL requires Access Administrators to make efforts to manage the identification codes of Authorised Users, examine the validity of functions to control access to the Access Controlled Computer and implement necessary measures, including enhancing functions (e.g., encryption of codes, definite deletion of codes which have not been used for a long time, implementing a batch program to address a security flaw, program updates and appointing an officer for network security) (Article 8).

The so-called "**Critical Information Infrastructure Operators**" are required to make an effort to deepen their interest and understanding of the importance of cybersecurity, and to voluntarily and proactively ensure cybersecurity for the purpose of providing services in a stable and appropriate manner (BAC, Article 6). Article 3(1) of the BAC defines "**Critical Information Infrastructure Operators**" as operators of businesses that provide an infrastructure which is a foundation of people's lives and economic activities which could be enormously impacted by the functional failure or deterioration of that infrastructure.

The CSHQ formulated the Cybersecurity Policy for Critical Infrastructure Protection as a non-mandatory guideline which designated 14 critical infrastructure areas under its coverage. These 14 areas are information and communication, financial services, aviation, airport, railway, electric power, gas supply, government and administrative supply, medical, water, logistics, chemical, credit card, and petroleum.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

(A) Cybersecurity Management Guidelines

The Ministry of Economy, Trade and Industry (the "**METI**") and the Independent Administrative Agency Information-technology Promotion Agency (the "**IPA**") jointly issued the Cybersecurity Management Guidelines (the latest version of which is as of November 2017). The guidelines describe three principles that the management of companies that have a dedicated division for information systems and that are utilising IT, should recognise to protect their company from cyber-attacks, and 10 material items on which management should give instructions to executives or directors in charge of IT security, including the chief information security officer (the "**CISO**").

The 10 material items and some examples of recommended actions for each item described in the guidelines are as follows:

(i) Recognise cybersecurity risks and develop company-wide measures.
Example: Develop a security policy which incorporates cybersecurity risk management while aligning it with the company's management policy, so that management can publish company-wide measures.

(ii) Build a structure or process for cybersecurity risk management.
Example: CISO to establish a system to manage cybersecurity risks and set forth the responsibilities clearly.
Example: Directors to examine whether a system which will manage cybersecurity risks has been established and is being operated properly.

(iii) Secure resources (e.g., budget and manpower) to execute cybersecurity measures.
Example: Allocating resources to implement specific cybersecurity measures.

(iv) Understand possible cybersecurity risks and develop plans to deal with such risks.
Example: During a business strategy exercise, identify information which needs protection and cybersecurity risks against that information (e.g., damage from leakage of trade secrets on a strategic basis).

(v) Build a structure to deal with cybersecurity risks (i.e., structure to detect, analyse and defend against cybersecurity risks).
Example: Secure the computing environment and network structure used for important operations by defending them through multiple layers.

(vi) Publish a cybersecurity measures framework (the "**PDCA**") and its action plan.
Example: Develop a structure or process where one can constantly respond to cybersecurity risks (assurance of implementation of a PDCA).

(vii) Develop an emergency response system (emergency contacts, initial action manual and Computer Security Incident Response Team (the "**CSIRT**")) and execute regular hands-on drills.
Example: Issue instructions to promptly cooperate with relevant organisations and to investigate relevant logs to ensure that efficient actions or investigations can be taken to identify the cause and damage of a cyber-attack.
Example: Execute drills, including planning activities, to prevent recurrence after Incidents and reporting Incidents to relevant authorities.

(viii) Develop a system to recover from the damages caused by an Incident.
Example: Establish protocols for recovery from business suspension, or other damages caused by an Incident, and execute drills in accordance with these protocols.

(ix) Ensure that entities in the company's entire supply chain, including business partners and outsourcing companies for system operations, take security measures.
Example: Conclude agreements or other documents to provide clearly how group companies, business partners and outsourcing companies for system operations in the company's supply chain will take security measures.

Example: Have access to and understand reports on how group companies, business partners and outsourcing companies for system operations in the company's supply chain take security measures.

(x) Collect information on cyber-attacks through participation in information-sharing activities and develop an environment to utilise such information.
Example: Help society guard against cyber-attacks by actively giving, sharing and utilising relevant information.
Example: Report information on malware and illegal access to the IPA in accordance with public notification procedures (standards for countermeasures for computer viruses and for illegal access to a computer).

(B) Common Standards on Information Security Measures of Governmental Entities

The CSHQ and the NISC jointly issued the Common Standards on Information Security Measures of Governmental Entities under Article 26(1) of the BAC. The standards are a unified framework for improving the level of information security of governmental entities and define the baseline for information security measures to ensure a higher level of information security. Although these standards do not apply to private companies, some entities refer to these standards for their information security measures.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There is no mandatory requirement to report Incidents.

However, under the guidelines for banks issued by the Financial Services Agency (the "**FSA**"), banks are required to report an Incident immediately after becoming aware of it. The guidelines are not legally binding; however, because the FSA is a powerful regulator of the financial sector, banks would typically comply with the FSA's guidelines (please see question 4.1). The report must include:

(i) the date and time when the Incident occurred and the location where the Incident occurred;
(ii) a summary of the Incident and which services were affected by the Incident;
(iii) causes of the Incident;
(iv) a summary of the facilities affected by the Incident;
(v) a summary of damages caused by the Incident, and how and when the situation was remedied or will be remedied;
(vi) any effect to other business providers;
(vii) how the banks responded to enquiries from users and how they notified users, public authorities and the public; and
(viii) possible measures to prevent similar Incidents from happening.

In addition, if a cyber-attack causes a serious Incident specified in the TBA and the enforcement rules of the TBA, such as a temporary suspension of telecommunications services or a violation of the secrecy of communications, the telecommunications carrier is required to report the Incident to the MIC promptly after its occurrence. In addition, the carrier is required to report the details of the said Incident to the MIC within 30 days from its occurrence. The detailed report must include:

(i) the date and time when the Incident occurred;
(ii) the date and time when the situation was remedied;
(iii) the location where the Incident occurred (the location of the facilities);
(iv) a summary of the Incident and which services were affected by the Incident;
(v) a summary of the facilities affected by the Incident;
(vi) details of the events or indications of the Incident, the number of users affected and the affected service area;
(vii) measures taken to deal with the Incident, including the persons who dealt with it, in chronological order;
(viii) causes which made the Incident serious, including how the facilities have been managed and maintained;
(ix) possible measures to prevent similar Incidents from happening;
(x) how the telecoms carrier responded to inquiries from users and how it notified users of the Incident;
(xi) internal rules in connection with the Incident;
(xii) if the telecoms carrier experienced similar Incidents in the past, a summary of the past Incidents;
(xiii) the name of the manager of the telecoms facilities; and
(xiv) the name and qualifications of the chief engineer of the telecoms facilities.

Furthermore, it is recommended that companies report the Incident to the IPA (please see question 2.3 above). The report must include:

(i) the location of where the infection was found;
(ii) the name of the computer virus. If the name is unknown, features of the virus found in the IT system;
(iii) the date when the infection was found;
(iv) the types of OS used and how the IT system is connected (e.g., LAN);
(v) how the infection was found;
(vi) possible cause of the infection (e.g., email or downloading files);
(vii) extent of the damage (e.g., the number of infected PCs); and
(viii) whether the infection has been completely removed.

The IPA also has a contact person whom the companies may consult, whether or not they file a report with the IPA, as to how they can deal with cyber-attacks or any Unauthorised Access. According to the IPA's website, it had 8,000 consultations in 2018.

If the Incidents involve any disclosure, loss or damage of Personal Information handled by a business operator, then, according to the guidelines issued by the Personal Information Protection Committee (the "**PPC**") regarding the APPI, the operator is expected to promptly submit to the PPC a summary of such disclosure, loss or damage and planned measures to prevent future occurrences.

However, under the newest amendments to the APPI, which were promulgated on 12 June 2020 and will come into force no later than 12 June 2022 (the "**Amended APPI**"), the business operator must report any Incident to the PPC.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The Cybersecurity Management Guidelines recommend knowing who should be notified if a cyber-attack has caused any damage, gathering information to be disclosed and promptly publishing the Incident, taking into account its impact on stakeholders (please see question 2.3).

Furthermore, if the Incidents involve any disclosure, loss or damage of Personal Information handled by a business operator, then, according to the guidelines issued by the PPC regarding the APPI, the operator is expected, depending on the contents or extent of the disclosure, loss or damage, to notify the affected individuals of the facts relevant to the disclosure, loss or damage, or to make the notification readily accessible to the affected individuals (e.g., posting the notification on the operator's website) in order to prevent secondary damages or similar Incidents.

However, under the Amended APPI, the business operator must notify the affected individuals of any Incident.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The MIC is the governmental agency primarily responsible for implementing the TBA.

The METI is not a regulator that has a specific mandated regulatory authority under specific laws. Rather, it promulgates desirable policies for each industry.

The PPC is an independent organ which supervises the enforcement and application of the APPI.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Other than the report of a serious Incident under the TBA (please see question 2.4) and under the Amended APPI (please see questions 2.4 and 2.5), reporting is not mandatory. If a telecommunications carrier does not report a serious Incident, it is subject to a fine of up to JPY 300,000. If a business operator does not report a serious Incident under the Amended APPI, the PPC may make recommendations or issue orders, and if the operator does not comply with a PPC order, it is subject to imprisonment of up to one year or a fine of up to JPY 1,000,000.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

No examples can be found based on publicly available information.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of beacons is permissible so long as the use complies with the Guidelines and Applicable Laws.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of honeypots is permissible so long as the use complies with the Guidelines and Applicable Laws.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of sinkholes is permissible so long as the use complies with the Guidelines and Applicable Laws.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

As described in question 2.1, to prevent cyber-attacks, the MIC issued reports which addressed whether a telecoms carrier may deal with cyber-attacks and the issues that may arise in connection with the secrecy of communications, and the Council regarding the Stable Use of the Internet issued the Guidelines. These reports and the Guidelines cover policies regarding electronic communications on organisations' networks.

In addition, when a business operator monitors an employee's email or internet usage, monitoring may be considered illegal if the employees' personal information or privacy is not protected. The PPC recommends paying close attention to the following when conducting monitoring as part of employee supervision or personal data security management:

(a) identify the purpose of monitoring, specify the purpose in internal regulations, and inform the employees of the purpose;
(b) assign a person responsible for monitoring and determine the authority of that person;
(c) establish rules regarding the implementation of monitoring and ensure that the organisation complies with them; and
(d) check the adequacy of monitoring operations.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Under the FEFTA, encryption and intrusion program-related software and hardware are subject to export control regulation.

Regarding encryption, a cryptographic algorithm that meets certain requirements and any of the following three conditions is subject to the following regulations: (i) one main function is the security management of an information system; (ii) it constructs, manages or operates a telecommunication line; or (iii) one main function is to record, store, and process information. However, there are many available exceptions. For example, hardware and software that use publicly known encryption technology or that secondarily use cryptographic functions are not subject to regulation.

Regarding intrusion program-related hardware or software (note that the intrusion program itself is not regulated), this cannot be exported if it includes vulnerability information and malware information about the program. However, in order to reduce the impact on cybersecurity practice, exporting such a hardware or software for the purpose of disclosing security vulnerabilities or responding to cyber-attacks is exempt from export control regulation.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

In general, the financial business sector and the telecommunications service sector closely collaborate with relevant authorities on information security.

The FSA issued in 2015, and updated in 2018, a summary of its policies to strengthen cybersecurity in the financial business sector. According to the updated summary, the FSA will continue to: (i) promote continuous dialogue with financial institutions to understand their cybersecurity risks; (ii) improve information-sharing among financial institutions; (iii) implement cybersecurity exercises in which financial institutions, the FSA and other public authorities participate; and (iv) develop cybersecurity human resources; and also respond to new issues such as accelerated digitalisation and international discussions. The FSA's guidelines require banks to, among others, establish an organisation to handle emergencies (e.g., the CSIRT), designate a manager in charge of cybersecurity, prepare multi-layered defences against cyber-attacks, and implement a periodic assessment of cybersecurity. The guidelines are not legally binding; however, because the FSA is a powerful regulator of the financial sector, banks would typically comply with the FSA's guidelines.

As described above, telecommunications carriers are required to report a serious Incident specified in the TBA (please see question 2.5). In addition, if a telecommunications carrier does not take appropriate measures to remedy problems with its services, the MIC may order it to improve its business. Failure to comply with the order is subject to a fine of up to JPY 2,000,000.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Please see question 4.1.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Under the Companies Act, a director has the duty to act with "due care as a prudent manager" in performing his/her functions as director (*zenkan chuui gimu*). The applicable standard of care is that which a person in the same position and situation would reasonably be expected to observe. In general, if a director fails to get relevant information, enquire or consider how to prevent Incidents, to the extent these acts are reasonably expected of him/her based on the facts when he/she made a decision (e.g., decision to purchase the IT system), then he/she would be in breach of this duty.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The Cybersecurity Management Guidelines, jointly issued by the METI and IPA, recommend companies to build a structure or process for cybersecurity risk management and, as an example, to designate a CISO according to the companies' policies, including the security policy (please see question 2.3).

Furthermore, the FSA's guidelines for banks provide the standards regarding cybersecurity management, such as establishing an organisation to handle emergencies (e.g., the CSIRT), designating a manager in charge of cybersecurity and implementing a periodic assessment of cybersecurity (please see question 3.1).

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no disclosure requirements that are specific to cybersecurity risks or Incidents, but the NISC recommends in its "Framework of Cybersecurity in Corporate Management" published on 2 August 2016, that companies should disclose their initiatives and policies for cybersecurity in their information security report, CSR report, sustainability report, annual report, or corporate governance report. The NISC's report "Trends in Private Companies' Disclosure of Cybersecurity Risks" published in March 2015 showed that cybersecurity risk is referred to in annual reports of 60% of the 225 listed companies included in the Nikkei 225, which is an equity index of Japanese blue-chip companies.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Basically, if a person breaches a contract, the other party may bring a civil action based on the breach. The plaintiff has the burden of proving the breach, the damages incurred by it and the causation between the breach and the plaintiff's damages.

In addition, the Civil Act of Japan provides for a claim based on tort. If a person causes damages to another, the injured party may bring a civil action based on tort. The plaintiff has the burden of proving the damages incurred by it, the act attributable to the defendant and the causation between the defendant's act and the plaintiff's damages.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

A vendor of a computer system was sued by a company which used the system provided by the vendor. The case related to cyber-attacks (SQL injections) to the system which resulted in the disclosure of credit card information of the company's clients. The company sought the payment of damages caused by the cyber-attacks in the amount of approximately JPY 100,000,000, based on breach of contract. The Tokyo District Court decided that although the vendor was required to provide programs which are suitable for blocking SQL injections in accordance with existing standards when the computer system was provided, the Incident was also partially attributable to the company because it ignored the vendor's proposal to improve the system. The vendor was ordered to pay only approximately JPY 20,000,000 (Tokyo District Court decision dated January 23, 2014).

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Tort theory is available under the Civil Act of Japan (please see question 6.1).

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. In general, there are two categories of insurance against Incidents, namely (i) insurance to cover the losses incurred by the vendor of an IT system, and (ii) insurance to cover the losses incurred by a business operator using the IT system.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations on insurance coverage under the law. The coverage may differ depending on the insurance products of different insurance companies.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcers have the power to investigate Incidents which are related to crimes under Applicable Laws. In accordance with the "cybercrime project" of the National Police Agency, the police in each prefecture have established a contact point where consultations and information regarding cybercrimes are handled.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there are no such requirements.

Hiromi Hayashi is a partner at Mori Hamada & Matsumoto. Hiromi specialises in communications law and regulation and authored the Japanese section of *The Preston Gates Guide to Telecommunications in Asia* in 2005. Hiromi's other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. Hiromi was admitted to the Bar in Japan in 2001 and in New York in 2007. Hiromi worked at Mizuho Corporate Bank from 1989–1994 and was with Davis Polk & Wardwell in New York from 2006–2007.

Mori Hamada & Matsumoto
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 5220 1811
Fax: +81 3 5220 1711
Email: hiromi.hayashi@mhm-global.com
URL: www.mhmjapan.com

Masaki Yukawa is a counsel at Mori Hamada & Matsumoto. Masaki advises on cybersecurity issues for financial institutions, telecommunications businesses and technology companies. Masaki was admitted to the Bar in Japan in 2009 and in California in 2016. Masaki worked at the Bank of Japan from 2003–2008 and was with the Financial Services Agency from 2014–2015.

Mori Hamada & Matsumoto
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 6266 8764
Fax: +81 3 6266 8664
Email: masaki.yukawa@mhm-global.com
URL: www.mhmjapan.com

Daisuke Tsuta is an associate at Mori Hamada & Matsumoto. Daisuke specialises in cybersecurity and privacy law. Daisuke was admitted to the Bar in Japan in 2010. Daisuke worked at the Kinki Local Finance Bureau of the Ministry of Finance from 2014–2015, at the Ministry of Internal Affairs and Communications from 2015–2017, and at the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) from 2017–2020.

Mori Hamada & Matsumoto
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 6266 8769
Fax: +81 3 6266 8669
Email: daisuke.tsuta@mhm-global.com
URL: www.mhmjapan.com

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo, with offices in Fukuoka, Nagoya, Osaka, Beijing, Shanghai, Singapore, Yangon, Bangkok and Ho Chi Minh, and a Jakarta desk. The firm has over 450 attorneys and a support staff of approximately 500, including legal assistants, translators and secretaries. The firm is one of the largest law firms in Japan and is particularly well-known in the areas of mergers and acquisitions, finance, litigation, insolvency, telecommunications, broadcasting and intellectual property, as well as domestic litigation, bankruptcy, restructuring and multi-jurisdictional litigation and arbitration. The firm regularly advises on some of the largest and most prominent cross-border transactions representing both Japanese and foreign clients. In particular, the firm has extensive practice in, exposure to and expertise on, telecommunications, broadcasting, the Internet, information technology and related areas, and provides legal advice and other legal services regarding the corporate, regulatory, financing and transactional requirements of clients in these areas.

www.mhmjapan.com

MORI HAMADA & MATSUMOTO

Korea


Hwan Kyoung Ko


Kyung Min Son

Lee & Ko

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Under the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. ("Network Act"), any person who infiltrates another's information communication network ("ICN") without authorised access or beyond the scope of authorised access is subject to imprisonment for not more than five years or a penalty of not more than KRW 50 million.

Similarly, under the Electronic Financial Transactions Act ("EFTA"), any person who accesses an electronic financial system without authorisation is subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Denial-of-service attacks
Under the Network Act, any person who causes disruption of an ICN by intentionally disturbing network operations with large volumes of signal/data or superfluous requests is subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.

Also, under the EFTA, any attacks on electronic financial systems using programs such as a computer virus, logic bomb or email bomb with the intention of destroying data on, or disrupting the operation of, electronic financial systems is subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Phishing
Under the Special Act On The Prevention Of Loss Caused By Telecommunications-Based Financial Fraud And Refund For Loss ("Special Act on Financial Fraud"), any person who causes other persons to input data or instructions into computers or other information processing units, or inputs data or instructions into computers or other information processing units by using other persons' data he or she acquires, for the purpose of telecommunications-based financial fraud, is subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Under the Network Act, any person who transmits malware that can damage, destroy, alter, falsify or disrupt the operation of ICN systems, data or programs, without a justifiable cause, is subject to imprisonment for not more than seven years or a penalty of not more than KRW 70 million.

Moreover, under the EFTA, any person who installs programs, such as a computer virus, logic bomb, or email bomb, for the purpose of destroying data of electronic financial infrastructure or obstructing the operation of electronic financial infrastructure, is subject to imprisonment for not more than 10 years or a penalty of not more than KRW 100 million.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Under the Network Act, any person who distributes malware that can damage, destroy, alter, falsify or disrupt the operation of ICN systems, data or programs, without a justifiable cause, is subject to imprisonment for not more than seven years or a penalty of not more than KRW 70 million.

Possession or use of hardware, software or other tools used to commit cybercrime
Under the Network Act, any person who mutilates, destroys, alters, or forges an information and communications system, data, program or similar without justifiable grounds, or conveys or spreads a program that is likely to interrupt the operation of such system, data, program or similar, is subject to imprisonment for not more than seven years or a penalty of not more than KRW 70 million.

Identity theft or identity fraud (e.g. in connection with access devices)
Under the EFTA, a person who forges or alters a means of access (i.e., means or information which is used to issue a transaction request in electronic financial transactions or to secure the authenticity and accuracy of users and the details of such transaction) is subject to imprisonment of not more than seven years or a penalty of not more than KRW 50 million. Moreover, any person who transfers or takes over a means of access, or borrows or lends a means of access in return for receipt, demand or promise of any compensation, is subject to imprisonment of not more than five years or a penalty of not more than KRW 30 million.

Under the Digital Signature Act ("DSA"), any person who steals or discloses another person's digital signature-creating key (i.e., a sequence of bits used to affix a digital signature to an electronic message), or has an authorised certificate issued in the name of another person or supports such issuance, is subject to imprisonment of not more than three years or a penalty of not more than KRW 30 million.

Moreover, under the Network Act and the Personal Information Protection Act ("PIPA"), anyone who collects another person's information or induces the provision of another person's information through the ICN by deceptive means, or acquires personal information or obtains the consent for processing of personal information through an illegitimate means or method, is subject to imprisonment for not more than three years or a penalty of not more than KRW 30 million.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Under the Unfair Competition Prevention and Trade Secret Protection Act, any person who acquires, uses, or leaks to any third party trade secrets for the purpose of making an improper profit or causing damage to a person who possesses trade secrets, is subject to imprisonment for not more than 10 years or a penalty of not more than KRW 500 million. If such act is considered a breach of fiduciary duty under the Criminal Act, the person is subject to imprisonment for not more than 10 years or a penalty of not more than KRW 30 million. Moreover, if an electronic theft implicates any copyright infringement, such act may result in imprisonment for not more than five years or a penalty of not more than KRW 50 million.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Under the Network Act, the unsolicited penetration testing constitutes hacking, which is an act of unauthorised access (or access beyond authorisation) to the ICN. As such, any person who engages in an unsolicited penetration testing will be subject to imprisonment for not more than five years or a penalty of not more than KRW 50 million.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Under the Network act, any person who mutilates another person's information processed, stored or transmitted through an ICN, or infringes, misappropriates or divulges another person's secret, is subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.

1.2 Do any of the above-mentioned offences have extraterritorial application?

There is no specific provision in the Network Act or PIPA that stipulates or implicates extraterritorial application of the above-mentioned offences. However, if the information collected and processed outside Korea is that of Korean users, the Korean regulatory authority may find that the Network Act or the PIPA is applicable to such case and impose necessary administrative fines or sanctions under the Network Act or the PIPA. Moreover, the Korean Criminal Act provides that the Act generally applies to aliens who commit crimes, including those provided by other Acts and subordinate statutes, against the Republic of Korea or its nationals outside the territory of the Republic of Korea. Moreover, the EFTA stipulates that, in principle, the Act applies to foreigners or foreign corporations.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

With respect to criminal prosecution of personal information leakage Incidents, the responsible party may be discharged from liability if the requisite safeguard measures (i.e., technical and managerial measures) under the PIPA have been properly implemented.

Moreover, if the responsible party voluntarily reports such leakage Incident, the Personal Information Protection Committee ("PIPC"), the pertinent regulatory authority in Korea, may take it into account as a mitigating factor and reduce the amount of penalty to be imposed against the responsible party.

On the other hand, "ethical hacking" will not be considered a mitigating factor or an exception under the Network Act because whether a certain unauthorised network intrusion causes damage or generates financial gains is unrelated to the legal elements constituting an act of hacking under the Network Act.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

In Korea, laws applicable to cybersecurity include: the Network Act; Protection of Communication Secret Act ("PCSA"); the Act on the Protection of Information and Communications Infrastructure ("PICIA"); Electronic Government Act ("EGA"); Act on Establishment of Infrastructure for Informatization of National Defence and Management of Informational Resources for National Defence; EFTA; Credit Information Use and Protection Act ("Credit Information Act"); Act on the Protection, Use, etc. of Location Information; Act on Prevention of Divulgence and protection of Industrial Technology; PIPA; Act on Prevention of Divulgence and Protection of Industrial Technology; Telecommunications Business Act; and Special Act on Financial Fraud.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Under the PICIA, the head of the organisation managing the critical ICN infrastructure facilities has an obligation to establish and implement managerial measures, including physical and technical measures (such as prevention, backup, recovery, etc.) to safely protect the facilities and data managed by the organisation.

Under the Network Act, companies that operate clustered information and communications facilities (i.e., business operators who operate and manage clustered information and communications facilities to render information and communications services on behalf of another person (e.g., Internet Data Centre)) are required to take protective measures to stably operate the information and communications facilities.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the "Standards of Technical and Managerial Safeguards for Personal Information" which have been adopted Notice pursuant to the Network Act, information communications service providers ("ICSPs") are required to install and operate systems equipped with the following functions to prevent illegal access and intrusion Incidents via ICNs:

1. functions restricting unauthorised access to the Personal Data Processing System ("PDPS") by limiting access authority by internet protocol ("IP") address etc.; and
2. detects any illegal attempts to acquire personal data by analysing the IP addresses, etc. that accessed the PDPS.

Moreover, under the Network Act, if an intrusion Incident occurs (e.g., intrusion of an ICN or any other related information systems by using the means of hacking, a computer virus, logic bomb, email bomb, denial of service, high-powered electromagnetic wave, etc.), the ICSPs are required to analyse the causes of any intrusion Incidents and keep damage from intrusion at bay.

In relation to this, the Framework Act on National Information also prescribes that the Minister of Science and ICT may establish and publish the standards for the performance and reliability of information protection systems (i.e., the common criteria for information protection systems evaluation), and recommend manufacturers and importers of information protection systems to comply with such standards.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under the Network Act, all ICSPs or Collective ICN Facility Operators must report any "infiltration Incidents" to the Minister of Science and ICT or Korea Internet and Security Agency ("KISA").

In addition, all ICSPs (and providers of similar services) must report any loss, theft, or leakage of personal information, including (i) the items of personal information lost, stolen or leaked, (ii) the time of the occurrence, (iii) actions that can be taken by the data subjects, (iv) protective response measures taken by the personal information service provider, and (v) contact information of the department to which the data subject can make inquiries, to the PIPC or KISA within 24 hours since the provider becomes aware of such Incident. The provider may report the Incident after the 24-hour period, only if the provider has a justifiable cause, in which case the provider must explain such cause to the PIPC.

In addition, the EFTA requires that if an Incident, such as disturbance or paralysis of an electronic financial infrastructure facility, occurs due to an electronic infringement, the relevant financial company and electronic financial business must, without delay, inform the Incident to the Financial Services Commission ("FSC").

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes, under the PIPA, any ICSP who becomes aware of a personal information Incident as described in question 2.5 must notify the data subject of the leaked information, without delay, including the following: (i) items of personal information affected (e.g., leaked); (ii) the timing of the leakage; (iii) the actions that can be taken by the data subject; (iv) the protective response measures taken by the ICSP; and (v) the name and contact information of the department to which the data subject can make inquires or file a report.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The PIPC, Korea Internet and Security Agency, and the Financial Services Commission are responsible for the above-mentioned requirements.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Failure to comply with the above-mentioned requirements may result in a monetary fine imposed by the relevant regulatory authorities.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In addition to a monetary fine, the regulatory authorities may require submission of any related articles and documents or enter the place of business of the person concerned to inspect account books and other documents. The regulatory authorities may also order the ICSP to take corrective measures as may be necessary to halt or correct the violation or announce to the public the fact that the provider has received the order to take such corrective measures.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

In Korea, there is no legislation or regulation prohibiting the use of beacons to detect and deflect Incidents in the organisations' networks.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
In Korea, there is no legislation or regulation prohibiting the use of honeypots to detect and deflect Incidents in the organisations' networks.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
In Korea, there is no legislation or regulation prohibiting the use of sinkholes to detect and deflect Incidents in the organisations' networks.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

No, unless consent has been obtained. Under the PCSA, monitoring or intercepting electronic communications of others is strictly prohibited unless proper consent has been obtained from the parties to the communication or such monitoring or intercepting has been made pursuant to a permission granted by the court. Therefore, organisations seeking to monitor or intercept electronic communications of employees on their networks must obtain consent from such employees (or any other relevant data subjects). Any person who violates this requirement is subject to imprisonment for at least one year but no more than 10 years, and suspension of qualification for no more than five years. For your reference, the Supreme Court of Korea has previously held that because "wiretapping of telecommunications" refers to an acquisition or recording of telecommunications transmitted via an electronic device or the like by a third party who is not a party to such telecommunications without the consent of the sender or recipient of the telecommunications, a company's recording of telecommunications of its employees made in connection with the company's business purposes will not constitute an act of "wiretapping of telecommunications".

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Yes. Under the Foreign Trade Act, the exportation of strategic items such as information security systems, equipment and components thereof, are restricted unless the exporter obtains an export licence from the Ministry of Trade, Industry, and Energy (if the items are exported for personal use, however, such export licence is not required). Any person who exports the strategic items without obtaining the licence is subject to imprisonment for a maximum of seven years or a penalty of up to five times the price of the exported item.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice varies across business sectors because different laws apply depending on the business sector. For example, in the financial sector, the Credit Information Act requires credit information companies to implement certain statutorily prescribed technical, physical, and managerial security measures, including security measures for the use of cloud services and some unique regulations such as network separation to prevent a third party's unlawful access to the company's credit information computer system. With respect to the information communications sector, the PIPA stipulates specific technical and managerial security measures that ICSPs are required to implement in order to prevent the leakage of personal information. As such, when it comes to Governance, Risk Management, Compliance ("GRC") matters, practices vary depending on the industry. In particular, stricter audit and reporting requirements would apply to companies in the financial sector.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

(a) In the financial sector, the EFTA sets forth the standards for ensuring safety with respect to the facilities, electronic apparatus and human resources, which must be implemented by financial companies, electronic financial business entities and subsidiary electronic financial business entities to ensure safety and reliability of the electronic financial transactions.

(b) With respect to the telecommunications sector, the Network Act requires that the following types of ICSPs must obtain a certification for their information protection management system: (i) common telecommunications business operators providing ICN services in Seoul Special Metropolitan City and any other Metropolitan Cities; (ii) companies that operate clustered information and communications facilities; and (iii) companies whose revenue generated in the sector of information and communications services in the previous year is not less than 10 billion won, or whose average number of daily users over the past three months is not less than one million.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

The Network Act requires that the CISO must be designated from the company's director-level employees (unless the ICSP or the like is a small business). If the CISO has reported issues relating to a potential Incident to the board of directors or representative director, and the directors have failed to properly respond to prevent the Incident occurring, such failure may amount to a breach of directors' duties.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) Under the amended version of the Network Act, in principle, all ICSPs (other than small business enterprises) must designate a director-level CISO and report such fact to the

Ministry of Science and ICT. The CISO of a company that meets certain thresholds in terms of their assets or number of employees (e.g., the company's total assets at the end of the immediately preceding business year was at least KRW 5 trillion) may not perform any duties other than that of the CISO as prescribed by law. Any financial company or electronic financial business must also appoint a CISO, and the CISO may not perform any duties other than that of the CISO if the financial company or electronic financial business entity meets certain thresholds in terms of their assets or number of employees.

(b) Any personal information processor that processes personal information of 10,000 data subjects or more must establish a manual which provides information regarding the measures to be implemented in response to personal information leakage Incidents.

(c) Under the EFTA, financial companies and electronic financial business must analyse and assess the vulnerability of electronic financial infrastructure, including the assessment on the information technology sector, at least once each business year. Moreover, under the PICIA, the head of the management organisation of the critical information and communications infrastructure must analyse and evaluate the vulnerabilities of the infrastructure every year.

(d) See point (c) above.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Under the Network Act, the Minister of Science and ICT may order the ICSPs and the Collective ICN Facility Operators to do the following, if he or she finds that it is necessary to analyse the cause of the infiltration Incident:

(i) retain relevant material such as records of access to the ICN;
(ii) submit the relevant material to the infiltration Incident; and
(iii) allow physical access to the business site to investigate the cause of the Incident.

Moreover, the providers of critical information communications services and the Collective ICN Facility Operators must submit information regarding any infiltration Incident, such as statistics by type of intrusion cases, statistics of traffic of the relevant ICNs, and statistics of use by access channel, to the Ministry of Science and ICT and KISA.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In the event that an Incident occurs due to the personal information processor's violation of the PIPA, the data subject may claim damages against the personal information processor. In this case, the personal information processor will be liable for damages unless it can prove that there was no wilful misconduct or negligence of the processor that caused the Incident. If the data subject incurs any damages caused by the Incident due to the personal information processor's wilful misconduct or gross negligence, the court may award up to treble damages. Also, the data subject may seek statutory damages up to KRW 3 million, if the Incident was caused by wilful misconduct or negligence of the personal information processor.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In 2014, there was a personal information leakage Incident of over 100 million items of personal information stored by one of the major card companies in Korea being leaked. The victims of the leakage brought a claim against the company and the court awarded damages in the amount of KRW 10,000 to each of the plaintiffs for the leakage Incident. Moreover, in recent years, the amount of fines imposed against companies involved in a leakage Incident increased substantially, as it is shown in the case where an internet shopping site was required to pay an administrative fine of KRW 4.5 billion (approx. USD 3.8 million) for a leakage Incident.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The personal information processor may be found liable for a tort under Korean Civil Act, if the plaintiff proves that (i) there was a violation of relevant data protection laws by the processor of the personal information, (ii) the data subject has incurred damages due to the Incident, and (iii) there is a causal relationship between the damage and the violation.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Under the Network Act, ICSPs of a certain size must purchase liability insurance policy, join a mutual aid programme or accumulate reserves for compensation of damages to their users, if any. Moreover, under the Credit Information Act, financial companies and credit information companies must also take measures necessary to fulfil liability to compensate damage by purchasing insurance, joining a mutual aid programme, or accumulating reserves.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No. As a reference matter, among the insurances mentioned in question 6.1 above, the insurance required under the Network Act is intended to ensure the ICSP's compensation of damages incurred by the user as a result of the ICSP's wilful misconduct or negligence amounting to a violation of the data protection/privacy provisions under the Network Act.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The following authorities have investigatory powers of law enforcement: National Intelligence Service; National Police Agency Cyber Bureau; Forensic Science Investigation Department of the Supreme Prosecutors' Office; and Financial Supervisory Service.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there is no legislation or regulation in Korea that requires organisations to implement backdoors in the IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys.

Hwan Kyoung Ko is a partner in the Technology, Media & Telecommunications/Data Protection, and Cybersecurity and Fintech Practice Group. He is regarded as a leading expert in the telecommunication, data protection and cybersecurity and fintech regulation field and was recognised as a leading lawyer of the year in the TMT practice area by *Legal Times* in 2016. He has advised numerous BigTech/IT companies and government agencies on data protection and cybersecurity-related issues. Mr. Ko has also been involved in efforts to promote the Big Data industry in Korea, as witnessed by his participation in a recent Hackathon event hosted by the Presidential Committee on the Fourth Industrial Revolution.

Mr. Ko is a recipient of the 2019 Presidential Citation (for active involvement in the promotion of legislation to drive the data economy), the 2016 Minister of the Interior and Safety's Award (in the data protection sector) and the 2014 KISA President's Award for Personal Data Protection.

Mr. Ko holds a B.A. from Korea University and an LL.M. from Georgetown University Law Center. He is admitted to the New York and Korean Bars.

Lee & Ko
Hanjin Building 63
Namdaemun-ro, Jung-gu
Seoul 04532
Korea

Tel: +82 2 772 4000
Fax: +82 2 772 4001/2
Email: hwankyoung.ko@leeko.com
URL: www.leeko.com

Kyung Min Son is a partner in the Technology, Media & Telecommunications Practice Group at Lee & Ko. He has advised various telecommunications and IT companies, with a focus on various issues in all TMT areas, including mobile and regulatory issues in internet services, such as issues on privacy, internet contents, and internet advertisements.

He also has expertise in the areas of data privacy & cybersecurity and fintech, where he represents various domestic and foreign companies. Prior to joining Lee & Ko, Mr. Son served as a judge advocate officer for the Korean Navy.

Mr. Son received his LL.B. from Seoul National University and his LL.M. from the University of Southern California. He is admitted to the Seoul Bar.

Lee & Ko
Hanjin Building 63
Namdaemun-ro, Jung-gu
Seoul 04532
Korea

Tel: +82 2 772 4918
Fax: +82 2 772 4001/2
Email: kyungmin.son@leeko.com
URL: www.leeko.com

Lee & Ko's evolution as the premier law firm in Korea parallels in many ways the solid economic development of the country for more than 40 years. Our firm is one of the top law firms in Korea that is recognised for its expertise in over 30 specialised practice areas, and consistently acclaimed over the years as one of the leading firms in Asia by internationally respected legal publications and league tables. Lee & Ko has a global client base that includes multinational corporations in many different industries.

In particular, the firm's DPC/TMT team (Data Privacy & Cybersecurity/Technology, Media & Telecommunications) has extensive experience, knowledge, and expertise in a wide range of cases involving, among others, security breaches, hacking Incidents and DPC/TMT-related regulatory issues, transactional matters and litigations. The team is known as one of the top experts in the field with unrivalled knowledge and knowhow in Korea.

www.leeko.com

Mexico

Creel, García-Cuéllar, Aiza y Enríquez

Begoña Cancino

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
The Federal Criminal Code provides for two different criminal types when it comes to unauthorised access: simple; and aggravated. The aggravation criteria depend on the purported intention to cause damages by obtaining a specific result with the unauthorised access, especially when it entails the violation of intellectual property rights. Unauthorised access is then a federal crime under articles 211 *bis* 1 to 211 *bis* 7 of the Federal Criminal Code, but also article 426, which is contained in a chapter devoted exclusively to copyrights and provides that performing any act with the purpose of breaking an encrypted satellite signal or carrying programs without the proper authorisation, would be penalised with imprisonment from six months to four years, as well as a fine. Development and distribution of equipment intended to receive an encrypted signal and services intended to receive or assisting others in receiving an encrypted signal, will be also penalised as described in this paragraph.

Also, the Federal Criminal Code provides that a person who, with or without authorisation, modifies, destroys or causes loss of information contained in credit institutions' systems or computer equipment protected by a security mechanism shall be penalised with imprisonment of up to six months to four years, as well as a fine. Moreover, an unauthorised person who knows or copies information from credit institutions' computer systems or equipment protected by a security mechanism shall be subject to imprisonment of three months to two years, as well as a fine.

Denial-of-service attacks
The Federal Criminal Code does not provide any definition, or similar definition, for this criminal offence. However, article 427 *quater*, it includes penalties of imprisonment from six months to six years and a fine to those who provide services to the public aimed primarily at circumventing an effective technological protection measure of any work of authorship (including, of course, software).

Phishing
The Federal Criminal Code does not provide any definition for phishing; however, such criminal offence could be considered fraud. According to article 386 of the Federal Criminal Code, a person commits fraud when he/she handles information through deceit, takes advantage of errors or misleads a person with the intent of obtaining a financial gain. In such case, the responsible party shall be subject to imprisonment of three days to 12 years, as well as a fine.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
The Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour may fall under the scope of hacking. The aforementioned penalties are applicable in this case. If the criminal offence is committed against the state, the relevant authority shall be subject to imprisonment of one year to four years, as well as a fine.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
The Federal Criminal Code contains a specific criminal offence in this regard, providing that those who manufacture, import, distribute, rent or in any way market devices, products or components intended to circumvent an effective technological measure, would be subject to imprisonment from six months to six years and a fine.

Possession or use of hardware, software or other tools used to commit cybercrime
The Federal Criminal Code provides that those who, knowingly, without authorisation and for profit, suppress or alter, by themselves or through another, any information on rights management, will be imposed with six months' to six years imprisonment and a fine. The same penalty will be imposed on any person who, for profit: distributes, or imports for distribution, information on rights management, knowing that it has been suppressed or altered without authorisation; or distributes, imports for distribution, transmits, communicates or makes available to the public, copies of works, performances, performances or phonograms, knowing that the information on rights management has been suppressed or altered without authorisation.

Identity theft or identity fraud (e.g. in connection with access devices)
The Credit Institutions Law provides that a person who produces, manufactures, reproduces, copies, prints, sells, trades or alters any credit card, debit card or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be given a prison sentence of three to nine years, by the relevant authority, as well as a fine.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
As mentioned, identity theft of identity fraud are penalised under the Credit Institutions Law, if such activities are committed by any counsellor, official, employee or service provider of any credit institution there would be grounds for alleging breach of confidence and the penalties would increase.

In addition, under the Mexican Industrial Property Law, the theft of trade secrets – by electronic means or not – by current or former employees constitutes a crime and triggers imprisonment and fines to the responsible parties.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
The Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour may fall under the scope of hacking. The aforementioned penalties are applicable in this case. If the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one year to four years, as well as a fine.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
In addition, activities such as espionage, conspiracy, crimes against means of communication, tapping of communications, acts of corruption, extortion and money laundering could be considered threats to the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

The Federal Criminal Code includes a complete chapter devoted to crimes in connection with copyrights, where the unauthorised production, reproduction, introduction in the country, storage, transportation, distribution, commercialisation or other uses for commercial speculation purposes will be sanctioned with imprisonment and fines.

1.2 Do any of the above-mentioned offences have extraterritorial application?

In principle, all of the above-mentioned offences are applicable only within Mexican territory; however, there might be cases of serious criminal offences in which the Mexican authorities may collaborate with other authorities in other jurisdictions.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The Federal Criminal Code does not provide for any exception such as "ethical hacking"; however, it should be noted that most of the crimes referred therein will be considered as such if the activity has been carried out for profit or with the aim to cause damage.

The Federal Law against Organized Crime provides that in the investigation of a crime which is assumed on good grounds that a member of organised crime is involved, it is possible to tap private communications by means of electronic systems and subject to a judicial order. The same occurs with the General Law to Prevent and Sanction Kidnapping Crimes, and when the Mexican government must request a judicial warrant to intercept private communications for national security purposes and accordingly, the Federal Telecommunications and Broadcasting Law in its articles 189 and 190 allows competent authorities to control and tap private communications and provide support to those official requests.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Please see the following Applicable Laws:

- the Mexican Constitution;
- the Federal Telecommunications and Broadcasting Law (FTBL);
- the Federal Law on the Protection of Personal Data held by Private Parties (the Data Protection Law), its regulations, recommendations, guidelines and similar regulations on data protection;
- the Federal Law on Transparency and Access to Public Information;
- the General Law on Transparency and Access to Public Information;
- General Standards as specified under the Mexican Official Standard regarding the requirements that shall be observed when keeping data messages;
- the Law on Negotiable Instruments and Credit Operations;
- the Mexican Federal Tax Code;
- the Credit Institutions Law;
- the Sole Circular for Banks;
- the Industrial Property Law;
- the Mexican Copyright Law;
- the Federal Labour Law;
- the Federal Criminal Code;
- the Law of the National Security Guard;
- the National Strategy of Cybersecurity 2017; and
- the White Paper on National Defense of the Mexican State.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

There is an industry-specific risk in certain sectors: financial; telecommunications; and health, not only in the private sector, but also at the governmental level. The National Security Guard Act, in November 8, 2019, which allows Mexican authorities to rule judicial decisions to intervene private communications for National Security purposes, anticipated the replacement of the Center of Investigation and National Security by the newly created National Intelligence Center, a Mexican intelligence agency controlled by the Ministry of Security and Civilian Protection, the main purpose of which is to preserve the State's integrity, stability and endurance. This was a radical structural change in the Mexican government as the former intelligence agency used to be under the control of the Ministry of Interior, the purpose being the reinvention of the image of the agency as an authority focused on security instead of conducting

"authorised" espionage. During 2019, the National Intelligence Center hosted an official meeting where representatives of the National Bureau of Investigation and the Department of Justice agreed with the Mexican Government on a programme to coordinate efforts to reinforce the exchange of information concerning cybersecurity, including best practices to cope with activities that pose a risk for Mexico and the USA (i.e. financial, telecommunications and health, not only in the private sector, but also at the governmental level).

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

According to Mexican law (specifically, the Mexican Privacy Law), organisations are compelled to implement corrective, preventive and improvement measures to make security measures adequate to avoid a breach. Organisations should be able to differentiate between material and non-material harm under Mexican laws by conducting a risk analysis. Material harm should be prioritised over non-material harm and will always depend on the business, scope, context and processing of the data compromised in the incident. Industry-specific risk identification of material and non-material harm is thus crucial for all companies facing a cybersecurity incident. Certain sectors, such as healthcare and banking, should provide companies with the required latitude to adapt their own internal policies. Compromising the security of databases, sites, programs or equipment (and this may include failure to implement required security measures) constitutes an administrative infringement of the Mexican Privacy Law, which could be sanctioned with fines of up to Mex$25.6 million, a fine that may be doubled if sensitive data is compromised.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

From those incidents involving personal data, the Mexican Data Privacy Law does not contain any obligation to the National Institute of Transparency, Access to Information and Protection of Personal Data ("INAI") about potential or actual incidents, including cyber threat or cyber-attacks. If the incident compromised personal data of identifiable individuals, then the business (understood as a data controller) must evaluate the breach through a risk assessment, implement the corrective, preventive and improvement actions to reinforce security measures, and determine if the event may result in prejudice to the property or non-pecuniary rights of the data subjects; if so, it should notify the affected parties. Under the Mexican Privacy Law (Federal Law on the Personal Data held by Private Parties), security breaches occurring at any stage of processing personal data must be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights. There is no official format to notify breaches; however, the Mexican Privacy Law and its regulations provide that the notification must include, at least, the nature of the breach, the personal data compromised, corrective actions implemented immediately by the data controller, recommendations concerning measures for the data owner to protect its interests after the breach and the means available for the data owner to obtain more information on the breach.

On the other hand and pursuant to article 106 of the Securities Market Law and its general provisions, listed entities are compelled to report to the National Banking and Securities Commission ("CNBV") all relevant events that may affect the value of its assets, including those involving incidents that impact a large amount of personal information, regardless of the cause of such events and including, of course, breaches of contracts, negligence or violation of other statutes such as the Mexican Privacy Law.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Rules for reporting threats of breaches that may involve the unauthorised use of personal data are contained in the Mexican Data Privacy Law and Regulations. These Regulations provide that the data controller must inform only the data subject, not the federal regulator or other authority. As per the timeline, the regulations only provide that this notification should be conducted immediately, and after assessing whether the breach significantly affects the property or non-pecuniary rights of the data subjects upon having conducted an exhaustive review of the magnitude of the breach, so that the prejudiced data subjects may act appropriately.

There is no official format to notify breaches related to data privacy matters; however, the Mexican Privacy Law and its regulations provide that the notification must include, at least, the nature of the breach, the personal data compromised, corrective actions implemented immediately by the data controller, recommendations concerning measures for the data owner to protect its interests after the breach and the means available for the data owner to obtain more information on the breach. Failure to comply with reporting obligations constitutes an administrative infringement to the Mexican Data Privacy Law and may trigger fines that increase in cases of repeated infringements.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The Applicable Laws empower the following authorities to investigate an Incident: (i) the General Attorney Office; (ii) Public Prosecutors; (iii) the National Banking and Securities Commission ("CNBV"); (iv) the INAI; and (v) the Federal Telecommunications Institute ("IFT"). Public Prosecutors in Mexico are in charge of investigating cyber activities and to resolve them, a cyber police has been created to follow up on crimes or unlawful activities committed through the internet. Complaints directed to the cyber police can be submitted via its website, by phone or through a Twitter or email account; in

addition, the Federal Police has created a scientific division called the National Centre For Cyber-Incidents Response, specialising in providing assistance to the victims or claimants of cyber threats and cyber-attacks. In the case of data protection, the INAI may conduct investigations to follow up personal data matters. Regarding telecommunications, the IFT is in charge of this sector.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

There is no single framework for non-compliance with notice requirements and penalties in Mexico; they will depend heavily on the relevant law and regulator, for example:

- Failure to comply with reporting obligations constitutes an administrative infringement of the Mexican Data Privacy Law and may trigger fines that increase in case of repeated infringements.
- Failure to comply with reporting obligations of relevant events under the Securities Market Law may trigger the imposition of injunctive measures or the temporary suspension of the registry of securities' issuer.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

As of April 2020, the INAI has sanctioned many companies in cases involving violation of Data Privacy Law, most of them involving cybersecurity issues, to the extent that such authority has imposed fines for up to US$21 million in the last nine years. Entities devoted to financial services have been fined with almost US$12 million, followed by entities related to the communication industry, which fines amount US$2.5 million.

According to INAI and figures obtained from the official source of the National Commission for the Protection and Defence of Users of Financial Services, Mexico takes the eight place in identity theft worldwide; 67% of those reported cases are due to the loss of documents, 63% for robbery, and 53% for information taken directly from credit accounts. During the third quarter of 2017, cyber fraud grew by 102% compared with the same period in 2016, representing a proportion from 13% to 51% per year. In 2018, 49,843 claims were filed upon identity theft and only 54% were decided in favour of the claimant. In addition, Mexico take the second place in Latin America with the greatest number of cyber-attacks to mobile devices.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Generally, yes.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Generally, yes.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Generally, yes.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Generally, yes, if organisations inform in advance that they will take these measures and obtain the proper consent from employees.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Generally, no, other than the restrictions already provided in the Industrial Property Law and the Copyright Law.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, according to the Mexican Data Privacy Law, data controllers have to implement technical, physical and administrative measures in order to protect personal data from damage, loss, alteration, destruction, unauthorised use, access or processing.

The Federal Criminal Code and the Law on Negotiable Instruments and Credit Operations also include penalties to prevent criminal offences or violation of cybersecurity measures.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes. Such requirements are found under the Law on Negotiable Instruments and Credit Operations, the Credit Institutions Law, the Securities Market Act and the Federal Criminal Code, among other official regulations and guidelines.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

There is not a single framework, nor penalties for non-compliance with: prevention; mitigation; response to incidents amounting to a breach of directors; or officers' duties in Mexico. This will depend heavily on the relevant law.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There is no single framework providing for requirements to designate a CISO or equivalent; establishing incident response plans, conducting risk assessments and performing vulnerability tests will depend heavily on the Applicable Law and industry. When personal data is involved, the appointment of a data privacy officer would then be required, as well as the implementation of other measures to avoid risks (including cyber risks).

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Requirements will depend heavily on the relevant law and especially whether the risk constitutes a relevant incident. Please refer to questions 2.4 and 2.6 above.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

According to Article 32 of the Federal Criminal Code, organisations and companies are civilly liable for the damages caused to third parties by crimes committed by their partners, managers and directors. The state is similarly liable for the crimes committed by its public officials.

The Federal Civil Code provides a standard of civil liability established in Article 1910, which provides that a party that illegally causes harm to another person shall be obliged to repair the damage, unless he/she proves that the damage was produced as a consequence of the victim's guilt or negligence.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

This is not applicable.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

This is not applicable.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Generally, yes.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

Generally, no.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Applicable Laws empower the following authorities to investigate an Incident: (i) the General Attorney Office; (ii) public Prosecutors; (iii) the INAI; and (iv) the IFT.

Public Prosecutors in Mexico are in charge of investigating and resolving cyber activities; a cyber police service has been created to follow up on crimes or unlawful activities committed through the Internet. Complaints directed to the cyber police can be submitted via its website, by phone, or through a Twitter or email account; in addition, the Federal Police have created a scientific division called the National Centre For Cyber-Incidents Response, specialised in providing assistance to the victims or claimants of cyber threats and cyber-attacks.

In the case of data protection, the INAI may conduct investigations to follow up personal data matters. The IFT is in charge of the telecommunications sector.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

This is not applicable in Mexican law.

Begoña Cancino is a partner in the Mexico City office. Her practice focuses on Intellectual Property, Data Privacy, Regulatory and Administrative Litigation. From the standard IP front, Ms. Cancino counsels clients from all kinds of industries with the protection and enforcement of their IP rights in Mexico, also assisting with the transfer of IP portfolios within the context of complex corporate transactions involving all sorts of IP rights (such as trademarks, copyrights and appellations of origin). Ms. Cancino also provides assistance with her legal advice on regulatory and advertising, assessing our clients to comply with all applicable provisions with COFEPRIS and PROFECO. She has represented clients in all sort of administrative litigation proceedings, in general, concerning advertising, health, environmental and, of course, IP matters, before administrative authorities and federal judicial courts. Pursuant to the data privacy aspects of her practice, Ms. Cancino has counselled clients from multiple industries in the drafting and implementation of internal policies, privacy notices and specific legal concerns, not only regarding client daily operations, but also within the context of cross-border transactions and internal investigations for compliance.

Creel, García-Cuéllar, Aiza y Enríquez
Torre Virreyes Pedregal no. 24, piso 24 col.
Molino del Rey, Ciudad de México 11040
Mexico

Tel: +52 55 4748 0600
Email: begona.cancino@creel.mx
URL: www.creel.mx

With over 80 years of history, Creel, García-Cuéllar, Aiza y Enríquez is a leading full-service corporate law firm with an unwavering commitment to excellence. We have an established reputation for delivering creative, specialised and responsive legal advice on the most complex and innovative matters in Mexico for the most sophisticated and demanding clients. Our practice is based on the philosophy that a client is best served by legal advice designed to anticipate and avoid problems, rather than respond to them. Our goal is to be the law firm of choice for clients with the most demanding transactions and projects, and, in such endeavour, become a strategic service provider to them, by offering the type of legal advice that gives clients certainty and peace of mind. We view our role as one of adding value to our clients and providing them with certainty and peace of mind. As such we strive to become their strategic service provider.

www.creel.mx

CREEL GARCÍA-CUÉLLAR AIZA Y ENRÍQUEZ

Norway


Stian Hultin Oddbjørnsen


Ove André Vanebo


Iver Jordheim Brække


Mari Klungsøyr Kristiansen

Kluge Advokatfirma AS

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Intrusion into a computer system, hacking included, constitutes a criminal offence under section 204 of the **Penal Code** of 20 May 2005. The provision states that a person who, by breach of a protective measure or other illicit means, obtains access to a computer system or part thereof, may be given a penalty of a fine or imprisonment for a term not exceeding two years. An example of a prosecution under this section is found in the Supreme Court Judgment HR-2020-2056-A, where a person was given a sentence of imprisonment for one year (with nine months being conditional).

As for the rest of the following activities, hacking would primarily be considered a criminal offence to be investigated by the prosecuting authority. Consequently, administrative offences are less likely.

Denial-of-service attacks
Denial-of-service attacks will typically fall within the scope of section 206 of the **Penal Code**, which stipulates that creation of a risk of operational disruption is a criminal offence. Under this section, a person who, by transferring, damaging, deleting, degrading, modifying, adding or removing information, illicitly creates a risk of interruption or significant disruption of the operation of a computer system, may be given a penalty of a fine or imprisonment for a term not exceeding two years.

Phishing
Phishing constitutes a criminal offence under section 202 of the **Penal Code**, which criminalises the violation of identity. Under this provision, a person who, *inter alia*, illicitly gains possession of another person's proof of identity or an identity that is easily mistakable for the identity of another person, with intent to:

a) make an illicit gain for himself/herself or for another person; or
b) cause another person loss or inconvenience,

may be punished with a fine or imprisonment for a term not exceeding two years.

An example of a prosecution under this section is found in the Supreme Court Judgment HR-2020-1352-A, where a person was given a sentence of imprisonment of one year and six months. However, this case also involved fraud by using the other person's proof of identity, which added to the sentence.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware constitutes a criminal offence under section 206 of the **Penal Code**. This is the same section that applies to denial-of-service attacks, mentioned above.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Section 201 of the **Penal Code** criminalises an act where any person who, with intent to commit a criminal act, illicitly makes available to another person:

a) a password or other information that may provide access to computerised information of a computer system; or
b) a computer program, or something else that is particularly suitable for committing criminal acts, targeting computerised information or computer systems.

Such distribution or sale is penalised with a fine or imprisonment for a term not exceeding one year. As section 16 of the **Penal Code** also criminalises attempts to offences which may be punishable by imprisonment for a term of one year or more, the offering for sale of such tools could also be considered a criminal act.

Possession or use of hardware, software or other tools used to commit cybercrime
The possession of tools to commit cybercrime is also criminalised by section 201 of the **Penal Code**, mentioned directly above, as this provision also applies to cases where the person produces, procures or possesses the mentioned authentication details, computer programs, etc.

When it comes to the use of the hardware, software or other tools used to commit cybercrime, it is not the *use* that is criminalised, but rather the more specified acts mentioned here in question 1.1. This includes violation of identity under section 202, intrusion into a computer system/hacking under section 204, violation of the right to private communication under section 205, risk of operational disruption under section 206, and the like.

Identity theft or identity fraud (e.g. in connection with access devices)
The above-mentioned section concerning violation of identity in the **Penal Code**, section 202, which criminalises phishing, also criminalises identity theft or identity fraud. In addition to criminalising the act where a person illicitly gains possession

of another person's proof of identity or an identity that is easily mistakable for the identity of another person, the provision criminalises the illicit *use* of such identity.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
The **Penal Code**'s "regular" theft section, section 321, only applies to tangible property, and there is no general *electronic* theft provision as such. However, there are different provisions that may apply to the electronic theft of specific types of information. *Inter alia*, the **Penal Code** section 208 penalises the illegal appropriation of a business secret with a fine or imprisonment not exceeding one year, and section 203 provides a similar penalty for the possession of a decoding device giving access to a protected communication service.

In addition, the **Copyright Act** of 15 June 2018 section 79, *cf.* sections 80 and 3, provides that streaming is punishable with a fine or imprisonment for a term not exceeding three years. Such punishment does, however, require that it was evident that the streaming was breaking the law and that the use of the illegal source was capable of significantly damaging the financial interests of the author.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
To our knowledge, there are no provisions directly addressing unsolicited penetration testing if the testing itself does not harm the system or its owner. However, if the access to the system is a result of intrusion into a computer system, such action is punishable under the above-mentioned section 204 of the **Penal Code**.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Another activity considered a criminal offence under Norwegian law is the violation of the right to private communication. Section 205 of the **Penal Code** provides, *inter alia*, that penalty of a fine or imprisonment for a term not exceeding two years may be applied to any person who illicitly breaches a protective measure and thereby gains access to information transmitted using electronic or other technical means.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The conditions for extraterritorial application of the **Penal Code** are set forth in section 5. Such application *usually*, although with several exceptions, requires:

a) a personal nexus to Norway (being if a person is a Norwegian national, domiciled in Norway or acts on behalf of an enterprise registered in Norway); and
b) that the offence is also punishable under the law of the country in which it is committed.

In addition, the prosecution of acts committed abroad are limited to cases where such prosecution is considered "in the public interest". Consequently, the above-mentioned offences may be given extraterritorial application.

What might, however, be more relevant for cybersecurity offences is how section 7 relatively openly regulates when an act is to be considered to have taken place in Norway, thereby not actualising the question of extraterritorial application. This provision provides that where the punishability of an act is contingent on or affected by an actual or intended effect, the act is also deemed to have been committed at the place where the effect has occurred or was intended to be caused. Hence, where the effects of one of the above-mentioned offences occur in Norway, e.g. where the intrusion into a computer system in Norway is executed from another country, such act is punishable under Norwegian law.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Section 78 of the **Penal Code** lists nine different mitigating factors that are to be considered when deciding the sentence of a criminal act. The most relevant factors in relation to the above-mentioned offences are where (1) the offender has made an unreserved confession, and (2) the offender has prevented, reversed, or limited the harm or loss of welfare caused by the offence, or sought to do so.

As for exceptions, there is no general rule stating that "ethical" intent excepts an act from being punished when it otherwise meets the conditions of the criminal offence. On the contrary, the main rule is that exceptions are not to be given. However, they could still be considered in extraordinary circumstances.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

There is no general Applicable Law especially dedicated to cybersecurity in Norway. The relevant Applicable Laws that regulate cybersecurity are fragmented and often sector-specific. We have listed *some* of the essential Applicable Laws regarding cybersecurity below:

a) All processing of personal data is subject to the **General Data Protection Regulation (GDPR)** (Regulation (EU) 2016/679) and the **Personal Data Act** of 15 June 2018.
b) The **National Security Act** of 1 June 2018 aims, *inter alia*, to prevent, detect and counteract activities threatening national sovereignty, including regulations on information security.
c) The **Electronic Communications Act** of 4 July 2003 and the **Electronic Communications Regulation** of 16 February 2004 aim to give secure and modern communication services to the public.
d) The **Energy Act** of 29 June 1990 and the **Power Supply Preparedness Regulation** of 7 December 2012 aim to secure power supply and include regulations on information security and safety measures for control systems.
e) The **Regulation on the Use of Information and Communication Technology** of 21 May 2003 (**ICT Regulation**) within the financial services regulates, *inter alia*, the use and security of ICT systems in that sector.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Applicable Laws mentioned in question 2.1 are all applicable to critical infrastructure, or operators of essential services if the provided service falls within the scope of the Applicable Laws. However, there are no provisions in the Applicable Laws that are specifically designed to solely regulate Incidents in this regard. The provisions are often written in a way that allows one single statutory provision to cover many types of circumstances, including Incidents regarding cybersecurity.

An example is **GDPR** article 24 (1), which states that the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the **GDPR**. The article will be relevant for all organisations processing personal data, including activities related to critical infrastructure or similar activities that require such processing.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

All of the above-mentioned Applicable Laws in question 2.1 require organisations to monitor, detect, prevent and mitigate Incidents.

Organisations that process personal data and can be defined as a data controller or processor must follow the regulations under the **GDPR**. Data controllers and processors are, among other statutory regulations in the **GDPR**, required to follow the principles relating to the processing of personal data according to **GDPR** article 5. The organisations are also obligated to implement technical and organisational measures to ensure a level of security appropriate to the risk of the data processing.

Organisations that fall within the scope of the **National Security Act** are required to carry out risk assessments and implement proportionate security measures.

The **Electronic Communications Act** requires organisations to implement necessary security measures for the protection of communications and data.

Energy suppliers and other organisations that fall within the scope of the **Energy Act** are obligated to implement necessary security measures for all processing of information relating to the power supplies. Organisations are also, *inter alia*, responsible for protecting sensitive information and preventing access to non-legitimate users.

Organisations that fall within the scope of the **ICT Regulation** are required to develop procedures to ensure the protection of equipment, systems, and information relevant to the activities in the organisation. The organisations are also required to do risk analyses and establish criteria for the acceptable risk associated with the use of the ICT systems.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

All organisations under the Applicable Laws described in question 2.1 are required to report information to authorities related to Incidents or potential Incidents. However, not all of the Applicable Laws set out the nature and scope of the information that is required to be reported. We have written an overview of the relevant authorities to which the information is required to be reported below in question 2.6.

Organisations that process personal data according to the **GDPR** shall, without undue delay, notify the personal data breach to the supervisory authority. The reporting obligation is triggered for any personal data breach unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The information the organisations are required to report shall at least include the nature of the personal data breach, the name and contact details of the data protection officer or other contact point, a description of the likely consequences of the personal data breach and a description of the measures taken to address the personal data breach.

In cases where they have been affected by security-threatening activities or if there is a well-founded suspicion of security-threatening activities, organisations that fall within the scope of the **National Security Act** are required to immediately notify the security authorities.

The **Electronic Communications Act** requires organisations to notify authorities if there are security breaches or risks of such. However, it is not necessary to notify the authorities if it is possible to document that satisfactory technical protection measures have been implemented for the data covered by the breach of security.

Energy suppliers and other organisations that fall within the scope of the **Energy Act** are required to give the authorities any necessary information for the implementation of provisions pursuant to the Act. This can include information about Incidents or potential Incidents.

Organisations that fall within the scope of the **ICT Regulation** are required to inform the authorities without undue delay about Incidents that result in a significant reduction in functionality resulting from breaches regarding confidentiality, integrity or access to ICT systems.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Some of the Applicable Laws described in question 2.1 require organisations to report information related to Incidents or potential Incidents to any affected individuals.

The **GDPR** requires organisations that process personal data and are considered data controllers to inform the data subject of personal data breaches that are likely to result in a high risk to the rights and freedoms of the affected individuals. The information the organisations are required to report shall at least include the nature of the personal data breach, the name and contact details of the data protection officer or other contact point, a description of the likely consequences of the personal data breach and a description of the measures taken to address the personal data breach.

Organisations that fall within the scope of the **Electronic Communications Act** must notify individuals of significant risks of security breaches, including security breaches that have damaged or destroyed data, or violated the individual's right to privacy. However, the organisations are not obligated to report Incidents to affected individuals if the organisations are able to prove that appropriate security measures have been implemented on the data affected by the Incident. There are no provisions in the Act that describe the nature and scope of information required to be reported.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The following regulators are responsible for enforcing the requirements according to the Applicable Laws described in question 2.1:

a) The **Norwegian Data Protection Authority** (**NDPA**) is responsible for enforcing provisions in the **GDPR**.
b) The **Norwegian National Security Authority** is responsible for enforcing the provisions in the **National Security Act**.
c) The **Norwegian Communication Authority** (**NCA**) is responsible for enforcing the **Electronic Communications Act** and the **Electronic Communications Regulations**.
d) The **Energy Directorate** is responsible for enforcing the provisions in the **Energy Act**.
e) The **Norwegian Financial Supervisory Authority** is responsible for enforcing the provisions in the **ICT Regulation**.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

We have described how the regulators mentioned in question 2.6 can sanction organisations below:

a) The **NDPA** can impose administrative fines up to EUR 20 million or, in the case of an undertaking, 4% of the total worldwide annual turnover. Infringements of the reporting requirements under the **GDPR** are limited to EUR 10 million or, in the case of an undertaking, 2% of the total worldwide annual turnover.
b) The **Norwegian National Security Authority** can impose coercive fines and administrative fines for violations of the **Security Act**.
c) The **NCA** can impose coercive fines and administrative fines for violations of the **Electronic Communications Act** and the **Electronic Communications Regulations**.
d) The **Energy Directorate** can impose coercive fines and administrative fines.
e) The **Norwegian Financial Supervisory Authority** can impose coercive fines.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The authorities mentioned in question 2.6 have, to our knowledge, not taken any enforcement action in cases of non-compliance where an organisation has been exposed to a cyber-attack, or any other enforcement action in direct relation to cybersecurity. However, the authorities have on several occasions fined organisations in cases of non-compliance with the Applicable Laws mentioned in question 2.1. The two cases mentioned below received a lot of media attention in Norway.

Nine hospitals received a fine of NOK 800,000 each from the **NDPA** in 2017. The hospitals outsourced ICT operations and processing of data concerning health to a processor in Bulgaria. The **NDPA** concluded that the outsourcing was not in compliance with the obligations under the **GDPR**, including the provisions regarding safety management, risk assessments and access management.

A Norwegian municipality was fined NOK 1.6 million by the **NDPA** in 2019 after a student had gained unauthorised access to a school's ICT systems, uncovering severe flaws in the security systems of the municipality including personal information.

The **NCA** sanctioned a telecom provider with a fine of NOK 11 million because the telecom provider failed to implement adequate security measures to prevent unauthorised access to the computer system that operates parts of the Norwegian emergency network.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

As there are no specific prohibitions against the use of beacons, organisations are permitted to use beacons under Norwegian law. However, as IP addresses would be considered personal data under Norwegian law if the organisation collecting the IP address has the means to identify the person using the IP address, the use of beacons will require the organisation to have a legal basis under **GDPR** article 6.

The use of beacons could also be regulated by section 2-7b of the **Electronic Communications Act**, regulating the use of cookies. This section provides that the user of the computer in question must be informed of and consent to the use of cookies. Such consent could, however, be provided through the user's browser settings.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
As is the case for beacons, there are no specific prohibitions against the use of honeypots. Consequently, organisations are permitted to use honeypots under Norwegian law as long as such use is compliant with the above-mentioned cybersecurity legislation.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The use of sinkholes is also permitted under Norwegian law, as long as such use is compliant with the above-mentioned cybersecurity legislation.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

As a rule, the **Regulation on Employers' Access to Email Inboxes and Other Electronically Stored Material** of 2 July 2018 provides that organisations are not permitted to monitor or intercept the employees' email accounts or internet usage. Section 2 in the mentioned regulation does, however, allow for organisations to access the email accounts when it is considered necessary to protect the daily management of the organisation or other legitimate interest of the organisation. The same section also allows the organisation to access the employees' internet usage when it is considered necessary to manage the organisation's network or to identify or solve a security breach in the network.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There are no restrictions as to the import or export of technology designed to prevent or mitigate the impact of cyber-attacks under Norwegian law.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Organisations must adhere to the legal requirements in Norway, and market practice in a specific sector that deviates from the requirements under the Applicable Laws will not be considered legitimate.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Some of the Applicable Laws mentioned in question 2.1 regulate specific market sectors:

a) Telecom providers and other organisations that operate in the telecommunications sector are subject to the **Electronic Communications Act** and the **Electronic Communications Regulation**.
b) The **Energy Act** applies to organisations that produce, transform, transfer, sell or distribute energy.
c) Banks, financial undertakings, and other organisations that operate within the financial sector are subject to the **ICT Regulation**.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

The failure by a company to prevent, mitigate, manage or respond to an Incident, primarily if the company is required by law to perform such activities (like the requirements mentioned under section 2) would normally be considered a breach of the board's duties under the **Limited Liability Company Act** of 13 June 1997, and the **Public Limited Liability Company Act** of 13 June 1997 sections 6-12 and/or 6-13. The officers' duties are normally more limited. However, in certain situations, depending on multiple factors, the failure might also constitute a breach of the officers' duties.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

The companies required to implement the measures listed in (a)–(d) are corresponding to the companies that fall within the scope of the statutes and regulations listed in question 2.1. However, not all measures are required under all acts. In summary, the following measures are required:

a) The **Power Supply Preparedness Act** section 2-2 provides that energy suppliers are required to designate a CISO; under the **ICT Regulation** section 2, financial undertakings are required to designate persons that are responsible for the different parts of their ICT systems, including information security; and under **GDPR** article 37, some companies are required to designate a data protection officer.
b) The **ICT Regulation** sections 2 and 5 and the **Power Supply Preparedness Act** sections 2-4 and 6-4 state that, respectively, electronic communication providers and financial undertakings are required to establish a written Incident response plan or policy. In addition, most companies processing personal data are required to establish such plans under **GDPR** article 32.
c) The **ICT Regulation** section 3 and the **Power Supply Preparedness Act** section 2-3 state that the above-mentioned companies are required to conduct cyber risk assessments. Under **GDPR** article 35, this also applies to most companies processing personal data.
d) The requirement to perform penetration tests or vulnerability assessments would in some cases follow from the requirements mentioned in c).

In addition, the **Electronic Communications Act** section 2-7 more generally provides that telecom providers are to

implement the security measures necessary to secure their data. Such measures could include all of the above, depending on the situation. The measures could also be required under the **Security Act** for companies that, due to a decision based on section 1-3 of the Act, have been decided to fall within the scope of the Act.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies are under no general obligation to specifically disclose any information in relation to cybersecurity requirements or Incidents under Norwegian law, other than those mentioned in section 2.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Proceedings related to cybersecurity are typically not the subject of private civil action lawsuits. It is more common that one of the responsible authorities mentioned in question 2.6 issues an administrative fine to a private subject. The private subject can then take the administrative fine to court if they disagree with the decision made by the authorities.

However, we believe that an increase in civil lawsuits between data subjects and organisations that have violated the data subject's rights under **GDPR** may occur. This is because it follows from **GDPR** article 82 that any data subject who has suffered material or non-material damage as a result of an infringement of the **GDPR** shall have the right to receive compensation from the controller or processor for the damage suffered.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There are, to our best knowledge, no examples of published civil or other private actions that have been brought into Norwegian jurisdiction in relation to Incidents.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Any person who negligently or wilfully causes an Incident may under the Norwegian law of torts be held liable for any foreseeable loss which has occurred due the negligent or wilful act.

However, the Norwegian law of torts will only be applicable if there is no other relevant law or contract that regulates the same matter. For example, a data subject cannot claim damages based on tort law if the data subject can claim compensation according to the rules in the **GDPR**.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations in Norway are permitted to take out insurance against Incidents.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

We are not familiar with any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The most relevant investigatory powers are set forth in the **Criminal Procedure Act** of 22 May 1981. Under this Act, the police, the prosecuting authority and/or the court – depending on the severity of the investigatory power – may, *inter alia*:

a) conduct a search of a data system and order any person with access to the system to give the encryption keys necessary to access the system. Such order could also include forced biometrical authentication;
b) order the expeditious preservation of specified computer data that has been stored by means of a computer system, including from providers of electronic communication services and networks;
c) seize evidence, including tangible property and electronically stored information; and
d) secretly put a suspect's computer under surveillance and thereby gather information through technical means, such as secretly installing a software on the computer, utilising the suspect's credentials if such are gathered or entering the computer's system through hacking.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Applicable Laws do not require organisations to implement backdoors in their IT systems. As for requirements for organisations to provide law enforcement authorities with encryption keys, such requirements exist (see question 8.1).

Stian Hultin Oddbjørnsen is specialised within "tech law". Stian is a recognised and ranked lawyer within TMT. Stian advises both public and private entities on, *inter alia*, regulatory and cybersecurity-related matters in this field of law. Furthermore, Stian has extensive knowledge and experience in procurement, contract drafting and negotiations within digitalisation projects. Stian is also a proven litigator and handles disputes and court cases. He has also acted as a deputy judge in Drammen District Court for a period of two-and-a-half years, handling both civil and criminal cases. He regularly publishes articles on tech law and often acts as a lecturer on such topics.

Kluge Advokatfirma AS
Bryggegata 6
0250 Oslo
Norway

Tel: +47 957 89 414
Email: sho@kluge.no
URL: www.kluge.no

Ove André Vanebo assists private and public clients with data privacy, labour law, cybersecurity and dispute resolution. He has wide-ranging experience with privacy matters, such as surveillance, storing and further processing of personal data and data breaches. He also frequently acts as a lecturer and has written numerous articles about privacy and data protection.

Kluge Advokatfirma AS
Bryggegata 6
0250 Oslo
Norway

Tel: +47 915 49 378
Email: ove.vanebo@kluge.no
URL: www.kluge.no

Iver Jordheim Brække is a part of Kluge's tech team. He primarily assists clients with advisory work within technology, public procurement and data privacy.

Kluge Advokatfirma AS
Bryggegata 6
0250 Oslo
Norway

Tel: +47 464 24 959
Email: iver.jordheim.brekke@kluge.no
URL: www.kluge.no

Mari Klungsøyr Kristiansen is a part of Kluge's tech team. She primarily assists clients with dispute resolution and advisory work within technology and public procurement.

Kluge Advokatfirma AS
Bryggegata 6
0250 Oslo
Norway

Tel: +47 479 03 123
Email: mari.klungsoyr.kristiansen@kluge.no
URL: www.kluge.no

Kluge is a full-service, independent law firm with offices in Oslo, Stavanger, Bergen and Hamar. Kluge offers comprehensive advice and assistance within all major fields of business law and is one of the leading law firms in Norway. Kluge's practice group within TMT (or "tech law") is especially renowned for large digitisation projects within the public sector but offers a wide range of services to both private and public clients within this field of law. Cybersecurity and privacy law are amongst the practice group's field of expertise, which includes several recognised practitioners.

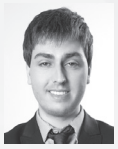
www.kluge.no

KLUGE

Poland


Mateusz Borkiewicz


Grzegorz Leśniewski


Jacek Cieśliński

Leśniewski Borkiewicz & Partners (LB&P)

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Criminal offence: Hacking is a criminal offence under Section 267 of the Polish Criminal Code. Anyone who, without being authorised to do so, acquires access to information not intended for him or her, by, *inter alia*, connecting to a cable transmitting information or by breaching electronic, magnetic or other special protection for that information is liable to a fine (up to PLN 1.08 million), the restriction of liberty or imprisonment for up to two years. This also applies to anyone who acquires access to any part of a computer system without being authorised to do so.

Administrative offence: Unauthorised access to information may constitute an act of unfair competition. This applies in particular to cases where such action is aimed at violating the interests of another entrepreneur (e.g. unauthorised access to information of economic value that may constitute a breach of the business secret of another entity). In such cases, hacking may be of interest to the President of the Office of Competition and Consumer Protection. This offence has a penalty of up to 10% of the annual turnover.

If unauthorised access to information includes information constituting personal data, a violation of the GDPR is also likely; this has a penalty of up to EUR 20 million or, in the case of an enterprise, up to 4% of its total annual global turnover (whichever is higher).

Denial-of-service attacks
Criminal offence: Denial-of-service (DoS) attacks are a criminal offence under Section 269a of the Polish Criminal Code. Anyone who, without being authorised to do so, by transmitting, damaging, deleting, destroying or altering information data, significantly disrupts a computer system or telecommunications network is liable to imprisonment for up to five years. In some cases, DoS attacks can also constitute offences under Sections: 268 (hindering access to information); 268a (damaging databases due to interfering or preventing automatic collection and transmission of data or hindering access to data); and 269 (if the offence regards data that is of particular significance for national defence, transport, safety or the operation of the government or any other state authority or local government).

Administrative offence: DoS attacks may constitute:

- act of unfair competition (i.e. restricting access to the market for another entrepreneur, in accordance with the Suppression of Unfair Competition Act of 16 April 1993); or
- unfair market practice, i.e. making it difficult for consumers to access services (in accordance with the Act on Combatting Unfair Market Practices).

In both cases, DoS attacks may be of interest to the President of the Office of Competition and Consumer Protection. The penalty for this offence is a fine of up to 10% of the annual turnover.

Phishing
Criminal offence: Phishing is a criminal offence under Section 287 of the Polish Criminal Code. Anyone who, in order to achieve material benefits or to inflict damage upon another person, affects the automatic processing, collection or transmission of data or changes, deletes or introduces new entries, without being authorised to do so, is liable to imprisonment for up to five years. If phishing leads to identity theft or fraud, it may also be considered an offence under Section 190a of the Polish Criminal Code (see more below).

Administrative offence: Cases where phishing is aimed at violating the interests of another entrepreneur, i.e. in order to: illegally obtain information covered by the business secret of another entity; disseminate false information about another entity; or restrict access to the market of another entity (e.g. obstructing the transaction's execution), it may be of interest to the President of the Office of Competition and Consumer Protection. A penalty of up to 10% of the annual turnover will apply.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Criminal offence: Infecting IT systems with malware is a criminal offence under Section 287 of the Polish Criminal Code (for quotation, see "Phishing" above). Moreover, according to Section 269 of the Polish Criminal Code, anyone who destroys, deletes or changes a record on a computer storage media that is of particular significance for national defence, transport, safety or the operation of the government or any other state authority

or local government, or that interferes with or prevents the automatic collection and transmission of such information, is liable to imprisonment for up to eight years. Infection of IT systems with malware may be also a criminal offence if it results in at least one of the following: unauthorised access to information; destruction of information; damage to databases; denial of service; computer fraud (i.e. phishing); or disruption of work on a network.

Administrative offence: If infection of IT systems with malware results in: unauthorised access to information; destruction of information; damage to databases; denial of service; computer fraud (i.e. phishing); or disruption of work on a network, it may constitute an administrative offence, including: a violation of the General Data Protection Regulation (GDPR) (e.g. if it concerns personal data), which has a penalty of up to EUR 20 million or, in the case of an enterprise, up to 4% of its total annual global turnover (whichever is higher); or an act of unfair competition (if the aim is to violate the interests of another entrepreneur), which has a penalty of up to 10% of the annual turnover.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Criminal offence: Such actions are criminal offences under Section 269b of the Polish Criminal Code. Anyone who creates, obtains, transfers or allows access to hardware or software adapted to commit cybercrime (e.g. damaging databases, preventing automatic collection and transmission of data or hindering access to data) is liable to imprisonment for up to five years.

Administrative offence: Such actions may also be of interest to the President of the Office of Competition and Consumer Protection, with a penalty of up to 10% of the annual turnover. In particular, the production, import, distribution, sale or rental, for commercial purposes, of prohibited devices (within the meaning of the provisions on the protection of certain services provided electronically based on conditional access) constitute an act of unfair competition (art. 15b of the Suppression of Unfair Competition Act of 16 April 1993).

Possession or use of hardware, software or other tools used to commit cybercrime

Criminal offence: Anyone who creates, obtains, transfers or allows access to hardware or software adapted to commit the offences specified above, including computer passwords, access codes or other data enabling access to the information collected in the computer system or telecommunications network, is liable to imprisonment for up to three years.

Administrative offence: In order to commit the acts of unfair competition described in the above points, it is sufficient that a given action 'threatens' the interests of another entrepreneur (specific violations, e.g. access to the information covered by the business secret, are not a necessary element). It means that, in specific cases, the mere possession of hardware, software or other tools used to commit cybercrime, could justify the actions of the President of the Office of Competition and Consumer Protection (a penalty of up to 10% of the annual turnover).

Identity theft or identity fraud (e.g. in connection with access devices)

Criminal offence: Identity theft or fraud is a criminal offence under Section 190a of the Polish Criminal Code. Anyone who pretends to be another person and uses his or her image, or other personal data, in order to cause property or personal damage may be subject to imprisonment for up to three years.

Administrative offence: A designation of a company that may mislead customers as to its identity (e.g. by using a company name or other distinctive symbol previously legally used to designate another entity) constitutes an act of unfair competition (art. 5 of the Suppression of Unfair Competition Act of 16 April 1993) and may be of interest to the President of the Office of Competition and Consumer Protection (with a penalty of up to 10% of the annual turnover).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Criminal offence: Electronic theft is a criminal offence under Section 266 of the Polish Criminal Code. Anyone who, in violation of the law or an obligation accepted, discloses or uses information learned in connection with the function or work performed, or public, social, economic or scientific activity pursued, is liable to a fine, the restriction of liberty or imprisonment for up to two years.

Administrative offence: Undertaking such actions may, in certain circumstances, constitute a breach of business secrets and result in a number of civil law consequences, and if committed by other entrepreneurs, it may even result in the President of the Office of Competition and Consumer Protection carrying out proceedings (with a penalty of up to 10% of the annual turnover).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Criminal offence: Unsolicited penetration testing is a criminal offence under Section 267 of the Polish Criminal Code. Anyone who, without being authorised to do so, acquires access to information not intended for him or her, by, *inter alia*, connecting to a cable transmitting information or by breaching electronic, magnetic or other special protection for that information, is liable to a fine (up to PLN 1.08 million), the restriction of liberty or imprisonment for up to two years. This also applies to anyone who acquires access to any part of a computer system without being authorised to do so.

Unsolicited penetration testing may also constitute a criminal offence under Section 266 of the Polish Criminal Code – Electronic theft (described in the point above).

Administrative offence: The exploitation of an IT system without the permission of its owner may constitute an act of unfair competition (a breach of the business secret of another entity). In such cases, it may be of interest to the President of the Office of Competition and Consumer Protection, with a penalty of up to 10% of the annual turnover.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

1. Under Section 165, subsect. 1 point 4 of the Polish Criminal Code, anyone who puts the lives or health of many people or possessions in danger by affecting computerised data commits a separate crime and may be sentenced for up to eight years of imprisonment. If any offence is committed due to or in relation to the offences listed above, the offender may be found guilty for committing several offences by one act, and if the offence is related to terrorism, the punishment may be even more severe.
2. The Polish legal system contains a number of regulations sanctioning threats to IT systems that do not result from external factors (such as hacking, phishing, etc.), but from the negligence of entrepreneurs using such systems (failure to meet certain security obligations imposed by law), i.e.:
   - National Cybersecurity System Act of 5 July 2018 (NCS) (NIS Directive implementation): a penalty of up to PLN 150,000, incl. for not carrying out a systematic risk assessment or not managing the risk of an Incident.
   - GDPR: a penalty of up to EUR 10 million and, in the case of an enterprise, up to 2% of its total annual

global turnover (whichever is higher), incl. for failure to implement security measures for IT systems adequately to the risk.
- Telecommunications Law of 16 July 2004: a penalty of up to 3% of the annual income, incl. for failure to implement technical and organisational IT security measures.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Criminal offences: All of the listed offences are included in the Polish Criminal Code and, although there are no specific regulations on extraterritorial application of these offences, the territorial application of the Polish Criminal Code depends on the place of the offence. The Polish Criminal Code (Sections 5 and 6, subsect. 2) is applicable when the offender acted or omitted an action to which they were obliged, or where the result occurred or should have occurred in accordance with the intention of the offender, or acted outside Poland but the result of one of the listed offences occurred in Poland, i.e. the offence affects IT systems located in Poland or systems used for providing services in Poland.

Administrative offences: The exterritorial application will depend on the context of the case, including the type of violation and the competent authority to investigate it. In most cases, the authorities will be able to take appropriate action against entities that have establishment in Poland or against actions that have or may have effects in Poland.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Yes, there are general principles set out in the Polish Criminal Code and applicable to all the offences specified in it (including the offences listed above), which allow for mitigating penalties:
- Section 59 – draw back – allows the court to draw back from imposing a penalty in case of milder offences.
- Section 60 – extraordinary mitigation of punishment – allows the court to extraordinarily mitigate the punishment in cases indicated in a statute or in particularly justified cases when even the mildest punishment would be incommensurably harsh.

Also, when it comes to administrative offences, Polish regulations provide mechanisms that allow the reduction of liability for illegal activities. Mitigating circumstances often include actions such as voluntary removal of the effects of a breach or cooperation with the authority.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

European Union – Key Applicable Laws:
1. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.
2. Regulation (EU) 2019/881 on European Union Agency for Cybersecurity (ENISA) and on information and communication technology cybersecurity certification – under this regulation, soon there will be a uniform system of certification of cybersecurity of ICT in the EU – allowing for easier verification of the level of cybersecurity provided by organisations.
3. Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market.
4. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).
5. Directive (EU) 2015/2366 on payment services in the internal market (PSD2).

Poland – Key Applicable Laws:
1. Criminal Code of 6 June 1997;
2. Labour Code of 26 June 1974;
3. Civil Code of 23 April 1964;
4. NCS (NIS Directive implementation);
5. Trust Services and Electronic Identification Act of 5 September 2016;
6. Data Protection Act of 10 May 2018;
7. Suppression of Unfair Competition Act of 16 April 1993;
8. Competition and Consumer Protection Act of 16 February 2007;
9. Telecommunications Law of 16 July 2004;
10. Counter-terrorism Act of 10 June 2016;
11. Crisis Management Act of 26 April 2007;
12. Payment Services Act of 19 August 2011;
13. Classified Information Protection Act of 5 August 2010; and
14. Recommendations and Instructions of the Financial Supervision Commission (KNF) concerning management of information technologies and security of the ICT environment.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Network and Information Systems Directive is implemented in Poland by the NCS. However, there are some sectors of critical infrastructure that are wholly or partially regulated in other Applicable Laws: the trust service providers; health service providers established by the Chief of Internal Security Agency or Chief of Foreign Intelligence Agency (i.e. Trust Services and Electronic Identification Act of 5 September 2016 and a set of regulations concerning some categories of health service providers); and telecommunications entrepreneur(s) referred to in the Telecommunications Law of 16 July 2004 (partially regulated in the NCS and partially in the Telecommunications Law – in relation to cybersecurity requirements and Incident reporting).

Financial service providers are also subject to additional obligations regulated in statutes, which are specific for different kinds of financial service providers, e.g. for payment service providers: Payment Services Act of 19 August 2011 (implementing PSD2) – please also see the answer to question 4.2.

The NCS exceeds the requirements of the NIS Directive by including public administration, and partially the telecommunications sector, into the scope of the regulation. The NCS makes public administration provide at least the same standard

of cybersecurity as operators of essential services and digital service providers, i.e. take measures to monitor, detect, prevent or mitigate Incidents at a similar level as operators of essential services and digital service providers.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes, organisations are required to undertake several activities to monitor, detect, prevent or mitigate Incidents. Under the NCS, operators of essential services shall implement a security management system for the information system used to provide the essential service that is relevant and proportionate to the estimated risk (having regard to the state of the art) and measures to prevent and minimise the impact of Incidents (examples are provided). Security audit of the information system must be carried out at least every two years. Under the NCS, digital service providers shall also face similar and relevant requirements.

In accordance with the Act on Provision of Electronic Services 2002, the service provider, in general, shall use appropriate cryptographic techniques.

In accordance with the Payment Services Act 2011, the provider, as part of the risk management system, takes risk mitigation measures and implements control mechanisms to manage risk through an effective Incident management procedure, including detection and classification of Incidents, including those related to ICT systems (e.g. strong user authentication).

In accordance with the GDPR, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (examples are given in Section 32, subsect. 1 of the GDPR).

In accordance with the Telecommunications Law 2004, the provider of publicly available telecommunications services is obligated to apply technical and organisational measures to ensure security and integrity of the network, services and transmission of messages in relation to the services provided and ensuring security of personal data processing (some duties are further specified).

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, although depending on the type of organisation, the obligation may differ.

Operators of essential services, under the NCS, are required to report information related to Incidents to the appropriate Computer Security Incident Response Team (CSIRT) within 24 hours of the Incident being detected. The obligation is triggered when the operator of essential services classifies the Incident as serious. The notification about the Incident should contain basic information on the Incident, reporting person and entity and measures taken.

Organisations being digital service providers under the NCS have similar obligations.

Organisations from the financial sector who provide payment services are also required to report certain Incidents related to the payment services and possibly to cybersecurity. Depending on the type of provider, they are required to report to the KNF, or another appropriate authority, operational Incidents, Incidents related to security, Incidents involving an account information service provider (AISP) and a payment initiation service provider (PISP), and annual report on frauds related to payment services. The obligation is usually triggered by the sole occurrence of the Incident.

Telecommunications entrepreneurs are required to report to the President of the Electronic Communication Authority (*Prezes Urzędu Komunikacji Elektronicznej*) any breach of security or integrity of the network or services that had a significant effect on the functioning of the network or services, giving information on the breach and any preventive and corrective measures taken. The obligation is triggered by every significant breach.

Moreover, if the Incident has an effect on personal data processed by any organisation, such organisation is required to report such an Incident to the President of the Personal Data Protection Authority (*Prezes Urzędu Ochrony Danych Osobowych*).

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under the GDPR, when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The communication shall describe in clear and plain language the nature of the personal data breach and contain basic information on the Incident specified in the Regulation.

There are situations when communication to the data subject may not be required.

Under the Act on Provision of Electronic Services 2002, the provider is obligated to ensure access by the customer to up-to-date information on special risks related to the use of the electronic service.

Under the Telecommunications Law 2004, when a personal data breach by a provider of publicly available telecommunications services may have adverse effects on the rights of the subscriber or end user who is a natural person, the provider shall immediately notify the breach to the subscriber or the end user with exceptions set out in the Telecommunications Law 2004, e.g. Section 174a, subsect. 5.

The President of the Office of Electronic Communications (UKE) may impose on the telecommunications entrepreneur the obligation to publicly disclose the security or integrity breach of the network or services.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The relevant authorities are:

- President of the Personal Data Protection Office (PUODO), https://www.uodo.gov.pl.
- Ministers responsible for the relevant sectors – depending on the sector where the given operator of essential services or digital service provider operates, and one central body (Polish Financial Supervision Authority).
- President of the UKE, https://www.uke.gov.pl/.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Infringements of the provisions concerning personal data connected with cybersecurity issues shall be subject to administrative fines up to EUR 10 million, or in the case of an undertaking, up to 2% of the total global annual turnover of the preceding financial year, whichever is higher.

Penalties stipulated by the NCS may be up to PLN 200,000; however, if through an inspection of the body responsible for cybersecurity, it is found that the operator of essential services or digital service provider persisted in breaching the NCS, a fine of up to PLN 1 million will be imposed.

The body responsible for cybersecurity may also impose a fine on the managers of the operator of essential services (not exceeding 200% of their monthly salary) if they failed to exercise due care to meet specific obligations.

Penalties imposed by the Telecommunications Law may reach up to 3% of the income of the penalised entity generated in the previous calendar year (imposed both by the President of UKE and the PUODO, as applicable).

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In April 2019, the PUODO issued a PLN 55,750.50 fine to the Lower Silesian Football Association for the unauthorised publishing on the internet of the personal data of people licensed as football referees in 2015. Published data included personal identification numbers and home addresses. It could have been avoided had the Association implemented requirements concerning technical and organisational measures in relation to the IT system used to process personal data.

In March 2019, the PUODO issued a PLN 943,470 fine to a company that failed to provide information on personal data processing (art. 14 of the GDPR) to the entrepreneurs whose personal data the company processed but lacked their email addresses. This could have been avoided had the company implemented requirements concerning technical and organisational measures in relation to the IT system.

In September 2019, the PUODO issued a PLN 2.8 million fine to a company that failed to implement data protection measures adequate to the risks, including: a lack of appropriate response procedures in case of detection of unusual network traffic; and an ineffective system of monitoring potential threats. This could have been avoided had the company implemented requirements concerning technical and organisational measures in relation to the IT system.

In October 2019, the PUODO issued a PLN 40,000 fine to a public entity (city Mayor) for violation of the principle of integrity and confidentiality of processing by: storing personal data without a backup system; and failing to conduct a risk analysis. This could have been avoided had the city Mayor implemented requirements concerning technical and organisational measures in relation to the IT system.

In November 2019, the PUODO issued a PLN 201,000 fine to a company that failed to implement technical measures, enabling a withdrawal of consent and exercising the right to request deletion of data. This could have been avoided had the company implemented requirements concerning technical and organisational measures in relation to the IT system.

The PUODO issued numerous fines for failure to cooperate with him for the purpose of the proceedings (key obligation in the event of violations related to cybersecurity):

- In March 2020: a fine for preventing the inspection (PLN 20,000).
- In July 2020: a fine for failing to provide the supervisory authority with access to personal data and other information necessary for the performance of its tasks (PLN 15,000).
- In July 2020: a fine for failing to provide the supervisory authority during the conducted inspection with access to premises, data-processing equipment and means, and access to personal data and information necessary for the performance of its tasks (PLN 100,000).

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

Yes. Currently there are no regulations prohibiting the use of beacons. However, due to the fact that beacons may acquire various information, e.g. IP address, which may constitute personal data, all regulations concerning technologies, such as cookies and other similar solutions, apply to beacons.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

Yes. There are no regulations prohibiting the use of honeypots. Moreover, NASK (*Narodowa Akademicka Sieć Komputerowa* – National Academic Computer Network – which is not only a research institute but also one of the three types of CSIRTs) is currently running a research project aimed at early identification and warning about cyberthreats based on honeypots.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

Yes. Sinkholes may be used as a measure to detect and deflect Incidents and there are no regulations prohibiting such measures. They are, in fact, used by various organisations (e.g. in the telecommunications sector).

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

1. Recording electronic communications, i.e. data operations in IT systems (their modification, reading, transfer or deletion) and assigning individual actions to specific persons, may constitute, in a specific case, a desirable technical solution to ensure an appropriate (required by law) level of information security.
   Similarly, logging network traffic to/from IT systems often serves as a measure to demonstrate compliance of IT systems with security requirements.
2. In certain cases, however, monitoring or interception of electronic communications may be subject to specific regulations, i.e. the Labour Code (permissible only under some circumstances). Section 222, subsect. 1 of the Labour Code allows this if it is necessary, e.g., for providing employees' safety or property protection. Section 223 of the Labour Code allows for, e.g. monitoring of employees' emails if it is necessary to ensure work organisation, allowing for proper management of full work time and proper usage of working equipment made accessible to the employee. However, while monitoring employees' emails/computers, the employer has to comply with confidence of correspondence and other personal rights of the employee – which includes compliance with the GDPR.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Most governments around the world do not regulate the importation or domestic use of cryptographic features in mass-market products, and the few economies that do typically use a very limited regulatory touch with a narrow product scope.

According to the World Semiconductor Council (WSC) principles for commercial cryptographic technologies in mass-marketed ICT products, the regulation of commercial encryption should be limited and encryption technology mandates should be prohibited, acknowledging the widespread use of encryption and the limited value in regulating the commercial market.

International standardisation in the field of cryptography plays a critical role in enabling both security and interoperability. Many governments around the world acknowledge the benefit of using voluntary global standards instead of regulating encryption in commercial/industrial market ICT products locally.

Nevertheless, pseudonymisation or anonymisation tools must meet specific security requirements resulting in particular from the application of the principles of privacy by design and privacy by default (art. 25 of the GDPR). This means, for example, that anonymisation solutions should not use techniques that are generally considered compromised. Similarly, the pseudonymisation tools must meet a certain level of security with regard to the encryption key management mechanisms. The use of solutions that do not meet the above-mentioned requirements exposes the recipient to liability for non-compliance with information security obligations.

However, in the current legal situation, the status of technology providers (importers/exporters of IT solutions) is not clear. Also, the European Data Protection Board (EDPB) does not explicitly support the acceptance or exclusion of the possibility of controlling technology providers in terms of compliance with art. 25 of the GDPR.

The potential assumption that technology providers are obliged to comply with privacy by design/by default rules opens the way to (examples show the relevance of the issue):

- application of art. 84 of the GDPR (introduction of new/use of current national regulations to impose sanctions on the technology provider for violation of art. 25 of the GDPR); and
- assessment of solutions created by the technology provider as 'unlawful' in the event of non-compliance with the requirements of art. 25 of the GDPR (as a result, replacing solutions that are incompatible with such obligations, on the market, could be qualified as a 'unfair competitive practice' and may have all consequences foreseen for such situations, including obligation to withdraw the solution from the market).

Regardless, importers/exporters of pseudonymisation or anonymisation tools have specific tax and customs obligations.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice varies across different business sectors but there are no recognised deviations from the strict legal requirements. The differences between sectors depend rather on specific characteristics of the sector and the relevance of this sector. Some sectors, e.g. the financial services, telecommunications or new technologies sectors, are naturally more concerned and conscious about information security issues.

Also, under the NCS, public administration became part of the cybersecurity system and fell under further reporting guidelines and procedures, issued by the authorities of adequate level, in regulations other than the Applicable Laws.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes, there are specific legal requirements in both sectors.

(a) Financial services sector: detailed requirements concerning providing security of information in IT systems for providers of financial services are set out in the Recommendations and Instructions of the KNF and specific statutes. In general, the providers are required to take measures to mitigate risk and develop control mechanisms aimed at risk management and security breach risk management.

(b) Telecommunications sector: companies are required (under Section 175, subsect. 1 of the Telecommunications Act) to take technical and organisational measures (providing a level of security appropriate to the risk, regarding the newest technological achievements and expected costs) aimed at providing security and integrity of the network, services and transfer of messages in relation to the provided services.

See also the answer to question 2.4.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Managers may be found liable towards the company if an Incident occurs due to their lack of due diligence (i.e. lack of internal procedures required in the given circumstances or failure to enforce them/lack of control if they are applied when they were responsible for compliance matters).

In some cases, a manager may be personally fined under the NCS if, due to his/her negligence, the company that is an operator of an essential service fails to execute regular risk assessments and audits, or fails to make proper notifications of the Incidents.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) No; however, under the NCS, companies that are operators of essential services are required to form an internal structure to ensure cybersecurity and designate a contact person to maintain contact with other state cybersecurity system elements.

(b) Operators of essential services are required to document cybersecurity measures related to the IT system used to provide essential services. Digital service providers are required to take measures allowing for risk management in relation to cybersecurity, but there is no obligation for a written form. Other companies are not required to establish any written Incident response plan or policy.

(c) Operators of essential services are required to conduct periodic cyber risk assessments and management of such risk and perform an audit at least once every two years. Digital service providers are required to take measures allowing for risk management, including monitoring, auditing and testing. Such measures may be necessary, under the GDPR, to any company processing personal data in IT systems – to ensure cybersecurity of such systems – including periodical risk assessment, testing and evaluation of taken technical and organisational measures.

(d) Please see the answers above.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies rendering electronic services must provide their clients with current information on any particular risks associated with the use of the electronic services provided.

Publicly traded companies must execute their duties on providing the market with current reports and periodic reports, and since cybersecurity risks or Incidents may have a significant effect on their financial or economic situation, they may be required to be disclosed.

The GDPR provides for a procedure on the reporting of Incidents concerning personal data protection (Section 33 of the GDPR).

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The action related to civil liability may be brought against an offender (facing punishment and being liable for damages) or a company that failed to provide proper security measures against an Incident (liable for damages).

Action for damages – under Section 415 of the Polish Civil Code, action can be brought to compensate for actual damage (*damnum emergens*) and cost of opportunity (*lucrum cessans*). Section 444 of the Polish Civil Code allows for the claim damages to cover all costs related to the injury (e.g. medical care and drugs to treat the injury).

Action for compensation – under Section 445 of the Polish Civil Code, in addition to the claim for damages indicated above, the person who suffered injury may also be compensated for any harm suffered (including, e.g. psychological suffering). Section 448 of the Polish Civil Code refers to compensation to cover harm that resulted from the infringement of personal rights (e.g. damage to reputation).

There is also a possibility to bring a civil claim in criminal cases. Under Section 46 of the Polish Criminal Code, if the court convicts the offender, it may order the offender to partially or fully remedy any damage caused by the offence or compensate for any injury. The criminal court applies civil law provisions. This also applies when an offender commits an Incident-related offence (see the answer to question 1.1) and a person suffers damage or injury (e.g. in case the Incident involved a hospital) due to the offence.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

V CSK 141/17 (Supreme Court, 18 January 2018): the bank's client wanted to access her bank account through the internet. She entered her log-in data but was shown a notice saying the website was under maintenance. Later she discovered that the money she had was gone. It was determined in a separate (criminal) proceeding that a third person acquired her log-in data through phishing. The bank was found liable for not providing effective security measures and thus had to compensate for the damage the client suffered.

VI ACa 509/17 (Appeal Court in Warsaw, 30 August 2018): a third person accessed the bank account of a client of a bank and made several transactions for PLN 137,285 in total. The third person used the client's log-in data using the same IP address the client used on the same day. The bank used a two-factor authentication to send several messages (containing verification codes) for the client to authorise the transactions. The client claimed that not all of the used codes were used by him. The client was not sure if his computer was properly secured (e.g. if the software was up to date). The court decided that, in this case, the client was negligent in taking security measures while using payment services provided by the bank. The court also pointed out that the bank provided effective security measures and could not be held liable for the loss of the client's money.

Currently, a case is pending against the postal service operator for (in accordance with the lawsuit) obtaining millions of personal data records from the PESEL register and processing them in order to organise presidential elections.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes. Civil liability is based on contract or tort – one does not exclude the other. Liability based on tort includes acts and omissions leading to damage (can be limited in contract), regardless of whether there was a contractual obligation for specific acts or omissions.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. They are permitted and the cybersecurity insurance market is still developing. Taking out insurance against Incidents would also be treated as acting with due diligence while providing technical, organisational and legal measures concerning cybersecurity.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations concerning taking out insurance coverage against any type of Incident. However, insurance can only cover random Incidents – not planned or financed – that cannot be rationally excluded or mitigated.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Various governmental bodies have specific powers. Apart from the police or public prosecutors in criminal proceedings, note that the PUODO, as part of their audit powers, is entitled to access buildings, premises or other spaces, to review documents and information that are directly related to the subject matter of the audit, and carry out inspections of places, objects, equipment, mediums and information systems and ICT systems used to process data.

In accordance with the NCS, a person carrying out inspections of entities that are businesses is entitled to free access to and movement around the premises of the audited entity without the obligation to obtain a security pass to inspect equipment, mediums and information systems.

Similar powers are also held by personnel of the UKE that may also carry out inspections of the audited telecommunications networks and apparatuses.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes, under Section 179 of the Telecommunications Act, a telecommunications entrepreneur has to take technical and organisational measures of accessing and recording for the police and some other enforcement authorities to access and record telecommunications messages, sent or received by an end user, or terminal telecommunications equipment, and to access and record the metadata of such messages (messages include written, oral and other types of messages).

Under Section 9 of the Counter-terrorism Act of 10 June 2016, the Chief of the Internal Security Agency may order for classified investigative operations concerning an individual who is not a Polish citizen, including obtaining access to and recording data stored on a data storage device or terminal telecommunications equipment, IT systems and ICT systems.

Mateusz Borkiewicz has been advising since 2010 and has advised leaders in the internet industry, particularly in the areas related to GDPR implementation, provision of electronic services, consumer law, cloud computing and intellectual property law.
He has advised on strategic topics concerning, among others, issues of unfair competition, protection of trademarks, cybersecurity, domain disputes, spam, violations of personal rights on the internet (particularly in the context of hate speech towards public figures), managerial bribery and computer crimes, including virtual currencies theft.
He has served as Data Security Administrator and Data Protection Officer in several companies operating in the financial services, retail and automotive sectors.
He is the author of two books concerning personal data protection and many professional publications.
He also entered into the list of attorneys kept by the District Bar Council in Wrocław, Poland.

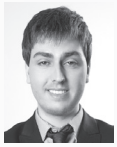
Leśniewski Borkiewicz & Partners (LB&P)
Podwale 83, room 11
50-414 Wrocław
Poland

Tel: +48 663 683 888
Email: mb@lbplegal.com
URL: www.lbplegal.com

Grzegorz Leśniewski has been advising since 2009. His main areas of practice include personal data protection, the law of new technologies, cybersecurity and M&A.
Before LB&P Legal, he developed the boutique law firm Leśniewski Legal, under which he advised on, among others, the implementation of GDPR by a Norwegian global provider of telecommunications and cable television services. He is also the Data Protection Officer at one of the major cloud computing companies in Poland since the entry of GDPR.
His former and current clients include, among others, globally present providers of digital products engineering services, multinational telecommunications service providers, the largest Polish social networking site (14 million active users), one of the largest multinational e-commerce businesses in the footwear industry, cloud computing service providers, as well as the market leader of call-center services in Poland.
He managed the implementation of numerous M&A processes, as well as negotiations in the process of buying/selling companies mostly from the TMT sector.
He also entered into the list of attorneys kept by the District Bar Council in Warsaw, Poland.

Leśniewski Borkiewicz & Partners (LB&P)
Podwale 83, room 11
50-414 Wrocław
Poland

Tel: +48 531 871 707
Email: gl@lbplegal.com
URL: www.lbplegal.com



Jacek Cieśliński has been advising since 2015. His counselling includes ongoing assistance focused largely on areas specific to the new tech sector, such as using modern marketing tools, including behavioural advertising (based on advanced profiling techniques) and remarketing conducted in cooperation with market-leading advertising networks, as well as combining/aggregating databases in groups of companies.
He also advised on the implementation of strategic projects, such as launching mobile applications and advanced stationary biometric scanning technology, combined with an e-commerce account.
He conducted a number of audits in the field of personal data protection and helped raise the awareness of IT/TMT industry employees in order to practically implement data protection standards (trainings for software developers, OPS departments, including second level).
He is associated with leading consulting companies in Poland and the Regional Chamber of Legal Advisers in Wrocław.

Leśniewski Borkiewicz & Partners (LB&P)
Podwale 83, room 11
50-414 Wrocław
Poland

Tel: +48 793 967 934
Email: jc@lbplegal.com
URL: www.lbplegal.com

Leśniewski Borkiewicz & Partners (LB&P) is a modern law firm that works mainly with clients operating within IT, TMT and e-commerce. We know the specifics of the new technologies sector and that allows us to propose practical solutions, taking into account typical risks, market practice and upcoming changes. LB&P has been created as a result of the further development of Leśniewski Legal. It has been formed by people with experience gained in one of the largest Polish advisory companies, as well as in specialised projects realised for international clients.
Our second brand, http://www.privacyfoxes.com, is dedicated to GDPR issues and implementing solutions for cross-border personal data flows.

www.lbplegal.com

Leśniewski Borkiewicz & Partners

Romania

Simion & Baciu


Ana-Maria Baciu


Cosmina Maria Simion


Andrei Cosma


Andrei Nicolae Dumbravă

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

In our jurisdiction, hacking constitutes the criminal offence of *Illegal access to a computer system*, regulated by the Romanian Criminal Code in article 360.

The law puts forward three ways in which this offence may be committed:

a. accessing a computer system without having a right to do so, punishable by three months to three years of imprisonment or a fine;
b. accessing a computer system without having a right to do so and with the purpose of obtaining computer data, punishable by six months to five years of imprisonment; or
c. accessing a computer system without the right to do so, if the access to the system was restricted or prohibited by any means for certain users, punishable by two to seven years of imprisonment.

A notable case of hacking activity prosecuted in Romania is that concerning the hacker Guccifer (Marcel Lazar Lehel), who, through illegal means, gained access to the emails of Collin Powell, the head of the Romanian intelligence service, members of the Bush and Rockefeller family as well as other celebrities. He was convicted for hacking.

Denial-of-service attacks

Denial-of-service (DoS) attacks fall under the *Disruption of the operation of computer systems* criminal offence regulated by article 363 of the Romanian Criminal Code. More specifically, this article states that gravely disrupting the operation of a computer system, without the right to do so, by inputting, transmitting, modifying deleting or corrupting data, or by restricting access to data is punishable by two to seven years of imprisonment.

Prosecution of DoS and distributed DoS (DDoS) types of attacks is less common in Romania. We note, however, one case in which the Prahova Tribunal where two persons were convicted for conducting DDoS attacks on the websites of public institutions and other private enterprises (Decision no. 391/2019).

Phishing

The deed of phishing is usually related to the criminal offence of *Misrepresentation*, regulated by article 244 of the Romanian Criminal Code. The offence covers misrepresenting false facts as being true and true facts as being false, with the purpose of obtaining undue material gains for oneself or for another, with the added condition that material damages were caused. The sanction is six months to three years of imprisonment.

The article stipulates another form of the offence, which refers to misrepresentation committed by using false names or capacities or other fraudulent means, which also covers phishing. The offence in this form is punishable by one to five years of imprisonment.

Two of the most common targets for perpetrators that perform phishing activities are customers of banks and customers of online shops. An example of a case is the one handled by the Court of Appeal Constanta, where the perpetrators used the method of phishing to gain access to eBay accounts of foreign citizens and afterwards perform online orders using those data (Decision no. 1251/2016).

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Since malware itself may be used for a variety of purposes, a variety of offences may be attributed to infecting IT systems with malware, depending on the purpose sought by the perpetrator.

As such, infecting an IT system with malware falls under:

a. the criminal offence of *Computer Fraud*, regulated by article 249 of the Romanian Criminal Code, defined as entering, altering or deleting computer data, restricting access to such data or hindering in any way the operation of a computer system in order to obtain a material benefit for oneself or for another, and, if it has caused damage to a person, the offence is punishable by two to seven years of imprisonment;
b. the criminal offence of *Illegal access to a computer system,* regulated by article 360 of the Romanian Criminal Code, as described above;
c. the criminal offence of *Illegal interception of computer data transmissions*, regulated by article 361 of the Romanian Criminal Code, refers to the interception, without the right to do so, of a transmission of computer data which is not public and which is intended for a computer system, and also to the interception, without a right to do so, of electromagnetic emissions from a computer system that contains computer data, deeds which are punishable by one to five years of imprisonment;
d. the criminal offence of *Altering the integrity of computer data*, regulated by article 362 of the Romanian Criminal Code and defined as the deed of altering, deleting or corrupting computer data or restricting access to such data, punishable by one to five years of imprisonment;

e. the criminal offence of *Disruption of the operation of computer systems*, regulated by article 363 of the Romanian Criminal Code, as described above; and
f. the criminal offence of *Unauthorised transfer of computer data*, regulated by article 364 of the Romanian Criminal Code, defined as the unauthorised transfer of computer data from a computer system or from a data storage device, punishable by one to five years of imprisonment.

We note a case in which infection with malware was used, handled by the Tribunal of Iasi (Decision no. 1234/2017). The malware infection was part of the application known as Cobalt Strike, and it was used to attack the banking system in order to obtain remote control of ATMs.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

In our jurisdiction this is covered by the criminal offence of *Illegal operations with devices or software*, regulated by article 365 of the Romanian Criminal Code. The text of law covers the production, import, distribution or the making available in any form of:

a. devices or software designed or adapted for the purpose of perpetrating the offences contained in Chapter VI of the Romanian Criminal Code, offences against security and integrity of computer systems and data, those being *Illegal access to a computer system, Illegal interception of computer data transmissions, Altering computer data integrity, Disruption of the operation of computer systems and Unauthorised transfer of computer data*; and
b. passwords, access codes or other such computer data allowing full or partial access to a computer system for the purpose of perpetrating the offences against security and integrity of computer systems and data, as regulated by Chapter VI of the Romanian Criminal Code.

Those deeds are punishable by six months to three years of imprisonment or by a fine.

Possession or use of hardware, software or other tools used to commit cybercrime

Following on the previously presented offence, article 365 of the Romanian Criminal Code has a second paragraph, which refers to owning a device, a piece of software, a password, access code or other data mentioned in the first paragraph. The legal provision specifies that the owning such articles must be with the **purpose** of perpetrating any offence against security and integrity of computer systems and data, regulated by Chapter VI of the Romanian Criminal Code. The sanction in this case is three months to two years of imprisonment, or a fine.

In a case handled by the Bucharest Tribunal (Decision no. 1899/2019), a person was sentenced for handling equipment meant to read passwords and other sensitive data related to credit cards and equipment installed at ATMs.

Identity theft or identity fraud (e.g. in connection with access devices)

There is no specific criminal or administrative offence regulated by the Romanian legislation covering the theft of online identity or identity fraud, except if it is done in relation to a public servant, with the intention to mislead or maintain the deceit, in order to produce legal consequences for oneself or for another.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Electronic theft may include:

a. electronic theft of know-how or trade secrets – the theft of know-how or trade secrets, to which a breach of confidence by a current of former employee is ascribed, is deemed illegal, but not considered an offence (either criminal or administrative) under the Governmental Emergency Ordinance no. 25/2019. However, the methods of obtaining such information may constitute the offence of *Illegal access to a computer system* or any other offence against the security and integrity of computer systems and data, such as *Unauthorised transfer of computer data*; and
b. making available to the public, via the Internet or computer networks, works carrying neighbouring rights; unauthorised reproduction of software on IT systems; and reproduction, distribution or publication communication of works carrying neighbouring rights, are considered criminal offences under Romanian law (Law no. 8/1996), and are sanctioned with a maximum of one to three years of imprisonment.

We note that the simple possession of pirated goods, without the purpose of distributing them, is not an offence, and as such there is no jurisprudence in this area. There are, however, cases in which pirated software was sold and installed as genuine licensed software (Decision no. 494/2017 issued by the Botosani Court).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

While not regulated as such by Romanian legislation, unsolicited penetration testing falls under the offence of *Illegal access to a computer system*, regulated by article 360 of the Romanian Criminal Code, punishable by three months to three years of imprisonment or by a fine. If the deed was committed on a computer system to which, through processes, access to devices or specialised programs is restricted or prohibited for certain categories of users, the sanction is imprisonment for a minimum of two years and a maximum of seven years.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Two other offences are worth mentioning, both concerning transactions and other financial operations:

a. the offence of *Making fraudulent operations*, regulated by article 250 of the Romanian Criminal Code, which includes making cash withdrawal operations, loading or unloading of an electronic money instrument or a fund transfer instrument, by using, without the consent of the owner, an electronic payment instrument or the identification information that allows its use. The offence is punishable by two to seven years of imprisonment.
   Performing the previously described operations by means of the unauthorised use of any identification information or by using fictitious identification data is punishable by the same period of imprisonment.
   Furthermore, the same text of law stipulates that the unauthorised transmission to another person of any identification information, in order to perform any of the previously described operations, is punishable by one to five years of imprisonment; and
b. the offence of *Accepting transactions made fraudulently*, regulated by article 251 of the Romanian Criminal Code, which refers to the acceptance of a cash withdrawal operation, loading or unloading of an electronic money instrument or fund transfer instrument, knowing that it is carried out by using an electronic payment instrument that was counterfeited or used without the consent of the owner, is punishable by one to five years of imprisonment. The same sanction applies for accepting one of those operations while

knowing that it was made by the unauthorised use of any identification information, or by using false identification information.

1.2 Do any of the above-mentioned offences have extraterritorial application?

There are several principles which apply regarding the jurisdiction of Romanian judicial authorities in cases of criminal nature:

a. Romanian criminal law shall apply to all offences committed on the Romanian territory.
b. As a rule, if the act was committed outside of the Romanian territory by a Romanian citizen or a Romanian legal entity, with the act also being criminalised by the criminal law of the country where it was committed or if it was committed in a location that is not subject to any state's jurisdiction, then Romanian law shall apply as well.
   If, on the other hand, the offence was committed outside of the Romanian territory, by a Romanian citizen or a Romanian legal entity, without the act being criminalised by the criminal laws of the country where it was committed, then Romanian criminal law shall only apply if the sentencing regulated by Romanian law is life imprisonment or a term of imprisonment longer than 10 years.
c. Romanian criminal law applies to offences committed outside Romanian territory by a foreign citizen or a stateless person against the Romanian State, against a Romanian citizen or against a Romanian legal entity.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

No specific mitigating factors are regulated by Romanian law for the above-mentioned offences. However, we note that certain deeds represent criminal offences only if performed with the view to obtain a material benefit for oneself or for another, and if they have caused damage to a person (e.g. *Computer Fraud*, regulated by article 249 of the Romanian Criminal Code), while others (such as hacking) are sanctioned irrespective of the outcome intended to be obtained by the perpetrator (e.g. *Illegal access to a computer system*, regulated by the Romanian Criminal Code in article 360). If the purpose is obtaining data, the sanction is more severe.

As such, ethical hacking does not represent a cause for exemption of liability, but the sanction is lower than in regular hacking cases. Of course, this is only applicable if the perpetrator does not have the consent of the system owner in order to access the system, for testing purposes, for example.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The main law regarding cybersecurity in our jurisdiction is the Romanian Criminal Code, which contains most of the offences related to cybersecurity. Further applicable laws include:

a. Law no. 161/2003 on certain measures to ensure transparency in the exercise of public dignity, public office and in the business environment, the prevention and sanctioning of corruption, which in Title III contains provisions regarding the prevention of cybercrimes.
b. Law no. 362/2018 on ensuring a high common level of security of computer networks and systems.
c. Governmental Emergency Ordinance 98/2010 on the identification, designation and protection of critical infrastructures.
d. Decision no. 494/2011 issued by the Romanian Government on the establishment of the National Cyber Security Incident Response Centre CERT-RO.
e. Decision no. 271/2013 for the approval of the Cyber Security Strategy of Romania and of the Action Plan at national level regarding the implementation of the National Cyber Security System.
f. Methodology for 2019 to establish the significant disruptive effect of Incidents on the networks and computer systems of essential service operators, approved by Order no. 601/2019 issued by the Ministry of Communications and Information Society.
g. 2012 methodology for identifying national critical infrastructures in the information and communication technology sector.
h. The 2014 Norms on the protection of nuclear installations against cyber threats, approved by Order no. 181/2014 issued by the National Commission for the Control of Nuclear Activities.
i. Law no. 209/2019 on payment services and for amending some normative acts, which contains requirements regarding operational and security risks and authentication in Chapter V.
j. Regulation 2/2020 issued by the National Bank of Romania on security measures relating to operational and security risks and reporting requirements for payment services.
k. Regulation (EU) 679/2016 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
l. Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, which implements Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
m. Governmental Emergency Ordinance no. 111/2011 regarding electronic communications.
n. Decision no. 512/2013 issued by the National Authority for Administration and Regulation in Communications on the establishment of minimum security measures to be taken by providers of public electronic communications networks or electronic communications services to the public and the reporting of Incidents with a significant impact on the provision of electronic communications networks and services.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

General requirements for operators of essential services as well

as digital service providers are regulated by Law no. 362/2018 on ensuring a high common level of security of computer networks and systems (implementing into Romanian legislation the provisions of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union).

Law no. 362/2018 does not apply to national security or intelligence related institutions. A draft law on security and cyber defence of Romania was put forward by the Ministry of National Defence in 2018 for public debate, but the project has not been registered for the Parliament's vote yet.

Operators of essential services (defined as operators that handle a service in support of social and/or economic activities of the greatest importance) are required to monitor, detect, prevent and mitigate Incidents based on Technical Norms developed by the National Cyber Security Incident Response Centre.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Organisations are required to provide security when processing personal data, as such organisations should apply measures provided by article 32 of Regulation (EU) 679/2016. Depending on the circumstances, organisations should pseudonymise and encrypt personal data, ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services and have the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical Incident.

Furthermore, Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector imposes the obligation of ensuring the security of personal data and privacy to the provider of an electronic communication service, under the conditions of ensuring that personal data can only be accessed by authorised persons, of protecting personal data stored or transmitted against accidental or unlawful destruction, accidental loss or damage and against unlawful storage, processing, access or disclosure and of ensuring the implementation of the security policy developed by the provider with regard to the processing of personal data.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Law no. 362/2018 imposes obligations to report Incidents on operators of essential services.

Technical Norms detailing the process and circumstances of notifying the authority tasked with handling the notifications, identified by the Law as the National Cyber Security Incident Response Centre, are still in the process of being drafted.

Until Technical Norms are approved, provisions with a general nature in Law no. 362/2018 must be followed, thus:

a. a report must be filed if an Incident occurs (the Incident being defined as any event that has a real negative impact on the security of networks and information systems);
b. general reporting regarding Incidents must be done to the National Cyber Security Incident Response Centre, while Incidents with significant impact on the provision of electronic communications networks and services are to be notified to The National Authority for Management and Regulation in Communications (ANCOM), according to the Decision no. 512/2013 of the President of ANCOM. Security Incidents regarding breaches of personal data should also be notified to the National Authority for the Supervision of Personal Data Processing;
c. with regard to the general obligation to report to the National Cyber Security Incident Response Centre, the nature and scope of the reported information refer to the identification elements of the infrastructure and the operator or provider concerned, a description of the Incident, the period in which the Incident took place, the estimated impact of the Incident, preliminary measures adopted, the list of state authorities affected by the Incident, the potential geographical extent of the Incident and the data on potential cross-border effects of the Incident; and
d. regarding the publication of such information, Law no. 362/2018 states that the security and commercial interests of the essential service operator and the digital service provider, as well as the confidentiality of the information provided during any type of activity related to an Incident, are protected and confidential.

Under applicable laws regarding privacy, in the case of a data breach, the supervisory authority, in this case the National Supervisory Authority For Personal Data Processing, shall be notified by the controller within 72 hours of becoming aware of it (with the exception of the case in which the breach is unlikely to result in a risk to the rights and freedoms of natural persons). The processor shall notify the supervisory authority immediately when becoming aware of the personal data breach. The notification should: describe the nature of the breach and the data subjects affected; contain the contact data of the data protection officer; state the likely consequences; and describe the measures taken to mitigate the possible adverse effects.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

With respect to Incidents in the area of essential services, it is the National Cyber Security Incident Response Centre that notifies the public when the notification is necessary in order to prevent an Incident or to manage an ongoing Incident.

GDPR Regulation 679/2016, on the other hand, explicitly requires the communication to the data subject affected of any personal data breach, if it is likely to result in a high risk to the rights and freedoms of natural persons, and the notification should contain the contact data of the data protection officer, the likely consequences of the data breach and the measures taken to mitigate the possible adverse effects. The notification is not required if the data in question was encrypted or measures similar to encryption were already in place, if measures that

render null the risk of rights and freedoms of natural persons being affected were taken or if notifying the data subjects would involve disproportionate effort.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The following authorities are responsible:

- CERT-TO, National Cyber Security Incident Response Centre, located in Bucharest, with its headquarters at 8–10 Maressal Alexandru Averescu Boulevard, Sector 1, postal code 011455.
- The National Supervisory Authority For Personal Data Processing, with its headquarters at 28–30 G-ral Gheorghe Magheru Boulevard, Sector 1, postal code 010336, Bucharest, Romania, email anspdcp@dataprotection.ro.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Non-compliance with requirements imposed in the field of essential services constitutes an administrative offence, punishable by a fine of 3,000 lei to 50,000 lei.

Regulation (EU) 679/2016 provides that breach of the above-mentioned requirements may be subject to administrative fines up to 10 million EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Under Law no. 506/2004, the penalty for not complying with the requirements contained in this law is a fine from 5,000 lei to 100,000 lei and, for commercial companies with a turnover of over 5 million lei, a fine in the amount of up to 2% of turnover.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

With regard to the National Cyber Security Incident Response Centre, no enforcement actions have been made available.

In the data privacy area, the most severe sanctions in the past two years were applied for data breaches by banks, hotels and the national Romanian airline, Tarom.

More details on sanctions applied by the Data Protection Authority are available on the authority's official website.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There are no legal provisions against the use of beacons.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are no legal provisions against the use of honeypots.

The National Cyber Security Incident Response Centre announced in 2018 that it included honeypots in its own resources regarding the collection of data of security Incidents.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There are no legal provisions against the use of sinkholes.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

The interception of such electronic communications is subject to the provisions of Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and, as such, any interception is subject to the legal requirement of legitimate interest provided in letter (f) of paragraph 1. of article 6 present in the GDPR Regulation.

Thus, as the Data Protection Working Party states in its Opinion 2/2-17 on data processing at work, employers utilising these products and applications must consider the proportionality of the measures they are implementing and whether any additional actions can be taken to mitigate or reduce the scale and impact of the data processing. As an example of good practice, this consideration could be undertaken via a DPIA prior to the introduction of any monitoring technology. Secondly, employers must implement and communicate acceptable use policies alongside privacy policies, outlining the permissible use of the organisation's network and equipment, and strictly detailing the processing taking place.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Certain restrictions are imposed on the import and/or export of dual-use items.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Stricter security measures are imposed in the areas of payment services/banking or nuclear activities, just to name a few.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Specific requirements exist in relation to critical infrastructure and services.

Specific requirements have also been imposed in the area of payment services, including the financial and banking sector (through Law no. 209/2019 and Regulation issued by the National Bank of Romania no. 2/2020) and nuclear energy sector (through 2014 Norms on the protection of nuclear installations

against cyber threats, approved by Order no. 181/2014 issued by the National Commission for the Control of Nuclear Activities).

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Besides the GDPR office tasked with serving as the point of contact between the company and the National Supervisory Authority For Personal Data Processing, the general provisions present in Law no. 362/2018 stipulate in articles 10 and 12 that operators of essential services and digital service providers are to establish permanent pathways of contact with the National Cyber Security Incident Response Centre and to establish the persons responsible with the security. However, those do not fulfil the role of an officer.

The Director of the National Cyber Security Incident Response Centre has recently expressed the view that he supports the idea of a cyber protection officer in institutions and organisations.

To the extent failure to prevent, mitigate, manage or respond to an Incident amounts to a breach of responsibilities, whether work, management or general compliance, the directors and/or officers have liability.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

As stated above, companies are not required to designate a CISO. With regard to establishing a written Incident plan or policy, operators of essential services and digital service providers are required to have an established Incident response plan or policy. Cyber risks assessments are to be conducted via an audit, which is mandatory if it is at the request of the National Cyber Security Incident Response Centre, according to Law no. 362/2018. A different requirement is set for payment service providers according to Regulation 2/2020 issued by the Romanian National Bank, where it states the cyber risk assessments are to be conducted annually.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

We are not aware of any disclosure requirements other than those mentioned in section 2. However, to the extent that the Incident meets the materiality thresholds in the relevant legislation, it might be subject to public disclosure for the benefit of regulatory bodies, investors/shareholders for listed companies.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Regarding civil or private actions filed in relations to Incidents, unless specific legal provisions apply, they fall under the general provision of action in tort and must meet the requirements of the action in tort. As such, the existence of damages, the liaison between the deed that led to the Incident and the damages, as well as the liability of the person against whom the action was filed, must be proven.

Such action may be filed either against the person who committed a cybersecurity offence and/or against the entity responsible for the security system that was breached and is deemed legally or contractually liable.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

Except for sanctions imposed by public authorities for breaches of security requirements, or court decisions issued in criminal cases related to cybersecurity, no relevant public information is available in relation to actions that have been brought in Romania in relation to Incidents.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Under general provision of the civil law, action in tort is possible in relation to failure to prevent an Incident.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

There are no legal provisions prohibiting taking out insurance against Incidents. As such, products on the insurance market dedicated to such Incidents are available in our jurisdiction.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no legal provisions that impose limitations to insurance coverage against specific types of loss.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The broadest investigative powers are ascribed to the prosecutorial bodies, who can use the full extent of investigative prerogatives stipulated in the Romanian Criminal Procedure Code in order to prosecute any cybersecurity-related offences. Those investigatory powers range from performing arrests (which must be approved by a judge first) and seizures, to conducting special technical supervision (which must also be approved by a judge). We note that, until recently, specialised technical investigations were conducted with the help of Romanian intelligence agencies but, right now, such collaborations are severely contested, even in the realm of national security, due to recent decisions passed by the Romanian Constitutional Court.

The National Cyber Security Incident Response Centre has general investigatory powers relating to any cybersecurity Incident, under which it may request documents from the operator or provider, take possession of any other physical documentation, and request any other information it deems necessary. If an offence is deemed to have been committed, then judicial authorities will become involved and make use of law enforcement powers such as operating seizures or arrests.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No such requirements have been identified in the publicly available information.

Ana-Maria Baciu is a regulatory and intellectual property lawyer, assisting clients in various industries, including retail, FMCG, gambling, IT, e-commerce and life sciences, for more than 20 years.
Licensed as a European trademark and design attorney, Ana-Maria assists clients on the full spectrum of intellectual property aspects, both contentious and advisory.
In the gaming field, Ana-Maria advises industry stakeholders, operators, suppliers, as well as industry-relevant associations, on the whole range of regulatory and operational gaming aspects.

Simion & Baciu
11 Maior Alexandru Campeanu St, 1st floor, Unit 3
Bucharest 011235
Romania

Tel: +40 722 256 758
Email: ana-maria.baciu@simionbaciu.ro
URL: www.simionbaciu.ro

Cosmina Maria Simion is a regulatory, intellectual property and technology lawyer with more than 20 years of professional experience, with expertise in various industries, with an emphasis on the media and entertainment, online and gaming industries.
Prior to setting up Simion & Baciu, Cosmina was an intellectual property partner and co-head of the gambling, consumer and advertising practices at the largest and oldest law firm in Romania. She combines her strong advisory expertise acquired during her coordination roles in leading law firms with the specific approach built during her in-house role (at a US group, leader in the regional media sector).

Simion & Baciu
11 Maior Alexandru Campeanu St, 1st floor, Unit 3
Bucharest 011235
Romania

Tel: +40 744 581 569
Email: cosmina.simion@simionbaciu.ro
URL: www.simionbaciu.ro

Andrei Cosma is a fully qualified business lawyer with significant expertise in the regulatory field in multiple practice areas.
While heavily involved in the gambling industry from the very beginning of the reformation of the Romanian legal framework and well-versed in dealing with all legal aspects relating to the operation of gambling and gaming activities, particularly of a regulatory nature but also contentious, Andrei Cosma also specialises in new technologies, including blockchain, cryptocurrency, artificial intelligence and fintech.
His other areas of expertise include intellectual property, advertising and audiovisual as well as consumer protection. He has been involved in a wide variety of complex legal projects for prominent clients in the gaming field, foreign investors, media giants or high-profile retail operators.

Simion & Baciu
11 Maior Alexandru Campeanu St, 1st floor, Unit 3
Bucharest 011235
Romania

Tel: +40 745 035 680
Email: andrei.cosma@simionbaciu.ro
URL: www.simionbaciu.ro

Andrei Nicolae Dumbravă provides assistance on consumer protection matters as well as other legal and regulatory matters for clients active in the retail sector. He also handles various other civil, commercial and gaming law matters and represents clients in front of the relevant public Romanian authorities.
Additionally, he acts as an IT assistant at ELSA (European Law Students' Association) International, an NGO of over 50,000 members, covering more than 375 law faculties.

Simion & Baciu
1 Maior Alexandru Campeanu St, 1st floor, Unit 3
Bucharest 011235
Romania

Tel: +40 740 092 682
Email: andrei.dumbrava@simionbaciu.ro
URL: www.simionbaciu.ro

Simion & Baciu unites a team of seasoned attorneys, with the drive and passion to deliver the best and most helpful results for its clients. With more than 20 years of experience, spanning over several areas of law, our team offers a fresh, business-oriented approach and successfully assists clients time and again.
With the technology sector continuing to evolve and become ever more important in business and in our lives generally, we work with technology companies, entrepreneurs and investors alike to help them stay ahead of the curve in terms of innovation, regulation and market practice.
Our clients turn to us for technical legal advice, with innovation and development in mind. We work on digital content technology, screen-sharing technology, user-generated creation and licensing.

We have experienced both sides of the negotiating table and are fully acquainted with all the issues that can drive each deal to a successful conclusion.

www.simionbaciu.ro

SIMION & BACIU

Saudi Arabia


Saeed Algarni


Mohammed Ashbah

Alburhan

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes, hacking constitutes an offence. According to the Anti-Cyber Crime Law ("ACCL"), penalties vary according to four cases:

1. According to articles 3-2 and 3-3 of the ACCL, where there is: unlawful access to computers with the intention to threaten or blackmail any person to compel him to take or refrain from taking an action, be it lawful or unlawful; or unlawful access to a website or hacking of a website with the intention of changing its design, destroying or modifying it, or occupying its URL, then the perpetrator shall be subject to imprisonment for a period not exceeding one year, a fine not exceeding SAR 500,000, or both.
2. According to article 2-4 of the ACCL, where a perpetrator illegally accesses bank or credit data, or data pertaining to ownership of securities in order to obtain data, information, funds or services offered, they shall be subject to imprisonment for a period not exceeding three years, a fine not exceeding SAR 2 million or both.
3. According to article 3-5 of the ACCL, where there is unlawful access to computers with the intention to delete, erase, destroy, leak, damage, alter or redistribute private data, the perpetrator shall be subject to imprisonment for a period not exceeding four years, a fine not exceeding SAR 3 million, or both.
4. According to article 2-7 of the ACCL, where there is unlawful access to a website or an information system either directly or through the information network or any computer, with the intent to obtain data jeopardising the internal or external security of the state or its national economy ("CNIs"), the perpetrator shall be subject to imprisonment for a period not exceeding 10 years, a fine not exceeding SAR 5 million, or both.

Denial-of-service attacks
Yes, this constitutes an offence. According to article 3-5 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding four years, a fine not exceeding SAR 3 million, or both.

Phishing
Yes, phishing constitutes an offence. According to article 1-4 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding three years, a fine not exceeding SAR 2 million, or both.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes, this constitutes an offence. According to articles 1-5 and 2-5 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding four years, a fine not exceeding SAR 3 million, or both.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Yes, this constitutes an offence according to article 1-9 of the Arab Convention for Cyber Crimes and the ACCL.

Possession or use of hardware, software or other tools used to commit cybercrime
Yes, this constitutes an offence according to article 2-9 of the ACCL.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes, this constitutes an offence. According to article 1-4 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding three years, a fine not exceeding SAR 2 million, or both.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Saudi law criminalises any attack in any way, and the conviction varies according to the relevant regulations. It emphasises that, in accordance with the spirit of Saudi legislation, the criminal penalty for the offender arises because of his or her act of harm, whatever the legal basis.

As for workers, a breach of confidence subjects him to two routes of penalty. There is an "internal" path (inside the facility), where, if the worker is still a current employee, the facility shall have the right to either: dismiss him without an end-of-service bonus or compensation for the penalty clause; or notify him if the accusation is proven against him after the establishment conducts an internal investigation with him and allows him to state his justifications in accordance with article 80 of the Labour Law. In the case of a "foreign" path, where there is a criminal offence, the necessary measures against him are taken, as with any non-worker.

As for copyright infringement, this is condemned in article 21 the Copyright Law. Article 22 defines five penalties for violations, in addition to the right of the judicial authority to punish defamation if it deems it necessary. The penalties must not exceed imprisonment for a period of six months, and a fine of SAR 250,000. More than one penalty can be applied and the maximum limits are doubled in case of repetition.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Yes, this constitutes an offence. The perpetrator shall be subject to the same penalty prescribed for the crime itself. However, the penalty may be reduced if the perpetrator submits evidence of good faith to the judiciary based on article 13 of the ACCL.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

1. Yes, this constitutes an offence. According to article 5 of the ACCL, the perpetrator shall be subject to imprisonment for a period not exceeding four years and a fine not exceeding SAR 3 million, or both.
2. If a website, information system or computer device obtains data affecting the national or external security of the state, or the national economy, then, according to article 7-2 of the ACCL, the perpetrator shall be punished with imprisonment for a period not exceeding 10 years, a fine not exceeding SAR 5 million, or both.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The Kingdom of Saudi Arabia has jurisdiction over any obligation (negative or positive) that arises, agreed upon or executed inside the Kingdom of Saudi Arabia, and it is exclusively competent with regard to any violations affecting CNIs. The prosecution of criminals under international agreements and bilateral treaties concluded by Saudi Arabia is also a case in point.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Yes, according to article 11 of the ACCL, the court has the right to exempt penalties for the offender who informs the authorities, with three conditions: 1) they must inform the authorities before the damage occurs; 2) they must inform the authorities before the authorities are aware of the Incident in general; and 3) where there are multiple perpetrators, they must inform all other perpetrators.

According to articles 9 and 10 of the ACCL, the penalty does not exceed half of the upper limit if the crime does not occur.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

1. ACCL.
2. Electronic Transaction Law.
3. Telecommunication Act ("TA").
4. Electronic Commerce Law.
5. CITC Ordinance.
6. Criminal Procedure Law.
7. Essential Cybersecurity Controls ("ECC").
8. Critical System Cybersecurity Controls ("CSCC").
9. Copyright Law.
10. ACCC.
11. Rules Governing Insurance Aggregation Activities of Cooperative Insurance Companies Control Law ("RGIAA").
12. Penal Law on Dissemination and Disclosure of Classified Information and Documents.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes, under the Applicable Law, the National Cybersecurity Authority ("NCE") issues controls and standards, and has issued the first edition of the ECC which must apply to all government agencies, all subsidiaries, and to private sector establishments that own, operate or host CNIs.

NCE then issued the first version of the CSCC, which is considered a complement to the ECC, except in systems or networks where there has been: disruption or illegal change to the way in which they operate; or unauthorised access to them or to the data and information that they store or process, negatively affecting: the availability of services; the work of the public entity; or the economy, finance or security, or having a social impact at a national level. This was defined in seven precise, detailed standards.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Applicable Law, if the facility owns, operates, or hosts CNIs, it must follow all the controls issued by the NCE (as per question 2.2 above), and the controls regarding cooperative insurance establishments are increased according to article 2-5 of the RGIAA. The RGIAA is required to develop a contingency plan that includes the procedures that should be taken in the event of failure of one or more elements of the automated system of the electronic platform. The plan should include corrective measures to ensure the continuity of work and the mechanism of reporting to the establishment.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Saudi law does not compel facilities to report the attacks, except if the facility owns, hosts or runs CNIs. Public Prosecution ("PP") is the authority to which it requires information to be reported, according to article 15 of the ACCL. PP makes decisions based on the requirements of each criminal case.

It is worth mentioning that there are many governmental institutions responsible for all aspects of cybersecurity: the Ministry of Communications and Information Technology; the CITC; the National Cybersecurity Authority; the Saudi Data & AI Authority ("SDAIA"); and the Saudi Federation for Cybersecurity, Programming and Drones.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Saudi law does not stipulate that facilities are required to do so, unless the establishment, in its contracts, has committed itself to do so under the terms of protection and privacy with customers or suppliers. It is, however, not exempt from legal liability, except from reporting the Incident. Any entity must also comply if the authorities request disclosure and report accordingly.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Cases related to crimes shall be reported to the police, whilst PP is responsible for the investigation, according to article 15 of the ACCL.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

There are no such penalties in Saudi law.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

There are no specific examples of this.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There is no law prohibiting the facility from using beacons, unless it owns, operates or hosts CNIs, in which case it must follow the regulations issued by NCE.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There is no law prohibiting the facility from using honeypots, unless it owns, operates or hosts CNIs, in which case it must follow the regulations issued by NCE.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There is no law prohibiting the facility from using sinkholes, unless it owns, operates or hosts CNIs, in which case it must follow aim 2-5 and its controls in the ECC.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

There is no law prohibiting the facility from monitoring or intercepting electronic communication, unless it owns, operates or hosts CNIs, in which case it must follow aim 12-2 and its controls of the ECC.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There is no law prohibiting the facility from restricting the import or export of such technology. The importer must fulfil the detailed requirements of Saudi customs and, if he wants to trade them, obtain the required licences from the Saudi Standards, Metrology and Quality Organisation ("SASO"), without prejudice to property rights and other requirements of laws.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Saudi law does not place many restrictions on the movement of the market to its internal organisation unless the facility wants to be a listed company and the practice in the market differs

from one industry to another, as some industries depend on high secrecy protected by written contracts, rather than the law generally.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

It applies to all government agencies and its subsidiaries, and all establishments that own, operate or host CNIs in accordance with the regulations issued by NCE.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Yes, if the failure of the company is clearly related to the accident and the company's manager did not take the measures in the Incident, according to article 32 of the Companies Law, bearing in mind that this is reserved for companies (other than individual institutions) exempt from a large number of obligations. There is no specific law regarding it.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Saudi law does not stipulate that facilities would be obligated to do so, except in the following circumstances:

With non-individual companies, the responsibility entrusted to the manager increases to achieving all that is necessary for the benefit of the company. This includes appointing a manager, establishing information and setting a written policy to respond to Incidents if this is necessary, and any failure to do so is considered a violation of the law that may, if an Incident were to happen, lead to accountability and liability according to article 32 of the Companies Law.

With establishments that own, operate or host CNIs, they must apply the controls issued by the NCE, which made the workforce an integral part of CNIs, and for which the Saudi Framework for Cybersecurity Cadres ("SCyWF") was issued in detail. They are also required to develop a written Incident response policy and conduct periodic assessments of electronic risks and penetration tests under aim 2 and its controls from the ECC.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no specific laws related to this disclosure; the Companies Law holds the executive management responsible for reporting the necessary reports that enable the Board of Directors to know the company's position. The Capital Market Authority ("CMA") also stipulates, in its regulations and requirements regarding listed companies, the necessity of financial disclosure of risks.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Regarding the conviction of the perpetrator who caused any violation of cybersecurity, the Criminal Court is the judicial authority responsible for judging the perpetrator by the legally determined penalty against him and compensation for the damage caused by what he did.

As for the conviction of the company's manager, the judiciary seeks the help of experts who are assigned the task of investigating and searching for the extent of the failure of the company who took the necessary measures, clearly and without ambiguity. The Saudi law holds managers accountable and it is a case of the principle of trust. The one who says the opposite is required to provide evidence of that, unless his employment contract or the company's articles of incorporation obligate the manager to take the preventive measures regarding the protection of cybersecurity.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There are no Incidents that can be disclosed.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The answer to this question does not differ from the answers discussed in sections 1–6, for the harm caused by any person to another makes it legally justified to argue against him, whether it is real or electronic, and whether it is positive or negative (such as negligence).

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Saudi law has no stipulations relating to insurance against Incidents. It is not known whether there are companies in this field, and this field may be a good legal and investment challenge soon. It should be noted that the authority concerned with organising all insurance affairs is the Saudi Arabian Monetary Authority ("SAMA").

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no such limitations. Accordingly, insurance companies in Saudi law may exclude or include clauses in their documents, after approval of the SAMA.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The relevant authorities are mainly the police, as well as PP and the CITC, according to articles 14 and 15 of ACCL, under the Applicable Law. As for terrorist cybercrime, article 7 of the ACCL stipulates a specific penalty, and the Law on Combating Terrorism Crimes and Financing stipulates that the competent court in terrorism cases is the "Specialised Criminal Court". Many security agencies also work together in fighting terrorism, including the Presidency of State Security in all its sectors.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There is no legal obligation for the facility to do so unless it owns, operates or hosts CNIs, in which case it must do so under article 56-5 of the TA.

Acknowledgment

The authors would like to thank Aljawhara A. Alleheidan for her active participation and valuable contribution in this chapter.

Saeed Algarni is a Managing Partner of Alburhan law firm, specialising in Commercial, Intellectual Property, Data Protection, and Information Technology Law. Saeed manages large legal projects for companies and governmental entities and advises on complex commercial matters for a range of local and international clients.

Alburhan
7013 Takhassusi St.
Al Rahmaniyah Dist.
RIYADH 12341-3507
Saudi Arabia

Tel: +966 555 355 950
Email: saeed@alburhan.sa
URL: www.alburhan.sa

Mohammed Ashbah is a Legal Consultant at Alburhan law firm. Boasting top academic work and nine years' experience working in Riyadh, Ashbah practises Administrative, Franchise, Labour, Cybersecurity Law and has been recommended leading in those fields as well as drafting regulations for regulatory authorities

Alburhan
7013 Takhassusi St.
Al Rahmaniyah Dist.
RIYADH 12341-3507
Saudi Arabia

Tel: +966 55 210 2207
Email: mhmdashbh@alburhan.sa
URL: www.alburhan.sa

Muhanned Alqaidy practises at Alburhan, focusing primarily on corporate, labour law, regulatory, and administrative law matters. His practice has included a broad and varied representation of public and private corporations and other entities in a variety of industries throughout Saudi Arabia.

Alburhan
7013 Takhassusi St.
Al Rahmaniyah Dist.
RIYADH 12341-3507
Saudi Arabia

Tel: +966 548 821 310
Email: muhanad@alburhan.sa
URL: www.alburhan.sa

Alburhan is a Saudi law firm that specialises in a broad range of practice areas. It is determined to lead the Middle East region at a time of significant change in the legal industry, by helping clients overcome the challenges of competing in the global economy through a new type of thinking and a different mindset. Alburhan has advised on some of the most complex legal issues, and provides its clients with professional legal expertise, quality strategic advice and maintains a superior level of client service.

www.alburhan.sa

Singapore


Lim Chong Kin


David N. Alfred


Albert Pichlmaier

Drew & Napier LLC

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. Under section 3(1) of the Computer Misuse Act (Cap. 50A) ("**CMA**"), it is an offence for any person to knowingly cause a computer to perform any function for the purpose of securing access without authority, to any program or data held in any computer. Upon conviction, an offender shall be liable for: a fine of up to $5,000; imprisonment for a term of up to two years; or both for the first offence.

In *Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin* [1999] 3 SLR(R) 653, the accused was found to have, *inter alia*, exploited certain vulnerabilities to hack into some of the servers of the victim, in order to gain unauthorised access to the computer files contained on the victim's server. The accused was sentenced to two months' imprisonment for the charge under section 3(1) of the CMA.

In *Tan Chye Guan Charles v Public Prosecutor* [2009] 4 SLR(R) 5, the accused was found to have accessed files on a laptop without authorisation, by copying them onto his thumbdrive when the laptop's owner left his laptop unattended to answer a phone call. The accused was sentenced to three weeks' imprisonment and fined $5,000.

Denial-of-service attacks

Yes. A denial-of-service ("**DOS**") attack is a cyber-attack meant to shut down a machine or network, thus making it inaccessible to its intended users.

Under section 7(1) of the CMA, any person who, knowingly and without authority or lawful excuse (a) interferes with, or interrupts or obstructs the lawful use of, a computer, or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer, shall be guilty of an offence. Upon conviction, an offender shall be liable for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for the first offence.

There have not been any published judgments by the Singapore courts involving an offence involving a DOS attack.

Phishing

Possibly. Whilst phishing itself may not be an offence, a number of provisions criminalise actions which could include phishing.

Under section 3 of the CMA, it is an offence for any person to cause a computer to perform any function for the purpose of securing access without authority to any data held in any computer. It is possible, depending on the exact circumstances, for this to include phishing. An offender who is convicted under this section shall be liable for: a fine of up to $5,000; imprisonment for a term of up to two years; or both for a first offence.

In *Public Prosecutor v Lim Yi Jie* [2019] SGDC 128, the Court found the accused to have facilitated a phishing scam involving the use of a phishing website, causing a victim to divulge her 2-factor-authentication and time-sensitive PIN number to the accused, as the victim assumed that the phishing website was an official bank website. Although the accused was not responsible for the execution of the phishing scam (which, in the Court's view, could be an offence under section 3(1) of the CMA, then named as the Computer Misuse and Cybersecurity Act), the accused had attempted to cash two cheques that were the criminal proceeds of the phishing scam. The accused was thus charged and convicted of an offence under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A).

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. Under section 5 of the CMA, it is an offence for any person who commits any act which he knows will cause an unauthorised modification of the contents of any computer. As the infection of IT systems with malware would cause an unauthorised modification of the contents of the infected computer, this could be an offence under section 5 of the CMA.

Upon conviction, the offender shall be liable for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

There are presently no published judgments by the Singapore courts involving an offence under the CMA for the infection of IT systems with malware.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Yes. Under section 8B(1)(b) of the CMA, a person shall be guilty of an offence if that person makes, supplies, offers to supply or makes available, by any means, any of the following items, intending it to be used to commit or facilitate the commission of an offence under section 3, 4, 5, 6 or 7 of the CMA:

(a) any device, including a computer program, that is primarily designed, adapted, or capable of being used for the purpose of committing an offence under section 3, 4, 5, 6 or 7; and
(b) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

A person found guilty of this offence shall be liable on conviction for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

There are presently no published judgments by the Singapore courts involving the distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime.

Possession or use of hardware, software or other tools used to commit cybercrime

Yes. Under section 8B(1)(a) of the CMA, it is an offence if a person obtains or retains certain items (as detailed in the following paragraph) and (i) intends to use it to commit or facilitate the commission of an offence under section 3, 4, 5, 6 or 7 of the CMA, or (ii) does so with a view to it being supplied or made available, by any means, for use in committing or in facilitating the commission of any of those offences.

The items in question are:

(a) any device, including a computer program, that is primarily designed, adapted or is capable of being used for the purpose of committing an offence under section 3, 4, 5, 6 or 7; and
(b) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

A person found guilty of this offence shall be liable on conviction for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

There are presently no published judgments by the Singapore courts involving the possession or use of hardware, software or other tools used to commit cybercrime.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes. Under section 4 of the CMA, it is an offence for a person to cause a computer to perform any function for the purposes of securing access to any program or data held in any computer, with the intent to commit a number of offences, including certain offences involving fraud or dishonesty. A person convicted of such an offence is liable for: a fine not exceeding $50,000; imprisonment for a term not exceeding 10 years; or both.

Penalties for identity theft and identity fraud are also set out in the Penal Code (Cap. 224) ("**Penal Code**"). Under section 419 read with section 416 of the Penal Code, a person who cheats by personation (i.e., if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is), is guilty of an offence and, upon conviction, liable for: imprisonment for a term of up to five years; a fine; or both. Whilst this offence is of general application, it could also extend to the cyber context.

Separately, section 170 of the Penal Code criminalises the offence of personating a public servant. Any person who is convicted of this offence shall be liable upon conviction for: imprisonment for a term which may extend to two years; a fine; or both.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes. Under section 8A(1) of the CMA, it is an offence for a person who, knowing or having reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of section 3, 4, 5 or 6 of the CMA:

(a) obtains or retains the personal information; or
(b) supplies, offers to supply, transmits or makes available, by any means the personal information.

Upon conviction, an offender may be sentenced to: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

Additionally, it is also an offence under section 136(1) of the Copyright Act (Cap. 63) ("**Copyright Act**") for a person who (a) makes for sale or hire, (b) sells or lets for hire, or by way of trade offers or exposes for sale or hire, or (c) by way of trade exhibits in public, any article which he knows or ought reasonably to know to be an infringing copy of the work. Upon conviction, an offender may be liable for a fine of up to: $10,000 for the article or for each article in respect of which the offence was committed, or $100,000 (whichever is the lower); imprisonment for a term of up to five years; or both.

In addition, it is also an offence under section 136(3) of the Copyright Act for any person who, at the time when copyright subsists in a work, distributes, for either (a) the purposes of trade, or (b) other purposes (but to such an extent as to affect prejudicially the owner of the copyright), articles which he knows to be infringing copies of the work. Upon conviction, an offender may be liable for: a fine of up to $50,000; imprisonment for a term of up to three years; or both.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Yes. Under section 3(1) of the CMA, any person who knowingly causes a computer to perform any function for the purpose of securing access without authority, to any program or data held in any computer, shall be guilty of an offence. Upon the first conviction, the offender shall be liable for a fine of up to $5,000; imprisonment for a term of up to two years; or both.

Given that penetration testing would necessarily involve gaining access to a computer system, it is possible that such unsolicited penetration testing (i.e., penetration testing done without any authorisation from the owner of the computer system) would constitute an offence under section 3(1) of the CMA.

Even if the penetration testing is unsuccessful, such an act may still be an offence. Under section 10 of the CMA, any person who attempts to commit an offence or does any act preparatory to an offence under the CMA shall be guilty of that offence and shall be liable on conviction for the punishment provided for the offence.

In *Public Prosecutor v James Raj s/o Arokiasamy* [2015] SGDC 36, the accused pleaded guilty and was convicted of the unauthorised hacking of a number of websites, including the websites of a well-known church in Singapore, the blog of a journalist, and a political party's website, as well as the unsolicited scanning and penetration testing of various government servers. The accused was sentenced to six months' imprisonment for the charges pertaining to the unsolicited scanning and penetration testing of various government servers under section 3(1) read with section 10 of the CMA.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Yes. The offences listed under Part II (i.e., sections 3 to 10) of the CMA are generally broad enough to address activities that adversely affect or threaten the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

For example, unauthorised modification of computer material (i.e., adversely affecting or threatening the integrity of computer material) is an offence under section 5 of the CMA, and unauthorised obstruction of use of computer (i.e., adversely affecting or threatening the availability of a computer system) is an offence under section 7 of the CMA.

Additionally, under section 10 of the CMA, abetments and attempts of the offences under Part II of the CMA are also treated as offences, and a person who abets or attempts to do any act preparatory to or in furtherance of the commission of any offence shall be guilty of that offence.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, the above offences have extraterritorial application.

In respect of the CMA, section 11 of the CMA provides that the provisions of the CMA shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore. Where an offence is committed outside Singapore, the offender may be dealt with as if the offence had been committed within Singapore, if:

(a) for the offence in question, the accused was in Singapore at the material time;
(b) for the offence in question (being one under section 3, 4, 5, 6, 7 or 8 of the CMA), the computer, program or data was in Singapore at the material time; or
(c) the offence causes, or creates a significant risk of, serious harm in Singapore.

Thus, where a person commits an offence under the CMA from a location outside Singapore, the person in question may nonetheless be prosecuted under the CMA as if the person had committed the offence within Singapore.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Not necessarily. The offences under the CMA do not set out any general exceptions or factors that must be considered by a court in mitigation.

Nonetheless, there are factors that may be taken into account by the court in determining the appropriate sentence. For example, the fact that an offender had no intention to make a financial gain through his actions, and did not, in fact, make any financial gain, may have some impact in mitigating the length of a sentence, or the quantum of a fine.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

There are a number of applicable laws in Singapore relating to cybersecurity. Some of these laws are:

Cybersecurity Act 2018 ("Cybersecurity Act")

The Cybersecurity Act sets out a framework for the monitoring of Critical Information Infrastructures ("**CIIs**"), including imposing obligations on owners of CIIs to report cybersecurity incidents, and provides for the appointment of a Commissioner of Cybersecurity to, amongst others, oversee and promote the cybersecurity of computers and computer systems in Singapore.

In addition, the Commissioner of Cybersecurity is also empowered under the Cybersecurity Act to issue or approve one or more codes of practice of standards of performance for the regulation of owners of CIIs with respect to measures to be taken by them to ensure the cybersecurity of the CII. However, these codes of practice are meant for guidance, and do not have legislative effect.

As of the time of writing, the Commissioner of Cybersecurity has issued one such code: the Cybersecurity Code of Practice for Critical Information Infrastructure.

Personal Data Protection Act 2012 ("PDPA")

The PDPA imposes a number of data protection obligations on organisations, in respect of personal data. Importantly, section 24 of the PDPA requires organisations to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Computer Misuse Act (Cap. 50A)

As mentioned above, the CMA covers a number of cyber offences, including, but not limited to, offences such as the exploiting of computer vulnerabilities to gain unauthorised access to a computer system (section 3 of the CMA).

Copyright Act (Cap. 63)

The Copyright Act criminalises copyright infringement. Specifically, it is an offence for a person to, at a time when copyright subsists in a work, (a) make for sale or hire, (b) sell or let for hire, or, by way of trade, offer or expose for sale or hire, or (c) by way of trade, exhibit in public, any article which he knows, or ought reasonably to know, to be an infringing copy of the work.

Strategic Goods (Control) Act (Cap. 300)

The Strategic Goods (Control) Act sets out provisions relating to the transfer and brokering of strategic goods and strategic goods technology. The list of items that have been prescribed by the Minister as strategic goods and strategic goods technology includes "information security" systems, equipment and components (i.e., systems, equipment and components designed or modified to use "cryptography for data confidentiality" having "in excess of 56 bits of symmetric key length, or equivalent").

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes. Under the Cybersecurity Act, the Commissioner of Cybersecurity may designate a computer or computer system as a CII under the Cybersecurity Act, if he is satisfied that (a) the computer or computer system is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore, and (b) the computer or computer system is located wholly or partly in Singapore.

The list of essential services are set out in the First Schedule to the Cybersecurity Act, which consists of services in the following industries: energy; info-communications; water; healthcare; banking and finance; security and emergency services; aviation; land transport; maritime; services relating to the functioning of Government; and media.

The obligations placed on owners of CIIs include having to report cybersecurity incidents to the Commissioner of Cybersecurity (section 14 of the Cybersecurity Act), conducting regular cybersecurity audits and risk assessments of CII (section 15 of the Cybersecurity Act) and furnishing information on, amongst others, the design, configuration and security of the CII to the Commissioner of Cybersecurity upon the Commissioner of Cybersecurity's written notice to do so (section 10 of the Cybersecurity Act).

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Under section 14(2) of the Cybersecurity Act, the owner of a CII must establish mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the CII, as set out in any applicable code of practice.

Separately, the Protection Obligation under the PDPA requires organisations to put in place reasonable security measures to protect personal data under its possession and/or control. However, the PDPA does not specify the specific measures that organisations should take.

In its Guide to Managing Data Breaches 2.0 (the "**Data Breach Guide**"), the Personal Data Protection Commission ("**PDPC**") sets out what organisations should do to prevent data breaches. First, it states that organisations should implement monitoring measures and tools to provide early detection and warning to organisations. Examples include:

(a) monitoring of inbound and outbound traffic for websites and databases for abnormal network activities;
(b) usage of real-time intrusion detection software designed to detect unauthorised user activities, attacks, and network compromises; and
(c) usage of security cameras for monitoring of internal and external perimeters of secure areas such as data centres and server rooms.

The Data Breach Guide also encourages organisations to put in place a data breach management plan, which would include the following information:

(a) a clear explanation of what constitutes a data breach (both suspected and confirmed);
(b) how to report a data breach internally;
(c) how to respond to a data breach; and
(d) responsibilities of the data breach management team.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. In respect of data protection, the PDPC encourages organisations to report information related to Incidents or potential Incidents. In respect of the Cybersecurity Act, owners of CIIs are statutorily obligated to report Incidents.

Personal Data Protection Act 2012

At present, the PDPA does not require organisations to make any reports to the PDPC.

However, in the Data Breach Guide, the PDPC encourages organisations to notify the PDPC and/or affected individuals of a data breach that is: (a) likely to result in significant harm or impact to the individuals to whom the information relates; or (b) of a significant scale (i.e., involves personal data of 500 or more individuals). The guide also states that organisations should inform the relevant parties as soon as practicable and, in the case of the PDPC, no later than 72 hours after assessing that the data breach has met one of the requirements for notification to the PDPC.

The organisation should inform the PDPC of the following:

- the extent of the data breach;
- the type(s) and volume of personal data involved;
- the cause or suspected cause of the breach;
- whether the breach has been rectified;
- the measures and processes that the organisation had put in place at the time of the breach;
- information on whether affected individuals of the data breach were notified and if not, when the organisation intends to do so; and
- the contact details of person(s) whom the PDPC could contact for further information or clarification.

In general, there are no express defences or exemptions which organisations may rely on to prevent publication of that information. The PDPC is empowered, under regulations 16 to 20 of the Personal Data Protection (Enforcement) Regulations 2014, to publish a decision or direction ("**Decision**"), or a summary of the decision or direction ("**Summary**"). However, where a Decision contains personal data or information that is treated as confidential under the PDPA, the PDPC may either redact such data and information from the published Decision or publish a Summary that excludes such data and information. Persons providing information to PDPC may identify any such information which is confidential and provide a written statement giving reasons why the information is confidential (section 59 (3) and (4) of the PDPA). In considering whether to publish a Decision or Summary, the PDPC has stated that it will generally publish a Decision relating to an organisation that is found to have contravened its obligations under the PDPA. Amongst other reasons, this is for transparency, and so that other organisations may take note of the manner in which the Commission has applied the PDPA in specific cases and take preventive measures to avoid similar occurrences.

Additionally, as of this time of writing, the PDPC has published the draft Personal Data Protection (Amendment) Bill 2020, which will introduce, *inter alia*, a mandatory breach notification obligation. This proposed mandatory breach notification obligation is in line with the existing guidelines under the Data Breach Guide (i.e., notification should be made if it is likely to result in significant harm or is of a significant scale). As of the time of writing, the Personal Data Protection (Amendment) Bill 2020 has yet to be passed.

Cybersecurity Act

Under section 14(1) of the Cybersecurity Act, the owner of a CII must notify the Commissioner of Cybersecurity of the occurrence of any of the following:

(a) a prescribed cybersecurity incident in respect of the critical information infrastructure;
(b) a prescribed cybersecurity incident in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with the critical information infrastructure; and/or
(c) any other type of cybersecurity incident in respect of the critical information infrastructure that the Commissioner has specified by written direction to the owner.

In particular, the owner of the CII is required to notify the Commissioner of Cybersecurity, within two hours after a cybersecurity incident, of the following:

(i) the critical information infrastructure affected;
(ii) the name and contact number of the owner of the critical information infrastructure;
(iii) the nature of the cybersecurity incident, whether it was in respect of the critical information infrastructure or an interconnected computer or computer system, and when and how it occurred;
(iv) the resulting effect that has been observed, including how the critical information infrastructure or any interconnected computer or computer system has been affected; and
(v) the name, designation, organisation and contact number of the individual submitting the notification.

The owner of the CII is then required to provide the following supplementary details within 14 days via the Cyber Security Agency of Singapore's website:

(i) the cause of the cybersecurity incident;
(ii) its impact on the critical information infrastructure, or any interconnected computer or computer system; and
(iii) what remedial measures have been taken.

The Cybersecurity Act also generally empowers the Commissioner of Cybersecurity to investigate and prevent cybersecurity incidents (not limited to those involving CIIs), including but not limited to requiring any person to answer any question or to produce any physical or electronic record that is in possession of that person to the incident response officer, which the incident response officer considers to be related to any matter relevant to the investigation.

Under section 43 of the Cybersecurity Act, every person must preserve, and aid in preserving, *inter alia*, all matters relating to a computer or computer system of any person that may have come to the Commissioner of Cybersecurity's and/or incident response officer's knowledge in the performance of his or her functions or the discharge of his or her duties under the Act. For this reason (amongst others), any information furnished would not likely be published.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

As stated above, the PDPC, in its Data Breach Guide, encourages organisations to notify the PDPC and/or affected individuals of a data breach that is: (a) likely to result in significant harm or impact to the individuals to whom the information relates; or (b) of a significant scale (involves personal data of 500 or more individuals). In respect of the affected individuals, the guide states that organisations should inform these affected individuals as soon as practicable.

The information that should be given to the affected individuals include:

- how and when the data breach occurred;
- types of personal data involved in the data breach;
- what the organisation has done or will be doing in response to the risks brought about by the data breach;
- specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused;
- contact details and how affected individuals can reach the organisation for further information or assistance (e.g., helpline numbers, e-mail addresses or websites); and/or
- where applicable, what type of harm/impact the individual may suffer from the compromised data.

In addition, the PDPC has published the draft Personal Data Protection (Amendment) Bill 2020, which will introduce, *inter alia*, a mandatory breach notification obligation that would require organisations to inform affected individuals of a breach. This has yet to take effect.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

There are different regulators responsible for enforcing the above requirements.

The PDPC, which is a division within the Infocomm Media Development Authority ("**IMDA**"), is the regulator responsible for enforcing the provisions under the PDPA.

The Commissioner of Cybersecurity, working together with his team at the Cyber Security Agency of Singapore ("**CSA**"), is responsible for the enforcement of the provisions under the Cybersecurity Act.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

There are a range of potential penalties, depending on the exact requirements that have not been complied with.

Under the PDPA, the PDPC is empowered to issue directions to ensure that organisations comply with the PDPA, including imposing a financial penalty of up to $1 million. It should be noted that, with the upcoming changes in the Personal Data Protection (Amendment) Bill 2020, the financial penalty that may be imposed will be increased to the higher of (a) 10% of an organisation's annual turnover, or (b) $1 million. However, as of the time of writing, this has yet to be passed.

Under the Cybersecurity Act, the failure of a CII owner to report a cybersecurity incident in respect of a CII, without reasonable excuse, is an offence and the owner shall be liable on conviction to a fine of up to $100,000; imprisonment for a term of up to two years; or both.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In respect of non-compliance with the PDPA, the PDPC has published a number of its enforcement decisions.

One of the more notable enforcement cases is *Re Singapore Health Services Pte. Ltd. & Ors.* [2019] SGPDPC 3. In that case, the PDPC took enforcement action against (1) Singapore Health Services Pte. Ltd. ("**SingHealth**"), and (2) Integrated Health information Systems Pte. Ltd. ("**IHiS**"), for failing to put in place reasonable security measures to protect personal data under its possession and control, leading to a data breach wherein the medical records of 1.5 million patients were leaked. The PDPC imposed a financial penalty of $250,000 on SingHealth and $750,000 on IHiS.

There are no published enforcement actions that have been taken against owners of CIIs under the Cybersecurity Act.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

There are likely to be no restrictions on the usage of beacons for protection purposes, *unless* the data collected by such beacons constitutes personal data under the PDPA.

Under the Consent Obligation of the PDPA, organisations are required to obtain consent (or deemed consent) from individuals before the collection, use and disclosure of that individual's personal data. Thus, beacons would not be permissible if they collect personal data without the consent (or deemed consent) of the individuals in question, unless an exception to the Consent Obligation applies under the PDPA.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

There are likely to be no restrictions on the usage of honeypots for the purpose of protection of IT systems. Neither the Cybersecurity Act nor the PDPA restrict the usage of honeypots as a way of protecting IT systems.

In fact, the relevant regulators have addressed the use of honeypots, and do not appear to object to their usage. In an article published by the CSA in 2019, it explained honeypots and their role in cyber defence. Additionally, the PDPC's Guide to Securing Personal Data in Electronic Medium encourages the use of "*defences that may be used to improve the security of networks*".

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

There are likely to be no restrictions on the usage of sinkholes for the purpose of protection of IT systems. As is the case for honeypots, neither the Cybersecurity Act nor the PDPA restrict the usage of sinkholes for the purpose of protecting IT systems.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes, organisations are permitted to monitor or intercept electronic communications on their networks in order to prevent or mitigate the impact of cyber-attacks.

There is no law prohibiting an organisation from monitoring or intercepting electronic communications on their *own* networks. However, if such data falls within the definition of personal data, then the organisation may be required to obtain consent from the relevant individuals.

We note that, under the Protection Obligation of the PDPA, organisations are required to put in place reasonable security measures to protect personal data under its possession or control. Depending on a number of factors, the monitoring or intercepting of electronic communications on an organisation's networks may be considered to be one such reasonable security measure.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Yes. Under the Strategic Goods (Control) Act, the import and export of certain types of strategic goods and strategic goods technology is controlled, including "information security" systems, equipment and components (i.e., systems, equipment and components designed or modified to use "cryptography for data confidentiality" having "in excess of 56 bits of symmetric key length, or equivalent").

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. The PDPA sets out the baseline standards that all organisations must meet, in respect of the protection of personal data. However, certain sectoral regulators may impose higher standards on a particular industry, especially where the personal data commonly collected, used and disclosed in these industries are sensitive in nature.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Financial Services Sector

In respect of the Financial Services Sector, the Monetary Authority of Singapore ("**MAS**") has set out, in its published Guidelines on Technology Risk Management ("**MAS TRM Guidelines**"), risk management principles and best practice standards to guide financial institutions in (a) establishing a sound and robust technology risk management framework, (b)

strengthening system security, reliability, resiliency, and recoverability, and (c) deploying strong authentication processes to protect customer data, transactions and systems. These include (non-exhaustively) requiring financial institutions to establish a technology risk management framework with oversight by the board and senior management to identify, assess, monitor, report and treat technology risks.

Additionally, the MAS has also issued a Notice on Cyber Hygiene, which requires banks to, amongst others, ensure that security patches are applied to address vulnerabilities in their computer systems.

Healthcare Sector

In the healthcare sector, the Ministry of Health has issued a Cybersecurity Advisory 1/2019 in the wake of the SingHealth data breach in 2018 (*Re Singapore Health Services Pte. Ltd. & Ors.* [2019] SGPDPC 3), which involved the medical personal data of 1.5 million individuals being leaked.

In this Cybersecurity Advisory, all licensees (i.e., hospitals, clinics, etc.) are strongly encouraged to review the Committee of Inquiry's recommendations and cybersecurity best practices, and to implement relevant measures, where appropriate.

Telecommunications Sector

The IMDA has published the Telecommunication Cybersecurity Codes of Practice, which are currently imposed on major Internet Service Providers (ISPs) in Singapore for mandatory compliance. Apart from security incident management requirements, the Codes include requirements to prevent, protect, detect and respond to cybersecurity threats. The Codes were formulated using international standards and best practices including the ISO/IEC 27011 and IETF Best Current Practices.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Under section 157 of the Companies Act, directors of a company are required to, amongst others, act honestly and use reasonable diligence in the discharge of the duties of their office. In addition, under the common law, directors are also required to carry out their duties with skill, care and diligence.

Thus, if a company fails to prevent, mitigate, manage or respond to an Incident due to a lack of honesty, or a lack of the requisite skill, care and diligence on the part of its directors, this may constitute a breach of directors' duties.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) There is no present requirement for companies to designate a CISO under the relevant cybersecurity laws. The provisions of the Cybersecurity Act generally apply to owners of CIIs.

In respect of the PDPA, companies are required to appoint a Data Protection Officer ("**DPO**") under section 11(3) of the PDPA, whose duties include, amongst others, to:

- ensure compliance of PDPA when developing and implementing policies and processes for handling personal data;
- foster a data protection culture among employees and communicate data protection policies to stakeholders;
- manage data protection-related queries and complaints;
- alert management to any risks that might arise with regard to personal data; and
- liaise with the PDPC on data protection matters, if necessary.

(b) Under the Cybersecurity Act and the Cybersecurity Code of Practice for Critical Information Infrastructure, owners of a CII may be required to establish a written Incident response plan or policy in respect of that CII.

In respect of the PDPA, there is no specific requirement to establish a written Incident response plan or policy. However, section 12 of the PDPA requires organisations to, amongst others, develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. This would likely include developing a policy relating to the handling of security incidents and data breaches.

Related to the above, the PDPC has recommended in its Data Breach Guide that organisations put in place a data breach management plan, which should set out, amongst others, how the organisation should respond to a data breach.

(c) Under the Cybersecurity Act and the Cybersecurity Code of Practice for Critical Information Infrastructure, owners of a CII may be required to conduct periodic cyber risk assessments.

There is no specific requirement under the PDPA for companies to conduct periodic cyber risk assessments, including for third-party vendors. However, in its Advisory Guidelines on Key Concepts in the PDPA, the PDPC has stated that organisations should take steps to ensure, amongst others, that its computer networks are secure, and that its IT service providers are able to provide the requisite standard of IT security.

(d) Under the Cybersecurity Act and the Cybersecurity Code of Practice for Critical Information Infrastructure, owners of a CII may be required to conduct periodic cyber risk assessments, which may include penetration testing and vulnerability assessments.

There is no specific requirement for companies to perform penetration tests or vulnerability assessments under the PDPA. However, as above, the PDPC has stated in its Guide to Data Protection Impact Assessments that organisations may conduct penetration tests as part of their reasonable security arrangements to protect personal data.

We further highlight that certain sectoral regulators in Singapore impose more stringent requirements on organisations within that sector. For example, the MAS imposes certain requirements in respect of cybersecurity on its licensees, including requiring its licensees to implement robust security measures to ensure that their systems and customer data are well protected against any breach or loss.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, companies are not subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents, other than

those already mentioned above (i.e., to the relevant regulatory bodies).

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

If an Incident gives rise to a private actionable claim, the affected individual may have recourse against the organisation that caused the Incident.

Section 32 of the PDPA provides for a right of private action. Under this section, any person who suffers loss or damage directly as a result of a contravention of the organisation's obligations under Parts IV, V or VI of the PDPA (which set out organisations' obligations to protect individuals personal data) shall have a right of action for relief in civil proceedings in a court. This includes a breach of section 24 of the PDPA, which requires organisations to protect personal data which is in its possession or under its control (as outlined further above).

Under the CMA, a court may order an offender to pay a compensation amount to a victim of the offence. The victim may also pursue a civil remedy against the offender separately, as the order for payment of compensation does not prejudice the right of the victim to recover more than was compensated to him under the compensation order.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In *IP Investment Management Pte Ltd and others v Alex Bellingham* [2019] SGDC 207, the third plaintiff (a natural person) successfully obtained an order enjoining the defendant, a former employee of the first and second plaintiffs (which were corporate entities engaged in a fund management business), from using, disclosing or communicating his personal data, and also obtained an order for the defendant to deliver up any copies of his personal data.

Finding the case in favour of the third plaintiff, the court held that the defendant had breached his obligations under the PDPA; in particular, the Consent Obligation and Purpose Limitation Obligation. The court also found that the third plaintiff had suffered loss as a result of the defendant's breach of the Consent Obligation and Purpose Limitation Obligation.

It is worth noting that the court found that the first and second plaintiffs had no legal standing to bring the claim under section 32 of the PDPA, as it held that section 32 of the PDPA did not extend to corporate entities. Thus, as the first and second plaintiffs were corporate entities, their applications were disallowed by the court.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes. Depending on the circumstances of the Incident, it is possible that one or more causes of action in tort may be applicable. For example, if an organisation had breached its duty of care under the tort of negligence, by failing to put in place measures to prevent an Incident, the organisation may be found liable under this tort.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents in Singapore.

As of the date of writing, a number of insurance providers in Singapore provide cyber insurance, which covers, amongst others, data protection/personal data liability and corporate data liability.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are presently no regulatory limitations to insurance coverage against specific types of loss in respect of cyber insurance.

However, it bears noting that as insurance contracts are ultimately contracts, they are also subject to contractual law principles. These principles include, amongst others, that such a contract will be enforceable only if it is not tainted by illegality or is contrary to public policy.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

There are a number of laws that would provide investigatory powers to the relevant regulators/law enforcement personnel.

Generally, the Singapore law enforcement authorities have fairly broad powers under the Criminal Procedure Code (Cap. 68) ("**CPC**") to access, inspect and check the operation of any computer that they suspect is or has been used in connection with, or contains or contained evidence relating to, an arrestable offence. This may include offences under the CMA.

In relation to the PDPA, section 50 of the PDPA empowers the PDPC with powers of investigation to investigate whether organisations are in compliance with the PDPA. The powers are set out in the Ninth Schedule of the PDPA, which includes, amongst others, the power to require documents or information to be produced by the organisation to the PDPC, as well as the power to enter premises (both without and with a warrant), subject to certain conditions being satisfied.

In relation to the Cybersecurity Act, the Commissioner of Cybersecurity is empowered under sections 19 and 20 to investigate and prevent cybersecurity incidents. These powers include requiring, by written notice, any person to produce to the incident response officer appointed by the Commissioner of Cybersecurity, any physical or electronic record, or document that is in the possession of that person.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there are no requirements for organisations to implement backdoors in their IT systems for law enforcement authorities. However, there is a requirement (under certain circumstances) to provide law enforcement authorities with encryption keys.

Under section 40 of the CPC, for the purposes of investigating an arrestable offence, an authorised police officer or other authorised person can require any person whom he reasonably suspects to be in possession of any decryption information, to grant him access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence.

Lim Chong Kin heads Drew & Napier's Technology, Media and Telecommunications Practice Group, and is co-head of the firm's Data Protection, Privacy & Cybersecurity Practice.
Under Chong Kin's leadership, these Practices are consistently ranked as the leading practices in Singapore. His clients include the telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers.
Chong Kin has been an external legal and regulatory advisor for the Personal Data Protection Commission of Singapore since 2013, and he played a key role in the liberalisation of Singapore's telecoms, media and postal sectors, where he drafted the competition frameworks.
Chong Kin is highly regarded by his peers, clients and rivals alike for his expertise, and is consistently recommended as a leading lawyer by major international legal publications such as *Chambers Asia-Pacific*, *The Legal 500 Asia Pacific*, *Who's Who Legal*, *The Guide to the World's Leading Competition & Antitrust Lawyers/Economists*, *Global Competition Review*, *Practical Law Company – Which Lawyer?*, *Asialaw Profiles* and *Best Lawyers*.

Drew & Napier LLC
10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 65314110
Fax: +65 65354864
Email: chongkin.law@drewnapier.com
URL: www.drewnapier.com

David N. Alfred is a director of Drew & Napier LLC and co-head of the firm's Data Protection, Privacy and Cybersecurity Practice. He is concurrently co-head and programme director of the Drew Data Protection & Cybersecurity Academy. David is a data protection, cybersecurity and technology lawyer with over 20 years' experience advising on a broad range of matters relating to digital technology, telecommunications and the internet.
David's practice over the last 10 years has focused on data protection and cybersecurity. He has substantial experience advising on data protection compliance, public policy and legislation, regulatory enforcement, data breaches and international aspects of data protection.
Prior to joining the firm, David was the first Chief Counsel to Singapore's data protection authority, the Personal Data Protection Commission. He has also worked in other in-house roles including with Singapore's media and telecom regulator, the Info-communications Media Development Authority.

Drew & Napier LLC
10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 65312342
Fax: +65 65354864
Email: david.alfred@drewnapier.com
URL: www.drewnapier.com

Albert Pichlmaier is a senior cybersecurity engineer with Drew & Napier LLC and concurrently course director (cybersecurity) with the Drew Data Protection & Cybersecurity Academy. Albert is an IT professional with 30 years of international experience in the private and public sectors. He has worked in a wide range of IT and security domains, from smart card firmware development and test automation, to artificial intelligence and blockchain development. Albert holds a degree in computer science and the CISSP and CDPSE certifications.
Prior to joining the firm, Albert worked for over 10 years in the public sector in Singapore. Most recently, he worked with Singapore's data protection authority, the Personal Data Protection Commission, where he was involved in technology and cybersecurity assessments for data protection compliance and enforcement cases. Prior to that, he was the technical manager for common criteria certifications with the Info-communications Development Authority of Singapore.

Drew & Napier LLC
10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 65314108
Fax: +65 65354864
Email: albert.pichlmaier@drewnapier.com
URL: www.drewnapier.com

Drew & Napier LLC has provided exceptional legal advice and representation to discerning clients since 1889 and is one of the leading and largest law firms in Singapore.
The firm's work in data protection, privacy and cybersecurity precedes the advent of Singapore's Personal Data Protection Act 2012 and Cybersecurity Act 2018. Over the last decade, Drew & Napier has been one of the leading Singapore practices in the fields of data protection, privacy and cybersecurity. The firm has advised and acted for a wide range of clients on a variety of matters which run the full gamut. These include implementation of group-wide data protection compliance programmes, localisation of global data privacy policies, data protection training programmes, requirements of Singapore's Cybersecurity Act 2018, developing a data breach management plan, dealing with data breaches and cybersecurity incidents (whether involving hacking, malware or accidental disclosure), data breach reporting requirements, conducting data protection and regulatory risk audits and addressing *ad hoc* legal queries.

www.drewnapier.com

DREW & NAPIER

Sweden

Jonas Forzelius

Esa Kymäläinen

TIME DANOWSKY Advokatbyrå AB

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Hacking is considered a breach of data security (Sw. *dataintrång*) under the Swedish Criminal Code and is punishable either by fine or prison for up to two years. Serious offences are punishable by prison for at least six months and up to six years.

If a breach of data security, such as hacking, is committed by an employee of a company, it may result in an administrative penalty for the company, if the company is deemed not to have implemented sufficient measures to prevent breaches of data security or if the offender holds a leading position or similar in the company. This also applies to foreign companies conducting business activities in Sweden.

In 2014, a police officer was convicted by the Swedish Supreme Court for breach of data security after having used the internal IT system at the Swedish Police Authority to carry out searches for private purposes. The officer in question had solicited access to the system for professional purposes only and was therefore sentenced to a fine for the unauthorised searches.

Denial-of-service attacks
To prevent or seriously disturb the use of electronic information is considered a breach of data security under the Swedish Criminal Code and, consequently, punishable by a fine or prison for up to two years. Serious offences are punishable by prison for six months to six years. A breach of data security may also entail corporate fines if the offence is committed by an employee of a company.

Phishing
Phishing is considered fraud (Sw. *bedrägeri*) under the Swedish Criminal Code and is punishable by a fine or prison for up to two years. Serious offences are punishable by prison for at least six months to six years.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
The Swedish Court of Appeal has ruled that unauthorised installation of software on a computer is not considered a breach of data security itself. If, however, the installation constitutes an intentional alteration, deletion or blocking of electronic information in the system, the prerequisites for breach of data security are met.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Distribution, sale or offering for sale of products used to commit a breach of data security may constitute complicity or preparation to commit breach of data security, which is considered a crime under the Swedish Criminal Code. Preparation to commit breach of data security is punishable by fine or prison for up to two years. Serious offences are punishable by prison for at least six months and up to six years. The same apply for complicity.

Possession or use of hardware, software or other tools used to commit cybercrime
Possession or use of tools to commit a breach of data security does not itself constitute a crime but may amount to complicity or preparation to commit breach of data security, which is considered a crime under the Swedish Criminal Code. Preparation to commit breach of data security is punishable by a fine or prison for up to two years. Serious offences are punishable by prison for at least six months and up to six years. The same applies for complicity.

Further, the use, development, marketing or possession of technical instruments, components or services with the purpose of gaining unauthorised access to copyright protected materials may constitute a breach of the Swedish Copyright Act, punishable by fine or prison for up to two years.

As for hardware or software designed to be used for decoding of certain services, as defined in the Swedish Act on Decoding (e.g. radio and TV broadcasting), the development, marketing or possession of such tools may constitute a breach of said act and is punishable by fine or prison for up to two years.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft and identity fraud is criminalised as unlawful identity use (Sw. *olovlig identitetsanvändning*) under the Swedish Criminal Code and punishable by fine or prison for up to two years.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Copyright infringement (Sw. *upphovsrättsbrott*) is subject to the penal provisions pursuant to the Swedish Copyright Act and punishable by a fine or prison for up to two years.

In general, disclosing of information subject to an employer-employee confidentiality agreement does not, itself, constitute a breach of law. However, subject to the Swedish Trade Secrets Act (Sw. *Lag om företagshemligheter*), the disclosure of information defined as trade secrets may amount to a criminal offence,

punishable by a fine or prison for up to two years. Serious offences are punishable by prison for at least six months and up to six years.

Further, as regards professions that are subject to statutory confidentiality, e.g. for doctors, breaches of confidentiality ("breach of duty of confidentiality", Sw. *brott mot tystnadsplikt*) are punishable under the Swedish Criminal Code by fine or prison for up to one year.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Penetration testing is a commonly used method amongst organisations to secure and develop IT systems in order to comply with cybersecurity regulations. However, unsolicited penetration testing may constitute and be punishable as a breach of data security under the Swedish Criminal Code, which is applicable to breaches of any form of data within an IT system regardless of any intention to make use of or damage it.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

In addition to the abovesaid, it may be noted that an action causing damage to physical equipment, such as computers, servers, etc. may constitute an act of damage to property (Sw. *skadegörelse*), which is punishable under the Swedish Criminal Code by prison for up to two years.

Damaging or destroying certain equipment of considerable importance in providing defence, supplying the needs of the population, the administration of justice or public administration in the country, or the maintenance of public order and security in the country, may constitute sabotage (Sw. *sabotage*), which is criminalised under the Swedish Criminal Code and punishable by fine or prison for up to two years. Serious offences are punishable by prison for at least six months and up to six years.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Generally, extraterritorial application of the Swedish Criminal Code requires that the relevant offence is also criminalised in the country where it was committed. Additionally, extraterritorial application presupposes a certain connection to Sweden as defined in the Swedish Criminal Code, e.g. that the offence has been committed by a Swedish citizen or a foreigner residing in Sweden, or that the offence is punishable by more than six months in prison and has been committed by a foreigner residing abroad but currently located in Sweden.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Most of the above-mentioned offences are criminalised as breach of data security under the Swedish Criminal Code, through which the requirements of EU law have been implemented. Criminal liability under said provision applies to different forms of unauthorised, intentional disposals of electronic information, such as hacking, denial-of-service attacks, phishing, infections of IT systems, etc. Accordingly, unintentional acts are not considered criminal breaches of data security. Criminal liability is also exempted in cases of authorised or consented access, such as assignments to perform penetration tests. However, this exception does not necessarily apply to acts without intent to cause damage and/or make a financial gain; the mere unauthorised access or disposal of electronic information constitutes a breach of data security.

Liability for complicity and preparation to commit offences under the Criminal Code, such as breach of data security, may be exempted in certain cases. The use, possession, distribution or sale of tools used to commit cybercrime does not entail criminal liability for preparation, if the tools in question lack clear connection to the criminal activity. Voluntary resignation may also exempt liability for preparation. There is no exception applicable for completed offences, but the penalty may be mitigated if the offender tried to prevent the offence or reduce the damage caused by it.

Unlawful disclosures under the Swedish Trade Secret Acts may, under certain circumstances, be deemed lawful. An employee, for instance, may disclose trade secrets to the public or the authorities if the disclosure aims to reveal something that can reasonably be suspected to constitute a crime that may lead to imprisonment, or if the information otherwise reveals misconduct deemed to be of public interest.

There are also some general exceptions for criminal copyright infringements under the Swedish Copyright Act (e.g. private use, educational purposes etc.).

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity legislation extends over several areas of Swedish law:

- Data protection, particularly the processing of personal data, is regulated directly by the EU General Data Protection Regulation (GDPR).
- Personal data processing by governmental authorities responsible for crime prevention, investigation and prosecution is regulated by the Swedish Act on Processing of Personal Data Relating to Criminal Offences (Sw. *Brottsdatalagen*).
- Criminal offences, including cybercrimes such as breaches of data security, are subject to the Swedish Criminal Code (Sw. *Brottsbalken*).
- Copyright infringement is regulated by the Swedish Copyright Act (Sw. *Lag om upphovsrätt till litterära och konstnärliga verk*).
- Decoding activities regarding radio and TV are criminalised and regulated by the Swedish Act on Decoding (Sw. *Avkodningslagen*).
- Acts of terrorism, including cyberattacks, are regulated by the Swedish Act on Criminal Responsibility for Terrorist Offences (Sw. *Lag om straff för terroristbrott*).
- Providers of electronic communication services are subject to the Swedish Act on Electronic Communication (Sw. *Lag om elektronisk kommunikation*).
- Certain entities that provide critical infrastructure services or IT systems are subject to the EU Directive on Security of Network and Information Systems (NIS), which has been implemented by the Swedish Act on Information Security

Regarding Providers of Critical Infrastructure and Digital Services (Sw. *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster*).

- The Swedish Act on Payment Services regulates payment services provided in Sweden (Sw. *Lag om betaltjänster*).
- Disclosure of trade secrets is prohibited by the Swedish Trade Secrets Act (Sw. *Lag om företagshemligheter*).
- Further, certain operations and activities deemed important to Swedish national security are regulated by the Swedish Protective Security Act (Sw. *Säkerhetsskyddslag*).

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Certain entities that provide critical infrastructure services or IT systems are subject to the EU Directive on Security of Network and Information Systems (NIS), which is implemented through the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services. The regulation entails obligations for such providers to carry out certain preventive measures in order to achieve a high degree of network security and IT-system security.

The Swedish Protective Security Act and the Protective Security Ordinance requires security-sensitive entities and businesses to prevent information security incidents and damages and to classify security-sensitive data.

Furthermore, in light of the development of 5G, a new EU directive will be implemented to Swedish law by amending the Swedish Act on Electronic Communications. The directive aims to ensure that the usage of radio transmitters will not constitute a threat to Swedish national security but also entails new obligations towards customers.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The GDPR regulates data controllers and processors processing personal data, the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services regulates providers of critical infrastructure services, the Swedish Act on Electronic Communications regulates electronic service providers and the Swedish Act on Payment Services regulates providers of payment services. These acts contain obligations for organisations to implement appropriate technical and organisational measures, generally including monitoring, detecting, preventing, and mitigating incidents.

Organisations carrying out security-sensitive activities are also obligated to establish and document security needs, plan and enforce security measures (such as classifying data) and follow up on the security work of the organisation. Such organisations must also report any important information to the relevant supervisory authority.

The Swedish Civil Contingencies Agency has issued regulations and requirements that all governmental authorities must follow. This includes drafting security policies and documenting security measures taken.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Several laws require organisations to report incidents to different authorities. The extent to which incident-related information must be reported, however, is generally not explicitly regulated by law but instead depends on the nature of the individual incident.

The GDPR requires data controllers to report personal data incidents to the Swedish Data Protection Authority without undue delay and not later than 72 hours after having become aware of it, unless the incident is of minor importance. The report should describe the nature of the incident, such as the scope of individuals and the categories of data subjects affected. Furthermore, the likely effects of the data breach, as well as a description of measures taken or proposed to address such effects, must be reported. The data controller must also provide its contact details to the authority.

Banks, health services and other providers of critical infrastructure services must report incidents to the Swedish Civil Contingencies Agency without undue delay. This follows from the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services. The supervisory authority drafts regulations specifying the information that such a report should include.

Any organisation that conducts security-sensitive activities under the Swedish Protective Security Act is required to report incidents to the supervisory authority, which may be either the Swedish Security Service or the Swedish Armed Forces.

Severe interruptions in electronic services must be reported by the provider to the Swedish Post and Telecom Authority. An incident is defined as an unlawful destruction, disclosure, or access to information. The provider must notify the authority within 24 hours in case of an integrity incident. If any subscribers to the electronic service are affected by the incident, the provider is obliged to notify them as well.

Providers of payment services subject to the Swedish Act on Payment Services are obliged to report incidents to the Swedish Financial Supervisory Authority without undue delay. The providers must also notify any affected individuals and provide them with information about the incident and how to mitigate the effects of it.

Generally, all individuals have the right to request and access documents from governmental authorities. This follows from the Principle of Public Access to Official Records. However, exceptions can be made if the requested information can be considered confidential.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The GDPR requires data controllers to communicate any personal data incident that is likely to result in a high risk to the rights of the affected data subject.

Entities subject to the Swedish Act on Electronic Communications are required to report incidents to affected subscribers without undue delay. The same applies to providers of payment services under the Swedish Act on Payment Services whenever an incident entails risks to user transactions.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The Swedish Post and Telecom Authority is responsible for supervising compliance of the Swedish Act on Electronic Communications. The Swedish Data Protection Authority is responsible for GDPR-related issues. Supervision of matters related to the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services are shared between the Post and Telecom Authority and the Swedish Civil Contingencies Agency. The latter is responsible for handling incident reports, among other things, while the Post and Telecom Authority is responsible for the supervision of the digital sector, i.e. cloud services.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Failure to comply with GDPR, including its requirements on incident reports and/or the implementation of technical and organisational measures, may result in an administrative fine. The amount payable depends on the extent and gravity of the infringement. It may, at most, amount to the highest of 20 million euros or four per cent of the data controller's worldwide annual turnover. Actors within the public sector may be fined up to 5 million SEK for less serious infringements and up to 10 million SEK for more serious infringements.

Infringements of obligations under the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services may result in a fine of between 5,000 SEK and 10 million SEK. The same applies to failure to comply with the Swedish Act on Payment Services, where, however, the maximum amount payable is set to 50 million SEK.

Non-compliance with the Swedish Act on Electronic Communications may result in a fine or up to six months of imprisonment.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Since the Swedish Data Protection Authorities started investigating GDPR compliance in June 2018, several penalties such as warnings, injunctions and administrative fines have been issued towards non-compliant companies. In a recent high-profile case from March 2020, the Data Protection Authority imposed a 75 million SEK fine on Google for failure to comply with the GDPR. According to the authority, Google had not fulfilled its obligations in respect of the right to request delisting from the search engine. Google has appealed against the decision and a judgment is pending August 2020.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
According to the Swedish Act on Electronic Communication, as well as the GDPR, the use of web beacons is permitted.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There are no explicit provisions in Swedish law to address honeypots. However, the honeypot mechanism may in some specific cases be considered a sting operation, which is prohibited as a law enforcement method in Sweden.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The use of sinkholes is not prohibited with consent provided by the relevant operator but may result in legal difficulties depending on the nature of the information that is received and re-directed.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes, if it is considered necessary and justified and the employee has been informed that such monitoring may occur. Due to the unbalanced relation between an employer and employee, however, the employee may not be considered able to freely consent to monitoring and network interception. The employer must ensure that such supervisory measures are compliant with applicable laws. For instance, if the monitoring includes processing of the employee's personal data, the GDPR must be considered.

Further, employees are bound to fulfil a general duty of loyalty towards their employers. This duty may include an obligation to report cyber incidents.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Export restrictions may apply for technology designed to prevent or mitigate the impact of cyberattacks. EU law and Swedish legislation regulate the control of dual-use products, i.e.

products with established civilian functions that can also be used for military purposes. EU Regulation 2019/2199 establishes a list of restricted dual-use items, including telecommunications and "information security" items. Control and compliance are handled by the Swedish Inspectorate for Strategic Products.

Some cryptographic equipment is included in the list of export-restricted dual-use items, but not for private use.

The above-mentioned regulation does not restrict transit within the EU or import.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Some market practices deviate from legal requirements through application of general standards implemented to ensure and simplify regulatory compliance. Examples of such standards are ISO 27002:2018, ISO 27001:2017 and NIST 800-88, none of which are mandatory. It is complicated to shortly detail business sectors subject to different standards; however, the financial and telecom sectors are generally more regulated than other sectors.

The Swedish Financial Supervisory Authority issues non-mandatory recommendations and regulations and regularly investigates compliance and standards. Also, the Swedish Standards Institute (SSI) provides standards to member companies, organisations and agencies and adopts European standards as part of the European Committee for Standardisation.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Actors in the financial sector, such as banks, are bound to comply with certain regulations and guidelines issued by the Swedish Financial Supervisory Authority with regard to their IT systems.

As mentioned in section 2, several laws apply to entities in different sectors in relation to cybersecurity. The legal requirements vary depending on what kind of activity that they carry out. Depending on whether the organisation is processing of personal data, providing electronic services, critical infrastructure services, or carrying out security-sensitive activities, etc. different laws apply: GDPR; the Act on Electronic Communication; the Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services; the Protective Act; and the Act on Payment Services.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Directors and officers are not personally responsible for breaches of Applicable Law by the company. However, if the company is penalised due to the directors' failure to take appropriate measures to comply with Applicable Laws, the director may be subject to sanctions in accordance with Swedish labour law.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

a) There are currently, in most cases, no requirements under any Applicable Laws to designate a CISO. In some cases, the GDPR demands that a Data Protection Officer (DPO) be appointed, e.g. for public authorities or bodies. Further, the GDPR, the Swedish Protective Act, the Swedish Act on Information Security Regarding Providers of Critical Infrastructure and Digital Services and the Swedish Act on Electronic Communications all require certain technical and organisational measures. However, technical and organisational measures are not defined in detail. The Swedish Act on Electronic Communications will be updated on 23rd December at the latest, due to the European Electronic Communications Codex (EECC) Directive. The EECC directive brings some clarification, e.g. by providing a definition of "security measures".

b) If a company is affected by the Swedish Protective Security Act, it must ensure that a Protective Security Officer is appointed – which could be considered equivalent to a CISO.

c) As for the GDPR, a written Incident response plan should be adopted to ensure that all requirements of the GDPR are fulfilled when dealing with a personal data breach, e.g. in order to comply with the maximum 72-hour reporting period.

d) Companies subject to the Swedish Protective Security Act are required to carry out protective security analyses and adopt protective security measures. It is not explicitly stated whether they need to be periodic or not, but the analyses must be updated when needed.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Companies that are listed on the public market are required by the Swedish Act on Market Abuse to disclose information that may affect the market price of the shares to the public. The obligation to make such information public applies without regard to the origin of the information, albeit with some exceptions.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The GDPR provides data subjects with different rights, *i.a.*, the right to be forgotten and, in certain situations, the right to consent before personal data is transferred to a third party. If such rights are ignored by a processing entity, the data subjects may file a lawsuit against the processing entity which may result in right to damages for the data subject.

A civil action may be brought on many different grounds. In case of an incident, there are generally several ways to seek damages inflicted from the responsible party.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In 2015, the Court of Appeal afforded damages of a total value of 5,000 SEK to be paid by a data intruder to the plaintiff. The case was brought by a public prosecutor against the data intruder, whereas the damages were sought by the plaintiff.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The Swedish Tort Liability Act provides a general possibility to seek remedies for damages caused by, e.g. negligence. However, The Swedish Tort Liability Act is subsidiary to other legislation, such as the GDPR.

Article 82 of the GDPR grants any physical person, who has suffered material or non-material damage a result of an infringement of the Regulation, the possibility to seek compensation from the responsible data controller or processor.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

In general, it is possible for organisations to purchase insurance against third-party claims, e.g. due to a data breach. However, it is unlikely for a person to be able to insure him/herself against claims from authorities, or for liability due to their own criminal actions, e.g. as breaches of data security, albeit this is not totally clear in Sweden.

An affected party, on the other hand, is entitled to insurance compensation even if the damage was caused by a criminal action.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no limitations as to types of loss an insurance may cover, with the exception of administrative fines and sanctions imposed by the authorities.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The authorities differ depending on the sector in question. If the Incident constitutes a crime punishable by the Swedish Criminal Code (or another Act where the penalty is prison) the Swedish Police, the Swedish Prosecution Authority and/or the Swedish Security Service will investigate it, depending on the crime.

If the Incident concerns GDPR-related issues, i.e. personal data, the Swedish Data Protection Authority is the investigative authority.

If the Incident is influencing IT systems that provide critical infrastructure, e.g. traffic, the Swedish Civil Contingencies Agency is the investigative authority.

If a service provider fails to report an Incident, The Swedish Post and Telecom Authority constitutes the investigative authority.

If the Incident is connected to payment services, the Swedish Financial Supervisory Authority is the investigative authority.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Swedish law does not require organisations to implement backdoors or provide encryption keys.

Jonas Forzelius is one of the founders of Time Danowsky Law Firm and has more than 20 years' experience of advising clients in IT, outsourcing, intellectual property, and regulatory matters relating to IT-procurements and other commercial and public projects. He has extensive experience in assisting clients in both the public and private sectors in complex projects, contract drafting, negotiations and regulatory advice including cybersecurity matters and litigation.

Experience
Partner, TIME DANOWSKY Advokatbyrå (since 2020).
Partner, Time Advokatbyrå (2007–2020).
Associate & managing associate, Linklaters Advokatbyrå (2001–2007).
Associate, Lagerlöf & Leman Advokatbyrå, London (1999–2001).
Law clerk, Stockholm County Court (1999).
Trainee, Lagerlöf & Leman Advokatbyrå (1998–1999).

TIME DANOWSKY Advokatbyrå AB
Birger Jarlsgatan 15
S-114 11 Stockholm
Sweden

Tel: +46 70 753 09 69
Email: jonas.forzelius@timedanowsky.se
URL: www.timedanowsky.se

Esa Kymäläinen has nearly 20 years' experience of working in the areas of IP and IT law, data protection, regulatory issues and dispute resolution. Esa also has extensive experience of crisis management and as an advisor in connection with internal investigations and threat situations.

Experience
Partner, TIME DANOWSKY Advokatbyrå (since 2020).
Partner, Danowsky & Partners Advokatbyrå (2012–2020).
Associate, Danowsky & Partners Advokatbyrå (2000–2011).
District Court Clerk, Stockholm City Court (2000).

TIME DANOWSKY Advokatbyrå AB
Birger Jarlsgatan 15
S-114 11 Stockholm
Sweden

Tel: +46 70 288 76 04
Email: esa.kymalainen@timedanowsky.se
URL: www.timedanowsky.se

TIME DANOWSKY is a law firm with focus on today's business, where technology, innovation and media/content form a natural part of all our business activities.
We offer high-end legal expertise with focus on tech/IT, media, and IP. Practice areas include all types of commercial legal matters, including contracts, M&A, outsourcing, protection of intellectual property rights, marketing, employment law, competition, public procurement and regulatory compliance and cybersecurity.
The Firm is also well known for its first-class dispute resolution practice, having represented Swedish and international clients in a number of complex, high-profile cases.
TIME DANOWSKY was formed in January 2020, through a merger between the law firms Time Advokatbyrå and Danowsky & Partners.

www.timedanowsky.se

TIMEĐANOWSKY

Switzerland


Dr. Oliver M. Brupbacher


Dr. Nicolas Mosimann


Marlen Schultze

Kellerhals Carrard

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

According to art. 143bis Swiss Criminal Code (SCC), hacking may constitute a criminal offence: Any person who obtains unauthorised access, by means of data transmission equipment, to a data-processing system that has been specially secured to prevent such access, may be prosecuted upon complaint and be liable for a custodial sentence not exceeding three years or a monetary penalty. Art. 143bis SCC was revised to reflect Switzerland's implementation of the Budapest Convention on Cybercrime.

Unauthorised access to another person's password-protected email account constitutes hacking and is punishable under art. 143bis SCC (BGer 6B_615/2014 and 6B_456/2007; *cf.* also BGE 130 III 28). According to a ruling by the Swiss Federal Supreme Court (FSC), it is irrelevant in the application of art. 143bis SCC how the offender came into possession of the password (BGE 145 IV 185).

Data theft is covered by art. 143 SCC: Any person who for their own or for another's unlawful gain obtains data for themselves or another, which is stored or transmitted electronically or in some similar manner and which is not intended for them and has been specially secured to prevent their access, is liable for a custodial sentence not exceeding five years or a monetary penalty.

In 2019, there were 16 convictions for crimes under art. 143bis SCC and seven convictions for crimes under art. 143 SCC in Switzerland.

Denial-of-service attacks

Denial-of-service attacks may constitute damage to data (art. 144bis SCC): Any person who without authority alters, deletes or renders unusable data that is stored or transmitted electronically or in some other similar way, may be prosecuted upon complaint, and be liable for a custodial sentence not exceeding three years or a monetary penalty. There is no requirement that the process is irreversible; even the temporary denial of access is punishable. A custodial sentence of a minimum of one to five years may be imposed on an offender who has caused major damage. Other than hacking, this offence is prosecuted *ex officio*.

In 2019, there were 16 convictions for crimes under art. 144bis SCC.

Depending on the specific *modus operandi* of the attack, further criminal provisions may apply, including extortion (art. 156 SCC), misuse of a telecommunications installation (art. 179^{septies} SCC) or coercion (art. 181 SCC).

Phishing

Depending on the circumstances, phishing may be covered by multiple criminal offences under the SCC, in particular:

- Unauthorised obtainment of data (art. 143 para. 1, custodial sentence not exceeding five years or a monetary penalty).
- Unauthorised access to a data-processing system (art. 143bis para. 1, prosecution upon complaint, custodial sentence not exceeding three years or a monetary penalty).
- Obtainment of personal data without authorisation (art. 179^{novies}, prosecution upon complaint, custodial sentence not exceeding three years or a monetary penalty).
- Forgery of a document (art. 251, custodial sentence not exceeding five years or a monetary penalty).
- Computer fraud (art. 147, custodial sentence not exceeding five years or a monetary penalty; if offenders act for commercial gain, they are liable for a custodial sentence not exceeding 10 years or a monetary penalty of a minimum of 90 daily penalty units).
- Fraud (art. 146, custodial sentence not exceeding five years or a monetary penalty; if offenders act for commercial gain, they are liable for a custodial sentence not exceeding 10 years or a monetary penalty of a minimum of 90 daily penalty units; for the interplay with art. 147 *cf.* BGE 129 IV 22, at 4.2).

The fraudulent use of a trademark or a copyright-protected work may be prosecuted under art. 62 Trade Mark Protection Act or art. 67 Copyright Act, each of which provides for a custodial sentence not exceeding one year or a monetary penalty.

2019 saw the first prosecution and conviction for "voice phishing" (Federal Criminal Court (FCC) SK.2019.9). One hundred and twenty-seven cyber-/phishing investigations by the Office of the Attorney General of Switzerland were pending at the end of 2019.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Apart from the application of the specific criminal provisions applicable to denial-of-service and phishing attacks (*cf.* above), the infection of IT systems with malware may be prosecuted under art. 143bis SCC, which penalises hacking, and art. 144bis para. 1 SCC, which covers damage to data.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
According to the so-called "virus offence" (art. 144bis para. 2 SCC), any person who without authorisation manufactures, imports, markets, advertises, offers or otherwise makes programs accessible, that they know or must assume will be used to cause damage to data (art. 144bis para. 1 SCC; *cf.* "Denial-of-service attacks" above), or provides instructions on the manufacture of such programs, is liable for a custodial sentence not exceeding three years or a monetary penalty. If the offender acts for commercial gain, a custodial sentence of a minimum of one to five years may be imposed. The FSC held that this provision also applies where the instructions have not been created by the offender, and even if they are incomplete, so long as they contain specific and relevant information for the manufacture of programs used to cause damage to data (BGE 129 IV 230).

Any person who markets or makes accessible passwords, programs or other data that they know or must assume are intended to be used to commit a hacking offence (art. 143bis para. 1 SCC; *cf.* "Hacking" above), is liable for a custodial sentence not exceeding three years or a monetary penalty (art. 143bis para. 2 SCC).

Possession or use of hardware, software or other tools used to commit cybercrime
The mere possession of such tools is not illegal.

Identity theft or identity fraud (e.g. in connection with access devices)
While not explicitly regulated, identity theft can be punishable under arts 143bis, 143 SCC (unauthorised access to a data-processing system and unauthorised obtainment of data; *cf.* "Hacking" above), arts 146, 147 SCC (fraud or computer fraud), arts 173–178 SCC (offences against personal honour), or art. 179^{novies} SCC (obtainment of personal data without authorisation).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Data theft is covered by art. 143 SCC (*cf.* "Hacking" above).

Further, the betrayal of a manufacturing or trade secret amounts to a criminal offence if the offender is under a statutory or contractual duty of confidentiality (art. 162 SCC). This offence may be prosecuted upon complaint and is punishable with a custodial sentence not exceeding three years or a monetary penalty.

Depending on the circumstances, political, industrial or military espionage (arts 272–274 SCC) may also apply. These offences are generally punishable with a custodial sentence not exceeding three years, a monetary penalty or, in serious cases, a custodial sentence of a minimum of one year.

A wilful breach of a professional duty of confidentiality (*e.g.* banking secrecy, medical secrecy or attorney-client privilege) concerning sensitive personal data collected in the exercise of the profession is punishable, upon complaint, with a monetary penalty (art. 35 Federal Act on Data Protection (FADP)).

Deliberate and unlawful copyright infringements are covered by arts 67 *et seqq.* Copyright Act and are punishable with a custodial sentence not exceeding one year or a monetary penalty.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Unsolicited penetration testing may qualify as hacking and be sanctioned under art. 143bis SCC (*cf.* "Hacking" above), given that this offence does not require an intent of unjust enrichment.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Beyond the above, notable other criminal offences, both general and sector-specific, include the following:

- Criminal mismanagement (art. 158 SCC): a custodial sentence not exceeding three years or a monetary penalty; or a custodial sentence of one to five years if the offender acts to secure an unlawful financial gain for himself or another.
- Participation in a criminal organisation (art. 260ter SCC): a custodial sentence not exceeding five years or a monetary penalty (*cf.* rulings on "cyber jihad/cyber terrorism" by the FCC [SK.2013.39] and the FSC [BGer 6B_645/2007]).
- Money laundering (art. 305bis SCC), which is of particular importance in connection with denial-of-service and ransomware attacks (*cf.* above): a custodial sentence not exceeding three years or a monetary penalty, in serious cases not exceeding five years or a monetary penalty whereby a custodial sentence is to be combined with a monetary penalty.
- Breach of official, postal or telecommunications secrecy and of professional confidentiality (arts 320 *et seqq.* SCC): generally, a custodial sentence not exceeding three years or a monetary penalty; further punishable breaches of confidentiality are covered in particular by art. 47 Banking Act, art. 147 Financial Market Infrastructure Act (FinMIA), and arts 43, 53 Telecommunications Act (TCA).
- Disruption of public services, in particular of the railway, postal, telegraphic or telephone services, or of a public utility or installation which provides water, light, power or heat (art. 239 SCC): a custodial sentence not exceeding three years or a monetary penalty.
- Falsification or suppression of information (art. 49 TCA): a custodial sentence not exceeding three years or a monetary penalty.
- Misuse of information (art. 50 TCA): a custodial sentence not exceeding one year or a monetary penalty.
- Unsolicited distribution of spam messages (art. 3 para. 1 lit. o, art. 23 Unfair Competition Act): a custodial sentence of up to three years or a monetary penalty.
- Export or brokerage of certain goods for the monitoring of internet or mobile telecommunications without permission (art. 9 Ordinance on the Export and Brokerage of Goods for Internet and Mobile Communication Surveillance): a custodial sentence of up to three years or a monetary penalty.

Because IT security is regulated in Switzerland with respect to specific objects (data, systems and products) and industries, further criminal offences may apply, depending on the circumstances.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Generally, the above-mentioned offences have extraterritorial application only if they are also liable for prosecution at

the place of commission (or the place of commission is not subject to criminal law jurisdiction), if the offender is located in Switzerland, and if he/she is not extradited (arts 6, 7 SCC).

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Sentencing under Swiss law is determined by multiple factors pertaining to the offender. Mitigating factors include: acting with honourable motives, under duress or in serious distress; excusable emotional strain; psychological stress; serious provocation; a show of genuine remorse, in particular if the offender has made reparations; or the time elapsed since the crime where the offender has exercised good behaviour (art. 48 SCC). Withdrawal from the act or active repentance are further potential mitigating factors (art. 23 SCC).

The competent authority shall refrain from prosecuting the offender, bringing him to court or punishing him if the level of culpability and the consequences of the offence are minor (art. 52 SCC).

Notably, "hacking" according to art. 143bis SCC does not require an intent of harm or unjust enrichment.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity Incidents may trigger the application of many different statutes. Rather than in a comprehensive manner, Switzerland regulates cybersecurity with respect to specific objects (data, systems and products) and specific industries. Moreover, minimum cybersecurity measures are rarely defined by law, but are left to self-regulation. There is hardly any case law to clarify the standards, either.

The 2018–2022 National Strategy for the Protection of Switzerland against Cyber Risks (NCS II) has acknowledged the need for greater standardisation and regulation across various objects and sectors.

Among the general laws applicable in the cybersecurity field are the following:

- Civil Code.
- Code of Obligations (CO).
- Criminal Code.
- Council of Europe Budapest Convention on Cybercrime of November 23, 2001 (ETS No. 185; in force in Switzerland since January 1, 2012).
- Employment Act.
- Unfair Competition Act.
- Copyright Act.
- Trade Mark Protection Act.

Among the object-specific or sector-specific laws are the following:

- FADP (revised Act approved by Parliament on September 25, 2020 and expected to enter into force in 2022) and related Ordinance, as well as cantonal data protection laws.
- Revised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108; not yet ratified and in force but approved by Parliament on June 19, 2020 – referendum deadline expired on October 8, 2020).
- Product Safety Act.
- Product Liability Act.
- Banking Act and related Ordinance.
- FinMIA.
- Financial Market Supervision Act (FINMASA).
- Therapeutic Products Act and related Ordinance.
- Electronic Health Records Act and related Ordinance.
- Revised Medical Devices Ordinance (MedDO) (main provisions will enter into force on May 26, 2021).
- TCA and related Ordinance.
- Embargo Act.
- Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods and related Ordinance.
- Ordinance on the Export and Brokerage of Goods for Internet and Mobile Communication Surveillance.
- Intelligence Service Act.
- Ordinance on Protection against Cyber Risks in the Federal Administration.

In the globalised universe of cybersecurity, laws often have an extraterritorial effect. Foreign laws, such as the EU General Data Protection Regulation (*cf.* art. 3), may therefore have to be taken into account as well when assessing Incidents in Switzerland.

Provisions on cybersecurity may also include guidelines and standards. While generally non-binding, they may be taken into account when interpreting statutory provisions. They may also be declared binding by sector-specific associations or by reference in contracts. For example, the National Cyber Security Centre (NCSC) maintains an "Information security checklist for SMEs". The Federal Office for National Economic Supply (FONES) issued "Minimum standards for improving ICT resilience" for operators of critical infrastructures that may be adopted by interested private parties as well. Non-governmental initiatives include the Swiss Code of Best Practice for Corporate Governance and the International Organisation for Standardisation's ISO/IEC 27000 family of standards focusing on security of digital information, as well as its standard ISO/IEC 30141:2018 regarding IoT Reference Architecture.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Currently, there are no generally applicable mandatory cybersecurity requirements for critical or essential infrastructure and services. The regulation of cybersecurity for such infrastructure and services is fragmented and inconsistent, and it often lacks a precise definition of the required security measures (*cf.* question 4.2 below).

However, the need for further standardisation and regulation has been recognised in the NCS II, as adopted by the Federal Council on April 18, 2018. One of its focus areas remains the improvement of ICT resilience of critical infrastructures.

Accordingly, the 2018–2022 Critical Infrastructure Protection Strategy (CIP II) defines the overriding goals and principles of action for all parties involved, and identifies 17 measures to improve the country's resilience, *i.e.* its resistance, versatility and regeneration capacity, with regard to its critical infrastructures.

The CIP II lists the following nine critical infrastructures for Switzerland: financial and insurance services; healthcare; telecommunications; and public administration (set out in greater detail in question 4.2 below), as well as: public transport; energy; food supply; waste management; and public security.

The draft of a new Federal Information Security Act is currently before Parliament. It contains minimum requirements for the protection of information and IT infrastructure hosted by the federal authorities. The Ordinance on Protection against Cyber Risks in the Federal Administration entered into force on July 1, 2020. It regulates the organisation of the Federal Administration`s protection against cyber risks as well as the tasks and responsibilities of the various offices in the cybersecurity domain, in particular the NCSC (*cf.* question 8.1 below).

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Other than for critical or essential infrastructures and services (*cf.* question 2.2 above) and sector-specific regulations (*cf.* question 4.2 below), there are currently no specific legal requirements with respect to the measures listed above.

Their implementation may instead be driven by general legal requirements that, depending on the circumstances, may include the implementation of some or all of the above measures. They include, notably, the overall responsibility for the due management of a company and individual professional confidentiality obligations as well as data protection requirements. Guidelines and standards may also include provisions on cybersecurity. While generally non-binding, they may be taken into account when interpreting statutory provisions. They may also be declared binding by sector-specific associations or by reference in contracts (*cf.* questions 5.1 and 5.2 below).

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Currently, Switzerland knows no general obligation to report Incidents or potential Incidents to the authorities. However, the introduction of such an obligation is contemplated as part of the federal government's NCS II.

Except for serious security incidents in critical infrastructures, Incident reporting is currently encouraged on a voluntary basis, typically via the recently established NCSC which incorporates the former Reporting and Analysis Centre for Information Assurance (MELANI) and serves as a new national contact point (*cf.* question 8.1 below). Reports can be made through a message on the NCSC's website and can also be submitted anonymously. MELANI's statistics for 2019 show a continued high activity in all areas of cybersecurity risk.

Illegal activity on the internet can also be reported to the Cybercrime Coordination Unit Switzerland (CYCO) which may forward the matter to the competent domestic and foreign law enforcement authorities.

Sector-specific regulations for critical infrastructures regularly require the reporting of serious security incidents without delay. The scope of serious security incidents generally extends beyond, but may include, Incidents. More precise criteria may be specified in non-binding guidelines which explain the regulator's intended enforcement practice and are regularly accepted and complied with by the industry. Among the most prominent cybersecurity reporting obligations for critical infrastructures are those for financial and insurance services (*cf.* art. 29 para. 2 FINMASA; Financial Market Supervisory Authority (FINMA) Guidance 05/2020; FINMA Circular 08/25), healthcare (*cf.* art. 12 para. 3 Electronic Health Records Ordinance; art. 66 revised MedDO), as well as telecommunications (art. 96 para. 2 Ordinance on Telecommunication Services) (*cf.* question 4.2 below). The critical infrastructure reporting duties in the case of serious security incidents are currently under review by the Federal Council, and decisions are expected by the end of 2020.

A specific reporting obligation for Incidents relating to personal data will be introduced by the revised FADP. Data controllers will have to notify the Federal Data Protection and Information Commissioner (FDPIC) as soon as possible of data breaches that are likely to result in a high risk for the personality or the fundamental rights of data subjects. Correspondingly, data processors will have to inform the data controller as soon as possible of any data breach. A notification of the FDPIC must at least refer to the nature of the data breach, its consequences, and any measures taken or planned. In any subsequent criminal proceeding, the notification may only be used against the notifying company or person with their consent (art. 24 paras 1–3 and 6 revised FADP; *cf.* art. 7 revised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There is currently no specific requirement under the FADP to notify data subjects of an Incident. Depending on the seriousness of the data breach, however, such a requirement may arise under the general principle of data processing in good faith (art. 4 para. 2).

The revised FADP will explicitly require data controllers to inform affected data subjects of a data breach if it is necessary for their protection or if the FDPIC – after having been informed of the data breach (*cf.* question 2.4 above) – so orders (art. 24 paras 1, 4). Exceptions will apply in particular in cases of overriding public or private third-party interests or where reporting would be impossible or require a disproportionate effort (art. 24 para. 5 lit. a, b).

Further obligations to report Incidents or potential Incidents to affected individuals or third parties may derive from the generally required lawfulness of all data processing (art. 4 para. 1 FADP; art. 6 para. 1 revised FADP), as well as from specific contractual obligations.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Where applicable, the general Incident reporting is overseen by the NCSC, CYCO, FDPIC, and the cantonal Data Protection Commissioners.

Sector-specific reporting is overseen by the respective regulatory authorities, most notably by FINMA for financial and insurance services, by the Federal Office of Public Health (FOPH) for healthcare, and by the Federal Office of Communications (OFCOM) for telecommunications (*cf.* question 4.2 below).

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

For lack of a general reporting obligation for Incidents, there are currently no generally applicable penalties for non-compliance with reporting obligations.

Sector-specific sanctions may apply, such as in case of financial and insurance services, healthcare and telecommunications (*cf.* question 4.2 below). Under the revised FADP, object-specific sanctions will apply for violations of the minimum security requirements for personal data and for non-compliance with orders by the FDPIC (arts 8, 24, 61 lit. c, and 63).

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Cyber risks are a key part of the prudential supervision by FINMA, which has stepped up its efforts in the area. These risks are monitored directly, for example through focused on-site audits by FINMA, and monitored by audit firms as part of the regulatory audit process. In addition, larger institutions are regularly reminded of the need to take appropriate precautions against cyber risks during self-assessments. According to FINMA's Annual Report 2019, self-assessments in the second half of 2018 focused on the ability of the participating institutions to identify cyber threats arising from institution-specific vulnerabilities, perform a commensurate risk assessment and define countermeasures (threat intelligence). The outcome of the self-assessments was that most of the participating institutions had made adequate provision for those risks.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There is no law specifically allowing or prohibiting the use of beacons. However, companies which intend to use beacons for such purposes should analyse, in each case, whether their use is in compliance with Applicable Laws, including the SCC, the Unfair Competition Act and the FADP.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There is no law specifically allowing or prohibiting the use of honeypots. Companies should, however, keep the same regulations in mind as with beacons.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There is no law specifically allowing or prohibiting the use of sinkholes. The same considerations apply as with beacons and honeypots.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Organisations may monitor the electronic communication of their employees, provided that they comply with the provisions pertaining to the processing of personal data in the CO (art. 328b) and the FADP. Consequently, such monitoring must, in particular, be: carried out lawfully; in good faith; proportionate (*i.e.* suitable, necessary and affecting the data subject's privacy in the mildest possible way); and known to the data subjects.

Depending on the circumstances, the monitoring of employee data can be justified on the basis of the employment contract, industry-specific laws applicable to the employer (*e.g.* in case of banks) or the overriding interest of the employer to prevent or detect cyber-attacks. Relying on employee consent as justification for the processing, however, entails certain risks due to the usually limited ability of employees to refuse consent. Under the principle of transparency, employers are recommended to issue a monitoring regulation setting out the specifics of the surveillance measures.

Ordinance 3 to the Employment Act prohibits surveillance and monitoring systems which monitor the behaviour of employees (art. 26). Employers must ensure that the health of employees is not affected by the monitoring. However, a non-personal – anonymous or pseudonymous – evaluation of employee data is usually sufficient in order to prevent cyber-attacks, and it is, in principle, lawful under this provision, even if conducted systematically. In certain individual cases (*e.g.* after a cyber-attack), an individualised analysis of employee data may also be permissible.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

The Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods, as well as the respective Ordinance and Annexes, provide for certain import and export restrictions for dual-use goods, including technology and software. Annex 2, part 2, 4A005, 4D004 and 4E001.c set forth export restrictions for technology for the development of intrusion software, whereby certain exceptions exist with regard to vulnerability disclosures and reactions to cyber Incidents.

Moreover, according to Annex 2, part 2, 5A002, systems for information security and their components, including cryptographic technology for the confidentiality of data with a specific security algorithm, are subject to export restrictions.

Exceptions are available, such as for technology which is available to consumers, cryptographic technology for digital signatures, symmetric algorithms below 56 bit-encryption and many more. Furthermore, export restrictions may apply to equipment, and its components, for the interception and interruption of mobile communication and surveillance equipment (Annex 2, part II, 5A001.f), and to systems and equipment, and its components, for the surveillance of IP communication networks (Annex 2, part II, 5A001.j).

The Ordinance on the Export and Brokerage of Goods for Internet and Mobile Communication Surveillance must also be taken into consideration.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The Applicable Laws and market practice vary across the different business sectors in Switzerland. The NCS II has acknowledged the need for greater standardisation and regulation across the different sectors (*cf.* question 2.1 above).

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Financial and insurance services

The focus of cybersecurity regulation in Switzerland has traditionally been on its financial and insurance services sector.

Financial market infrastructures, as defined in art. 2 lit. a FinMIA (*e.g.* stock exchanges, multilateral trading facilities, payment systems), are obliged to operate IT systems that: ensure the fulfilment of the duties imposed by the FinMIA; are appropriate for the activities conducted; provide for effective emergency procedures; and ensure the continuity of the business activity (art. 14 FinMIA). Special IT systems requirements apply to financial market infrastructures with systemic importance in order to protect against the risks to the stability of the financial system (art. 23 FinMIA).

According to FINMA, cyber risks are among the most significant operational risks for banks and insurance companies. Accordingly, they are required to implement appropriate risk management measures to tackle operational risks, including cyber risks, and must safeguard their infrastructure against various types of attacks (art. 3f para. 2 Banking Act; art. 12 Ordinance on Banks; and the non-legally binding FINMA Circulars 2008/21 "Operational Risks – Banks" and 2017/2 "Corporate governance – insurers").

Supervised persons and entities must immediately report Incidents that are of substantial importance to the supervision to FINMA (art. 29 para. 2 FINMASA; FINMA Guidance 05/2020; FINMA Circular 08/25). Violations of the reporting obligations may face sanctions, including: a custodial sentence of up to three years or a monetary penalty for the wilful provision of false information or the omission of reporting to FINMA; a fine of up to CHF 250,000 in case of negligence (arts 45 *et seq.* FINMASA); and a revocation of the licence, a withdrawal of the recognition or a cancellation of the registration in case of serious infringements (art. 37 FINMASA).

Healthcare

Cybersecurity in the healthcare sector has recently received increased attention in Switzerland, in particular in view of the cybersecurity risks relating to the electronic patient record and medical devices connected to the internet.

The first electronic patient records are being certified in 2020. Certification requires a risk-based data security and data protection system, the technical and organisational specifications of which are defined by the FOPH. Relevant security Incidents have to be notified to the FOPH. The violation of these requirements may lead to a suspension or removal of the certification (art. 12 para. 1 lit. b Electronic Health Records Act; art. 12, 38 para. 1 Electronic Health Records Ordinance).

In line with the developments in the EU, in particular the Medical Devices Regulation 2017/745 of April 5, 2017 (MDR), Switzerland has revised its MedDO, the main provisions of which will enter into force on May 26, 2021. Accordingly, medical devices will have to fulfil the general safety and performance requirements in Annex I of the MDR, both with respect to hardware and software (art. 6 paras 1, 2 MedDO). Manufacturers of medical devices may have to notify severe Incidents as well as their corrective measures (art. 66 MedDO).

Telecommunications

Another emphasis of cybersecurity regulations lies on the telecommunications sector.

The OFCOM issued the non-binding "Directives on the security and availability of telecommunication infrastructures and services" (based on art. 96 para. 2 Ordinance on Telecommunications Services (OTS)). They specify security requirements and define minimum security levels which each telecommunication services provider should maintain in order to contribute to the reliability and availability of the national telecommunications network. With the revision of the TCA (date of entry into force not yet determined), a specific obligation to protect against cyber-attacks will be introduced (art. 48a revised TCA).

Telecommunications service providers are required to immediately inform the OFCOM of faults in the operation of their networks that affect a relevant number of customers (art. 96 para. 1 OTS). Such disturbances may also result from cyber-attacks. Failure to report may result in a fine not exceeding CHF 5,000 (art. 53 TCA).

Federal Administration

The draft of a new Federal Information Security Act is currently before Parliament. It contains minimum requirements for the protection of information and IT infrastructure hosted by the federal authorities.

The Ordinance on Protection against Cyber Risks in the Federal Administration entered into force on July 1, 2020. It regulates the organisation of the Federal Administration`s protection against cyber risks as well as the tasks and responsibilities of the various offices in the cybersecurity domain, in particular the NCSC (*cf.* question 8.1 below).

Other important sectors

Further sector-specific regulations apply, including for critical infrastructures. The NCS II and the 2018–2022 CIP II aim to implement measures to improve cybersecurity across various sectors on the basis of periodically updated risk and vulnerability analyses (*cf.* questions 2.1 and 2.2 above).

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

As a general principle, the primary responsibility for cybersecurity lies with the organisation (*cf.* question 5.2 below) rather than with the individuals entrusted with the task.

The board of directors, managing directors and executive officers of companies limited by shares, as well as the managing directors of limited liability companies, have a duty of loyalty and care and in particular a non-transferable and inalienable responsibility for the overall management of the company, the company's organisation, including accounting and financial controls, as well as the overall supervision of the persons entrusted with managing the company (arts 716a, 717, 810, 812 CO). Hence, the ultimate responsibility for the cybersecurity strategy of such companies, including the adoption of an appropriate organisation and of the necessary directives, processes and controls, lies with the respective management. In light of the increasing importance of cybersecurity, management must either have the requisite know-how itself or obtain relevant advice and cannot simply delegate the task to the IT department. Accordingly, if such companies suffer loss because of an Incident that results from an intentional or negligent breach of their duties, management may become personally liable both to the company and to the individual shareholders and creditors (arts 754, 827 CO).

The current FADP does not provide for sanctions for breaches of data security (art. 7). As of the expected entry into force of the revised FADP in 2022, however, the company's management or – if data security has been internally delegated – its data protection officer, IT manager or compliance officer may face fines of up to CHF 250,000 for intentional violations of the statutory minimum data security requirements (art. 8 para. 3, art. 61 lit. c.).

Criminal sanctions against individuals may also apply under various other, including sector-specific, laws, notably for intentional breaches of professional confidentiality (*e.g.* art. 35 FADP/ art. 62 revised FADP; arts 320 *et seqq.* SCC), but also at times for negligence (*e.g.* art. 47 Banking Act; arts 43, 53 TCA; art. 16 Product Safety Act).

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Other than for critical or essential infrastructures and services (*cf.* question 2.2 above) and in sector-specific regulations (*cf.* question 4.2 above), there are currently no specific legal requirements with respect to the IT security measures listed above. Their implementation may instead be driven by general legal requirements that, depending on the circumstances, may include the implementation of some or all of the above IT security measures. They include, notably, the overall responsibility for the due management of a company and individual professional confidentiality obligations (*cf.* question 5.1 above) as well as data protection requirements.

Privacy by design requires that the confidentiality, availability, and integrity of personal data must be protected through adequate technical and organisational measures, taking into account the purpose, nature, and extent of the data processing, the possible risks and the current state of the art. The measures must be reviewed periodically. More specific requirements apply for the automated processing of personal data (arts 7 FADP and 8 *et seq.* Ordinance to the FADP; arts 7, 8 revised FADP). The revised FADP will introduce additional obligations to maintain an inventory of processing activities and to conduct privacy impact assessments (arts 12, 22).

Beyond the applicable regulations, guidelines and standards may also include provisions on cybersecurity (*cf.* question 2.1 above). While generally non-binding, they may be declared binding by sector-specific associations or by reference in contracts. They may also be taken into account when interpreting statutory provisions. For example, manufacturers of data-processing systems or programs, as well as private persons or federal bodies that process personal data, may obtain a data protection certification (art. 11 FADP). The applicable standard in such cases is ISO/IEC 27001:2013.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There is currently no specific requirement under the FADP to notify the public of an Incident. Depending on the seriousness and on the number of affected data subjects, however, the general principles of lawful and good-faith data processing (art. 4 paras 1, 2 FADP; *cf.* also art. 6 paras 1, 2 revised FADP) may require an Incident to be reported publicly (*cf.* questions 2.4, 2.5 above). This option is explicitly foreseen in the revised FADP (art. 24 para. 5 lit. c).

If Incidents or cybersecurity risks lead to the expectation of a future cash outflow, a company may be required to book the probably required provisions and charge them to the profit and loss account (*cf.* art. 960e CO or other applicable financial reporting standards).

Companies listed on the SIX Swiss Exchange are subject to specific periodic disclosure requirements (art. 49 *et seq.* Listing Rules (LR)). They may also have to consider whether an Incident amounts to a qualified reportable event and, hence, triggers *ad hoc* publicity obligations (art. 53 LR; Directive on *Ad Hoc* Publicity). Whether an Incident represents a qualified reportable event has to be assessed on a case-by-case basis, considering whether it has a substantial impact on the development of a company's share price and therefore has the potential to influence average investors in their investment decision.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Liability is a key consideration in cybersecurity. While legally possible, civil action against cybercriminals will regularly prove unfeasible. In practice, the focus is therefore on secondary liability: entities affected by an Incident may turn to the provider of a defective product or service; and third parties suffering damage from the Incident may look to the affected organisation for having failed to comply with appropriate data security standards.

In case of a contractual relationship that contains a respective IT security representation, the third party (client, supplier,

etc.) can bring a contractual liability claim against the organisation affected by the Incident, provided it can demonstrate a breach of contract, damage, causation as well as fault (arts 97 *et seqq.* CO). The latter is generally presumed, which is why it is for the defendant to prove that it was not at fault with respect to the Incident. Special contractual liability provisions may provide for strict liability, such as in case of direct losses caused to a buyer (art. 208 para. 2 CO).

If there is no IT security representation, the defendant's fault will be assessed against a standard of due care and the related threshold question of what level of cybersecurity is reasonable and appropriate to avert damage from a third party, taking into account the level of risk, applicable industry standards, and the state of technology.

General commercial terms often contain liability limitations for third-party actions and consequential damages. It is questionable whether such general terms would be upheld in the event of an Incident, and any advance exclusion of liability for gross negligence would in any case be void (art. 100 para. 1 CO). Difficult questions may also arise where a multitude of parties contribute, albeit unintentionally, to an Incident.

For liability based on tort, or other civil wrongs independent of contract, *cf.* question 6.3 below.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There is no published case law in relation to Incidents for a failure to comply with appropriate data security standards or the delivery of defective security products or services.

Since Swiss law currently remains unfriendly to mass claim proceedings, data subjects affected by a security breach will, in most cases, encounter difficulties in asserting financial damages in an amount that merits a claim.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

In the absence of a contractual relationship (*cf.* question 6.1 above), entities may incur liability in tort, or another civil wrong independent of contract, for the harm that an Incident causes to third parties, irrespective of contractual disclaimers or limitations of liability.

General tort law provides relief for damages caused by an illicit act, whether wilfully or negligently (such fault not being presumed; arts 41 *et seqq.* CO). An illicit act exists in case of a breach of an absolute right of the victim (personality, intellectual property or similar rights) or a financial damage resulting from the breach of a specific legal provision that is designed to protect against such damage, which must be determined on a case-by-case basis. Disgorgement of profits arising from a cyber-attack may be sought based on unjust enrichment or on agency without authorisation (arts 62 *et seqq.*, 423 CO).

In the software and IoT context (*e.g.* hacked medical devices, cars, etc.), product liability rules may be of particular relevance: If a defective product, which does not provide the safety that would reasonably be expected, leads to an Incident, the manufacturer, importer or supplier is, in principle, strictly liable for personal injuries and damage to privately used property caused by the product (arts 1, 4 Product Liability Act).

If a company limited by shares or a limited liability company suffers loss because of a severe data breach that results from a lack of appropriate internal cybersecurity controls and procedures, the respective board members, managing directors and executive officers may become personally liable to both the company and the individual shareholders and creditors for any loss or damage arising from an intentional or negligent breach of their duties (arts 754, 827 CO; *cf.* question 5.1 above).

To the extent an Incident due to insufficient data protection or data security leads to a violation of personality rights, such as in case of data theft or illegal data processing, affected persons may bring an action seeking, *e.g.* damages, moral compensation, disgorgement of profits, injunctions and notification to third parties or publication (art. 15 para. 1 FADP/art. 32 para. 2 revised FADP; arts 28 *et seqq.* Civil Code; arts 41 *et seqq.*, 49, 423 CO).

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Organisations in Switzerland are permitted to take out insurance against Incidents, and insurers have offered cyber products for a number of years already. The respective offerings often close a coverage gap as many property and liability insurance policies exclude cyber risks.

Cyber insurance solutions are very much customised and can include almost every cyber risk, including denial-of-service and ransomware attacks, costs of internal investigations and crisis management, recovery of stolen, destroyed or damaged data, reputational damage, and the defence against third-party claims. The implementation of a customary and up-to-date cyber risk management and respective protective measures are a necessary condition of admission and coverage under many cyber insurances. Unless contractually excluded, art. 14 para. 2 Insurance Contract Act entitles the insurer to reduce its coverage in case of gross negligence of the insured.

In addition to the high degree of customisation, many key coverage terms have not been analysed by the courts, and cyber risks are complicated and constantly evolving. Accordingly, foreign cases such as *Mondelez International, Inc. v. Zurich American Insurance Co.*, No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct., Oct. 10, 2018) are also monitored closely in the jurisdiction.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are not.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Switzerland does not have a central enforcement agency for cybercrimes. Instead, prosecution of the various cybercrimes lies with the competent police departments and public prosecutors' offices on cantonal and federal level. Equally, while reporting duties for serious security events, including Incidents, exist for critical infrastructures such as finance and insurance,

healthcare and telecommunications, there is currently no general and specific duty to notify cybersecurity breaches (*cf.* question 2.4 above).

The NCSC, headed by the Federal Cyber Security Delegate, is Switzerland's new cybersecurity competence centre (*cf.* Ordinance on Protection against Cyber-Risks in the Federal Administration of July 1, 2020). Its aim is to enable the Confederation to play a more active role in protecting the country against cyber risks by supporting the general public, businesses and educational institutions as well as public administrations in their protection against cyber risks, by improving the security of the Federal Administration's own infrastructure. MELANI, together with the national Computer Emergency Response Team (GovCERT), have been integrated into the NCSC as a national contact point and technical expertise hub. Incident reporting to MELANI is voluntary. Upon receipt of a report, MELANI will analyse it and provide assessments and recommendations. MELANI can adopt an active lead role where an Incident jeopardises the proper functioning of the Federal Administration.

The CYCO at the Federal Office of Police (FEDPOL) is Switzerland's central office for anyone who wishes to report illegal activity on the internet. It also actively investigates illegal internet activity. The CYCO does not prosecute the matters itself but, after a first review and data backup, passes them on to the competent domestic and foreign law enforcement authorities.

Switzerland is a member of the Budapest Convention on Cybercrime. Besides committing its member states to increase their national efforts to effectively fight cybercrime, the Convention fosters an increased, rapid, and well-functioning international cooperation.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there are not.

Dr. Oliver M. Brupbacher is a partner at Kellerhals Carrard. He represents clients in litigation and arbitration in commercial matters as well as in investigations. He specialises in healthcare and life sciences, cross-border proceedings and mutual legal assistance, as well as data protection and information governance. He also advises clients on cybersecurity prevention and crisis management. As a former Senior Litigation Counsel, Head of Global Discovery and a global product lawyer at Novartis, Oliver Brupbacher combines deep expertise in his areas of practice with an intimate understanding of the industry and of clients' needs at all organisational levels, in both domestic and international contexts.

Kellerhals Carrard
Henric Petri-Strasse 35
P.O. Box 257 CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: oliver.brupbacher@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

Dr. Nicolas Mosimann is a partner at Kellerhals Carrard. His practice focuses on M&A, corporate law, technology and intellectual property law and commercial law. He advises both Swiss and international companies and institutions on transactions (*e.g.* acquisitions, joint ventures, financing rounds, licences and outsourcing) and technology projects (*e.g.* IoT and blockchain-based platforms), research and cooperation agreements, commercial contracts and data protection (including the EU GDPR). In addition, Nicolas specialises in advising both providers and customers on software (from development to protection and licensing, including SaaS and open source software) and cloud projects. Moreover, as a founding member and co-head of the Startup Desk of Kellerhals Carrard, Nicolas knows the needs of founders and their companies in the seed and growth phases.
As a long-time member of AIJA, Nicolas has an excellent international network, and advises clients across a range of industries and sectors, such as IT, technology, life-sciences, advertising and arts and entertainment, throughout the world.

Kellerhals Carrard
Henric Petri-Strasse 35
P.O. Box 257 CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: nicolas.mosimann@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

Marlen Schultze is an associate at Kellerhals Carrard. She has extensive experience in criminal law and criminal procedural law, with a focus on white-collar crime, the prevention of corruption and money laundering and international mutual assistance in criminal matters. In addition, she advises clients on compliance, conducts internal investigations and advises and represents clients in domestic and international litigation and arbitration.

Kellerhals Carrard
Henric Petri-Strasse 35
P.O. Box 257 CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: marlen.schultze@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

With more than 200 legal professionals (consisting of partners, of counsels, associates, tax advisors and notaries) and more than 300 employees, the firm, which has its origins in 1885, is one of the largest and most traditional law firms in Switzerland, with offices in Basel, Bern, Geneva, Lausanne, Lugano and Zurich, and representative offices in Binningen, Sion, Shanghai and Tokyo.
Kellerhals Carrard is active throughout Switzerland, maintaining very strong local roots, whilst advising clients nationally and abroad.
Kellerhals Carrard advises and represents companies and entrepreneurs from all industries and economic sectors, public authorities, national and international organisations and private individuals before all judicial and administrative bodies nationally and abroad in practically all areas of the law. Our activities are focused on:

- Company and corporate law, external legal department.
- Litigation, arbitration and insolvency law.
- M&A and capital markets law.
- Regulatory financial markets law, financial services, collective investments, leasing, insurance.
- IT/IP, distribution, competition and anti-trust law.
- International sports law.
- Tax.
- Public law.
- Employment and social insurance law.
- Commercial criminal law and international mutual assistance/compliance.
- Family and inheritance law for private customers.
- Notarial office.
- Kellerhals Carrard focuses in particular on the areas of financial services, life sciences, IMT (Information, Technology and Media), sport, energy, real estate/construction, as well as on trading and retail.

www.kellerhals-carrard.ch

Taiwan

Lee and Li, Attorneys-at-Law

Ken-Ying Tseng

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Pursuant to Article 358 of the ROC Criminal Code, a person who breaks into someone else's computer or related equipment by entering another's account code and password without authorisation, breaking into the protection measure, or taking advantage of a loophole of such system shall be sentenced to imprisonment for no more than three years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of no more than NTD300,000 may be imposed. Hacking, i.e., the unauthorised access of another's system, is likely to be deemed as constituting such an offence.

Denial-of-service attacks
Pursuant to Article 360 of the ROC Criminal Code, a person who, without authorisation, interferes with the computer or related equipment of another person and causes injury to the public or another through the use of computer programs or other electromagnetic methods shall be sentenced to imprisonment for no more than three years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of not more than NTD300,000 may be imposed. "Denial-of-service attacks" may be deemed as such unauthorised interference of another's computer system and may be subject to the above criminal sanctions.

Phishing
Pursuant to Article 359 of the ROC Criminal Code, a person who, without authorisation, obtains, deletes or alters the magnetic record of another's computer or relating equipment and causes injury to the public or others shall be sentenced to imprisonment of no more than five years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of no more than NTD600,000 may be imposed. "Phishing" in general refers to the activities of obtaining someone else's important information, such as account number and password, or personal information by using the internet, which may constitute the above offence if injury to the public or others is caused.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware may be deemed as interfering with another's computer system and altering the records in another's computer system without authorisation and may be deemed as the offences as set forth under Article 360 and/or Article 359 of the ROC Criminal Code and may be subject to the criminal sanctions as set forth above.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Pursuant to Article 362 of the ROC Criminal Code, a person who makes computer programs specifically for themselves or another to commit the offences specified as set forth under Articles 358 to 361 of the ROC Criminal Code and causes injury to the public or another shall be punished with imprisonment of no more than five years or short-term imprisonment; *in lieu* thereof, or in addition thereto, a fine of no more than NTD600,000 may be imposed. The mere distribution, sale or offering of software that may be used to commit cybercrime may not be deemed as constituting the offence as set forth under Article 362 of the Criminal Code. Whether a person will be held criminally liable with regard to possessing such software will depend on the actual activities that the person conducts by possessing or using such software.

Possession or use of hardware, software or other tools used to commit cybercrime
Please see above.

Identity theft or identity fraud (e.g. in connection with access devices)
Depending on how the identity information is stolen, the activity to obtain the identification information may constitute either the offence set forth under Article 358 or Article 359 of the ROC Criminal Code as set forth above. As for using another's identity for fraud purposes, it may constitute either the general criminal offence concerning "fraud" activity as set forth under Article 339 of the ROC Criminal Code or depending on the factual situation, constitute the criminal offence set forth under Article 339-3 of the ROC Criminal Code, which stipulates that a person who for the purpose of exercising unlawful control over other's property for themselves or for a third person takes the property of another by entering false data or wrongful directives into a computer or relating equipment to create the records of acquisition, loss or alteration of property ownership shall be sentenced to imprisonment for no more than seven years; in addition thereto, a fine of no more than NTD700,000 may be imposed. Tricking an auto-machine, such as an ATM, by stealing someone else's identity is another criminal offence under the ROC Criminal Code. Pursuant to Article 339-2, such activity may incur criminal sanction, such as imprisonment for no more than three years and/or a criminal fine of no more than NTD300,000. Whether the activities concerning identity theft or identity fraud would

constitute any other criminal offence shall depend on the actual activity that was conducted.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Under Taiwan law, either infringing another's copyright or trade secret may incur criminal liabilities. In addition, an individual breaching the confidentiality obligations that he/she was imposed during his/her prior employment relationship with his/her former employer may incur civil liability for breach of contract. If the confidential information constitutes a trade secret of the former employer, the individual may be subject to a criminal sanction of up to five years' imprisonment or short-term detention, and a criminal fine ranging from NTD1 million to NTD10 million may be imposed. If the purpose of the infringement of a trade secret is for the trade secret to be implemented or exercised in the PRC, Hong Kong or Macau, the individual may be subject to imprisonment of one to 10 years and a criminal fine of NTD3 million to 50 million may be imposed. As for infringing another's copyright, depending on the actual infringement being conducted, the amount of the criminal fine may be as high as NTD5 million, and the length of imprisonment may be as long as five years.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Depending on the relevant facts, such activity may be deemed as constituting one or more criminal offences as listed above.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Depending on the actual fact concerning such activity, such activity may be deemed as constituting one or more criminal offences as listed above. For example, in 2016, a group of Russians and Eastern Europeans hacked into the system of a Taiwan bank from London and remotely accessed and controlled certain ATMs of the Taiwan bank located in Taiwan and obtained cash from the machines. The individuals came to Taiwan to collect the cash, which was then seized by the Taiwan police, while the hackers outside of Taiwan remain untouched. The Russian and Eastern Europeans who were seized by the Taiwan law enforcement authorities were sentenced to criminal sanctions including imprisonment for having committed almost all of the above-mentioned criminal offences.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The relevant statutes do not "spell out" any extraterritorial application but whether those will have extraterritorial application shall be subject to the general provisions under the ROC Criminal Code. If the relevant actions cause any consequence in Taiwan or one of the elements of the actions is conducted in Taiwan, the Taiwan court will have jurisdiction over such offences and the ROC Criminal Code will become applicable.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The relevant statute does not stipulate any specific reporting or notification mechanism that can exempt the offender from the relevant penalties. It seems that other than "surrendering himself/herself" to the law enforcement authority, there is no other mechanism that can reduce the criminal liability.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The following Taiwan statutes may be relevant to cybersecurity:
1. Cybersecurity Management Act;
2. Personal Data Protection Act ("PDPA");
3. Criminal Code (the relevant offences in regard to computer crime and fraud, etc.);
4. Communication Security and Surveillance Act;
5. Trade Secret Act;
6. Copyright Act;
7. Patent Act;
8. National Security Act;
9. Counter-Terrorism Financing Act; and
10. Regulation Governing Export and Import of Strategic High-Tech Commodities.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes. On June 6, 2018, the very first cybersecurity legislation of Taiwan, the Cybersecurity Management Act, became an official statute of Taiwan and took effect on January 1, 2019. The Cybersecurity Management Act imposes cybersecurity obligations on the government agencies, as well as the "specific non-government agencies", which includes the critical infrastructure providers. Private businesses in the following businesses may be designated by the government as critical infrastructure providers and may therefore be subject to the Cybersecurity Management Act: energy; water resources; communications; transportations; finance; hospitals; and high-tech parks.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Cybersecurity Management Act requires Taiwan government agencies as well as the specific non-government agencies to adopt cybersecurity maintenance plans and report any cybersecurity Incident to the relevant government authorities. Each of the competent authorities has issued guidelines for adopting cybersecurity plans in this regard for the reference of the businesses that are subject to their jurisdictions. In such guidelines, general security standards, including ISO27001, were referred to and recommended. Although, in such general securities standards, there is no reference to the specific obligation that shall be imposed on a government agency or a non-government agency with regard to the monitoring, detecting, preventing or mitigating the occurrence of any Incidents, reference to implementing anti-virus measures or adopting periodical checks on

the security procedures were made. In sum, the obligations that a government agency or a specific non-government agency is imposed with are a general security obligation.

With regard to personal data protection, a private organisation is required to take proper security measures to protect the personal data that it holds so that the personal data will not be stolen, altered, damaged, or lost. The competent authority of each industry has the power to require the private organisations under its jurisdiction to stipulate personal data file security maintenance plans.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Pursuant to the Cybersecurity Management Act, the agencies subject to the Cybersecurity Management Act shall report to their supervisory agency or to the competent authority of the industry that the private agency is engaging in as applicable when the agency becomes aware of a cybersecurity Incident. A cybersecurity Incident refers to any Incident under which the system or information may have been accessed without authorisation and used, controlled, disclosed, damaged, altered, deleted, or otherwise infringed, affecting the function of the information communication system and thereby threatening the cybersecurity policy.

The "Regulations for Reporting and Responding to Cybersecurity Incidents" set forth further details about the reporting of a cybersecurity Incident as required under the Cybersecurity Management Act. A "specific non-government agency" shall report to its regulator at the central government within "one hour" after it becomes aware of the cybersecurity Incident and the regulator shall respond within two to eight hours depending on the classification of the cybersecurity Incident. Meanwhile, the specific non-government agency shall complete damages control or recovery of the system within 36 to 72 hours depending on the classification of the cybersecurity Incident.

When making such a report to the authority, descriptions such as the time when the Incident occurs and when the agency becomes aware of the Incident, what had actually happened, the assessment of the risk level, the responsive measures that have been taken; the evaluation of any assistance from outside resources; and other relevant matters shall be included.

There are no specific provisions with regard to exemption of the reporting requirements, and it is not necessary for the authority to make such report publicly available.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

There are no such legal requirements under the Cybersecurity Management Act. However, under the Personal Data Protection Act, if there is any data breach Incident, a data controller shall notify the affected data subjects after it has the opportunity to inspect the relevant Incident. In the notification to the data subjects, the data controller shall briefly describe the data breach Incident and the corrective measures that the data controller has taken to protect the data subjects.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The sectoral regulators at the central government level in Taiwan are in charge of enforcing the relevant matters with regard to cybersecurity matters. With regard to personal data protection, either the sectoral regulators at the central government level or the municipal governments have the power to enforce the PDPA.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

With regard to cybersecurity, a private organisation that has been designated as a provider of the critical infrastructure may be ordered to take corrective measures by a certain deadline or it may be imposed with an administrative fine ranging from NTD100,000 to NTD1 million for its failure to comply with the obligations to (i) stipulate the relevant cybersecurity management plan, (ii) stipulate the responsive measures which should be taken in a cybersecurity Incident, or (iii) report the Incident to the relevant authority or submit the relevant investigation report, etc. and may be imposed with such fine consecutively until correction measures are taken.

With regard to a personal data breach Incident, if a private organisation fails to take proper security measures to protect the personal data that it retains or breaches its obligation to notify the data subjects affected by the personal data breach Incident, the competent authority has the power to order the private organisation to take corrective measures, and if no corrective measure is taken before the designated deadline, the authority has the power to impose an administrative fine ranging from NTD20,000 to NTD200,000 consecutively until corrective measures are made.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

As the Cybersecurity Management Act was recently implemented, thus far, no enforcement examples have been found.

As for the PDPA, given that the enforcement power lies in the competent authority in charge of each different industry and there are no comprehensive methods to search such precedents, it is difficult to evaluate the level of the actual enforcement of each authority. The Financial Supervisory Commission (the "FSC"), however, has made the relevant enforcement decisions, which are online for public access. Based on the search in the FSC's database, there have been quite a few financial institutions being imposed with administrative fines for their failure to adopt proper security measures to protect the personal data that they retain or failure to notify the affected data subjects with regard to particular security Incidents.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There is no specific law or statute permitting or prohibiting an organisation from taking such a measure to protect its IT system. We believe that as long as the implementation of such technology will not be deemed as one of the criminal offences as described under section 1 above, an organisation shall be permitted to take such a measure.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There is no specific law or statute permitting or prohibiting an organisation from taking such a measure to protect its IT system. We believe that as long as the implementation of such technology will not be deemed as one of the criminal offences as described under section 1 above, an organisation shall be permitted to take such a measure.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
There is no specific law or statute permitting or prohibiting an organisation from taking such a measure to protect its IT system. We believe that as long as the implementation of such technology will not be deemed as one of the criminal offences as described under section 1 above, an organisation shall be permitted to take such a measure.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes. Employee monitoring practices are permitted if (i) the employees no longer have a reasonable expectation of privacy, and (ii) such monitoring is not expressly prohibited by law. Employees are deemed not to have a reasonable expectation of privacy if their employer has expressly announced the monitoring policy and/or employees have consented to the monitoring. Furthermore, employees are deemed to have given an implied consent if they continue to use the equipment provided by the employer after the employer has announced the monitoring policy.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Taiwan follows the same practice of the international society with regard to the restriction on importation and exportation of encryption technology. We basically follow the principles set forth by the relevant international organisations, such as the "Nuclear Suppliers Group", the "Australia Group", as well as the relevant international conventions, such as "the Wassenaar Arrangement" and the "Chemical Weapons Convention".

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, different sectors implement different standards. For example, the regulators of the financial industry stipulate quite a few information security requirements and standards with specific security requirements, while the regulators of other industries may stipulate only general standards.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

With regard to the financial industry, there are various information security regulations and rulings requiring the financial institutions to take sufficient cybersecurity measures so as to protect their customers. For example, there are specific security standards for securities firms to offer "online" trading services to their customers, for banks to offer "online" banking services to their customers, and for insurance companies to offer insurance policies online.

As for the telecommunications sector, the competent authority, i.e., the National Communications Commission ("NCC"), also stipulates the relevant information security standards and measures and requires the telecommunications operators to adopt and follow the standards. The NCC also took certain measures to encourage telecommunications operators to maintain their information security, such as holding training sessions and seminars.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Directors bear "fiduciary duty" to the company and will be held liable when they breach such duty to the company. A company's failure to prevent, mitigate, manage or respond to an Incident may not necessarily lead to the conclusion that their directors have breached their fiduciary duty. Under Taiwanese

law, directors are in charge of making business decisions for a company by forming the joint decision of the board, but they are not responsible for implementing any business decisions or the daily operation of the company. With regard to cybersecurity Incidents, it would depend on the internal rules of a company as to whether such an Incident shall be reported to the board of directors. If the management has reported an Incident to the board of directors pursuant to the internal rules, but the board of directors fails to take proper action to address or resolve the Incident or even try to conceal or cover the Incident, the board of directors may be held liable.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

It is not mandatory under Taiwanese law for a company to designate a CISO. Other than the specific non-government agency as designated by the relevant competent authority or the regulated companies, such as financial institutions or telecommunications operators, a company is not legally required to stipulate a written Incident response plan or policy, conduct periodical cyber risk assessments, or perform penetration tests or vulnerability assessments.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, unless such risks or Incidents are major or material to the operation of a listed company.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

In an Incident under which the computer system of a private organisation was hacked or invaded by others and the private organisation therefore suffered loss or damage, the private organisation, being the victim of the Incident, may file a civil lawsuit against the hacker or the other relevant wrongdoers either based on a tort claim or an unjustified enrichment claim, especially if there have been criminal proceedings launched against the hacker or the relevant wrongdoers at the same time. The private organisation, being the plaintiff, needs to establish the facts with regard to how the system was attacked, invaded or altered and how such activities can be linked to the hacker or the wrongdoers. The private organisation will also be required to substantiate the amount of the actual damage and the causation between the occurrence of the actual damage and the hacking activities.

Such a private organisation should also be able to file a civil action against the vendor that provided the IT/cybersecurity services to the private organisation if the vendor has failed to perform the required services or has failed to meet the required security standard. In this regard, the private organisation is required to establish that the vendor bears such an obligation to provide it with a security service meeting a certain level or standard based on the relevant contract as well as substantiate the actual amount of the damage.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

Since 2016, there have been quite a few "business email compromise" ("BEC") Incidents and many civil lawsuits were filed with the Taiwan court. Many of the cases involve a cross-border BEC scheme, under which a foreign company sought civil relief at the Taiwan court against individuals in Taiwan. Such individuals offered their bank accounts as the nominee accounts to receive the improper funds for the real hackers and their identities were discovered through the records in the banking system. The Taiwan law enforcement authority then worked with the foreign law enforcement authority to seize the nominee accounts and track down the individuals offering the nominee accounts. The nominee account holder would be held criminally liable under Taiwan law, either for being the accomplice of the hacker or breaching the Money Laundering Control Act. The victim would then bring a civil lawsuit against the nominee account holder. There are also court cases under which the nominee account holders were not found or criminally indicted but still the court ruled in favour of the victims against the nominee account holders and declared that the nominee account holders shall return the improper gain to the victims.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Under the PDPA, where a company fails to take proper security measures and thus causes the illegal disclosure of the personal data files they keep, they may be held civilly liable by the affected data subjects; this civil liability is by nature a tort liability under Taiwan law. In respect of the application of the general tort theory against a company that failed to prevent an Incident, this shall be determined on a case-by-case basis.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, they are permitted.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no such regulatory limitations.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

If the police suspect or become aware of a certain crime being conducted in relation to an Incident, the police have the power to conduct an investigation of the suspect by requiring the suspect or third party to provide the relevant "information" to the police. If the police intend to seize the hardware or devices, the police would need to prepare all collected evidence for the prosecutor and request the prosecutor to apply with the court for the issuance of a search warrant to seize the hardware or devices. The court will review the warrant application submitted by the prosecutor. If the evidence collected by the police meets the standard of probable cause, the court, in most cases, would issue the search warrant.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such specific statutes under Taiwan law.

Ken-Ying Tseng established and currently heads Lee and Li's personal data protection practice group. Prior to 2018, she was the head of Lee and Li's M&A practice group for 12 years. She received an LL.M. from Harvard Law School. Ken-Ying advises on various forms of mergers and acquisitions, and is experienced in resolving both legal and commercial issues. She assisted and represented several multinational corporations in their M&A activities, including BASF, Henkel, Yahoo!, Arrow, Bureau Veritas, Aleees, Sony, Micrel, Energy Absolute, Qualcomm and McDonald's, among others.

In addition to M&A, Ken-Ying constantly advises various tech companies that are in the businesses of social networks, instant messengers, search engines, portal sites, sharing economy, e-commerce, OTT, online gaming, P2P lending, e-payments, cloud computing, and so on. Ken-Ying also frequently advises clients, including multinational companies, on privacy and data protection (GDPR), e-marketing, big data, e-signature, domain name, telecommunications, satellite, fintech, cybersecurity, Internet governance, and other legal issues.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000
Email: kenying@leeandli.com
URL: www.leeandli.com

Lee and Li, Attorneys-at-Law is a full-service law firm and the largest law firm in Taiwan. Its history can be traced back to the 1940s. Lee and Li has formed practice groups which span corporate and investment, banking and capital markets, trademark and copyright, patent and technology, and litigation and ADR. Its services are performed by over 100 lawyers admitted in Taiwan and more than 100 technology experts, patent agents, patent attorneys, and trademark attorneys. Lee and Li was recognised as the 'Taiwan Firm of the Year' or the 'National Law Firm of the Year' by *IFLR* in 2001–2019. Lee and Li has also been recognised by other international institutions as the best law firm in the region, including, *Who's Who Legal*, *China Law & Practice*, *Leaders League*, *Chambers and Partners*, *Asialaw* Regional Awards, etc.

www.leeandli.com

Thailand


Supawat Srirungruang


Saroj Jongsaritwang

R&T Asia (Thailand) Limited

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Yes. The Computer Crime Act B.E. 2550 (2007) ("**CCA**") provides that whoever illegally accesses a computer system that has specific security measures and such security measures are not intended for that person's use shall be liable for imprisonment not exceeding six months and/or a fine not exceeding THB 10,000 (CCA, s.5).

Whoever illegally accesses computer data that has specific security measures which are not intended for that person's use shall be liable for imprisonment not exceeding two years and/or a fine not exceeding THB 40,000 (CCA, s.7).

With regard to the personal data, the data processor and data controller are obligated under the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") to provide appropriate security measures for preventing unauthorised or unlawful loss, access to, use, alteration, correction or disclosure of personal data. Failure to do so may result in an administrative fine of up to THB 3 million (PDPA, ss83 and 86).

Denial-of-service attacks
Yes. Whoever illegally acts in a manner that causes suspension, deceleration, obstruction or interference to a computer system of another person so that it is not capable of functioning normally shall be liable for imprisonment not exceeding five years and/or a fine not exceeding THB 100,000 (CCA, s.10).

Phishing
Yes. Whoever dishonestly or deceitfully inputs into a computer system computer data which is distorted or forged, either in whole or in part, or computer data which is false, in such a manner likely to cause injury to the general public which is not the offence of defamation under the Criminal Code, shall be liable for imprisonment not exceeding five years and/or a fine not exceeding THB 100,000 (CCA, s.14(1)).

Where the offence above is not committed against the general public but rather against a person, the offender shall be liable for imprisonment not exceeding three years and/or a fine not exceeding THB 60,000; and such offence shall be deemed a compoundable offence.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Yes. In addition to the above, whoever illegally acts in a manner that damages, destroys, alters, amends, or makes additions to, either in whole or in part, computer data of another person shall be liable for imprisonment not exceeding five years and/or a fine not exceeding THB 100,000, or both (CCA, s.9).

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Yes. A person who distributes or disseminates a computer program created specifically for the purpose of committing the offences specified shall be subject to imprisonment not exceeding two years and/or a fine not exceeding THB 40,000. Moreover, where there is a person who uses such computer program to commit an offence specified, the person who distributes or disseminates such computer program shall also be liable for a higher degree of penalty if he or she knew or might have been aware of the consequences that have occurred (CCA, s.13).

Possession or use of hardware, software or other tools used to commit cybercrime
Yes. Under the CCA, where the court orders to destroy any computer data (including software), any person knowing that the computer data in his/her possession is the computer data that is subject to such court order must destroy such computer data. Failing to do so may result in a criminal penalty of up to two-and-a-half years of imprisonment and/or a fine of up to THB 100,000, depending on the relevant offence (CCA, s.16/2).

In addition, the competent officials may order a person who possesses or controls the computer data or equipment which stores the computer data, to deliver the computer data or such equipment to the competent official as deemed necessary for the benefit of using it as evidence in order to establish that the offence has been committed, and to find the whereabouts of the offender. Whoever fails to comply with such order of the competent official shall be liable for a fine not exceeding THB 200,000 and a daily fine not exceeding THB 5,000 until the order is properly complied with (CCA, s.18(5) and s.27).

Identity theft or identity fraud (e.g. in connection with access devices)
Yes. Pursuant to Section 342(1) of the Criminal Code, identity theft/fraud would be considered as the offence of cheating and fraud committed by the offender showing himself or herself to be another person, and is subject to imprisonment not exceeding five years and/or a fine not exceeding THB 100,000, or both.

Section 269/5 also provides that whoever illegally uses the electronic card of another person in a manner likely to cause damage to other person(s) or people shall be liable for imprisonment not exceeding five years and/or a fine not exceeding THB 100,000, or both.

Identity theft/fraud would also be considered as the act of causing damage to the computer data of another person under the CCA (CCA, s.9). In addition, whoever inputs into a publicly accessible computer system computer data that will appear as an image of the other person and the image has been created, edited, appended or adapted by electronic means or whatsoever means, and in doing so is likely to cause such other person to be defamed, denounced, detested or humiliated, shall be liable for imprisonment not exceeding three years and/or a fine not exceeding THB 200,000 (CCA, s.16).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

There are no specific laws for electronic theft in Thailand. However, criminal copyright infringement usually constitutes an offence under the Copyright Act B.E. 2537 (1994).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

There are no specific laws for penetration testing. Given that a penetration test is a simulated cyber-attack on the designated system, unsolicited penetration testing without permission of the system owner may be considered unauthorised access to a computer system or computer data. Please see our comments regarding hacking in question 1.1 above for details.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Yes. Under the CCA, if a person who has knowledge of the security measures to access a computer system specifically created by another person illegally discloses such security measures in a manner that is likely to cause damage to another person, such person shall be liable for imprisonment not exceeding one year and/or a fine not exceeding THB 20,000 (CCA, s.6).

A person who illegally makes, by any electronic means, an interception of computer data of another person that is being transmitted in a computer system and such computer data is not for the benefit of the public or is not available for other persons to utilise would be liable for imprisonment not exceeding three years and/or a fine not exceeding THB 60,000 (CCA, s.8).

A person who sends computer data or an electronic mail to another person while hiding or faking its source(s), in a manner that interferes with such other person's normal utilisation of the computer system shall be liable for a fine not exceeding THB 100,000. Further, if the person sends computer data or electronic mail to another person in a manner that disturbs the recipient, without giving the recipient an easy opportunity to cancel or notify his/her wish to deny receipt of such computer data or electronic mail, such person shall be liable for a fine not exceeding THB 200,000 (CCA, s.11).

In case the commission of the above offences is associated with computer data or a computer system that relates to national security and safety, public security, economic security or infrastructure which is for the public interest, the offender shall be liable for imprisonment for up to 15 years and a fine for up to THB 300,000 (CCA, s.12).

A person who inputs into a computer system: (i) false computer data in a manner which is likely to cause damage to the protection of national security, public safety, economic security or infrastructure which is for the public interest or to cause panic to the general public; or (ii) computer data which is an offence related to national security or terrorism under the Criminal Code, shall be liable for imprisonment not exceeding five years and/or THB 100,000 (CCA, ss14(2)–(3)).

In addition, any service provider who cooperates, consents to or acquiesces in the commission of an offence under Section 14 with regard to a computer system in his control would be liable for the same penalty (CCA, ss14–15).

Under the PDPA, it is prohibited, except where permitted to do so by the provisions of the PDPA or any other law, to collect, use, or disclose personal data, unless the data subject has given consent prior to or at the time of such collection, use, or disclosure. (PDPA, s.19).

1.2 Do any of the above-mentioned offences have extraterritorial application?

Generally, under the Criminal Code, where the criminal offence relating to public security, cheating or fraud is committed outside Thailand and (i) the offender is a Thai national and there is a request for punishment by the government of the country where the offence has occurred or by the injured person, or (ii) the offender is a non-Thai national and the Thai Government or a Thai person is an injured person and there is a request for punishment by the injured person, the offender could be punished under the laws of Thailand.

The PDPA applies to the collection, use, or disclosure of personal data by a data controller or a data processor that is in Thailand, regardless of whether such collection, use, or disclosure takes place in Thailand or not. Where a data controller or a data processor is outside Thailand, the PDPA shall apply to the collection, use, or disclosure of personal data of data subjects who are in Thailand, provided that the activities of such data controller or data processor are the following activities:

(1) the offering of goods or services to the data subjects who are in Thailand, irrespective of whether the payment is made by the data subject; and
(2) the monitoring of the data subject's behaviour, where the behaviour takes place in Thailand (PDPA, s.5).

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Yes. There is an exception which applies only to service providers for the offences under Sections 14–15 of the CCA. Where the service provider is able to prove it has complied with the Ministerial Notification setting out procedures for the notification and suppression of the dissemination/removal of such offended computer data from the computer system, it would be exempt from the penalty (CCA, s.15).

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The following regulations apply to cybersecurity issues:

(1) Section 32 of the Constitution of the Kingdom of Thailand.
(2) Criminal Code.
(3) CCA.
(4) Cybersecurity Act.
(5) PDPA (as fully enforced in June 2021).
(6) Electronic Transactions Act B.E. 2544 (2001), as amended.
(7) Financial Institutions Businesses Act, B.E. 2551 (2008) ("**FIBA**").
(8) Special Case Investigation Act B.E. 2547 (2004), as amended.
(9) Telecommunications Business Act B.E. 2544 (2011), as amended ("**TBA**").
(10) Payment Systems Act B.E. 2560 (2017) ("**Payment Systems Act**").
(11) The National Council for Peace and Order Announcements.
(12) The Royal Decree prescribing Criteria and Procedures for Electronic Transactions of the Government Sector B.E. 2549 (2006).
(13) The Royal Decree on Security Procedures for Electronic Transactions B.E. 2553 (2010).
(14) The Notifications issued by the Electronic Transactions Commission ("**ETC**").

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes. The Cybersecurity Act sets out obligations for the Organization of Critical Information Infrastructure ("**CII Organization**") including, but not limited to, conducting risk assessment on maintaining cybersecurity and establishing a mechanism or process to monitor cyber threats or cybersecurity incidents in accordance with the required standards. In the event of a cyber threat significantly occurring to the system of the CII Organization, the CII Organization shall report to the Office of the National Cybersecurity Committee ("**Office**") and the supervising or regulating organisation, and cope with the cyber threats (Cybersecurity Act, ss48–57).

Under Section 49 of the Cybersecurity Act, CII Organisations are businesses whose nature qualify the characteristics as prescribed by the National Cybersecurity Committee, which includes the service providers of the following aspects:

(1) national security;
(2) substantive public service;
(3) banking and finance;
(4) information technology and telecommunications;
(5) transportation and logistics;
(6) energy and public utilities;
(7) public health; or
(8) other as prescribed by the National Cybersecurity Committee.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Under the Cybersecurity Act, the CII Organisation has the duty to conduct risk assessment on maintaining cybersecurity and to establish a mechanism or process to monitor cyber threats or cybersecurity Incidents which relates to its critical information infrastructure and shall participate in assessment of the readiness in coping with cyber threats as held by the Office (Cybersecurity Act, ss54–56).

Under the PDPA, the organisation which is the data controller or the data processor also required to take measures to monitor, detect, prevent or mitigate Incidents. (PDPA, ss37 and 40).

Additionally, specific requirements may also apply to organisations in specific industries; for example, Section 50 of the TBA and the notification issued thereof, the telecommunication licensee shall put in place protection and security measures pertaining to personal data both in technical and internal organisational management aspects suitable with each type of telecommunications services.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. Section 57 of the Cybersecurity Act requires the CII Organization to report any event of a cyber threat significantly occurring to its system to the Office and the supervising or regulating organisation. The Cybersecurity Regulating Committee ("**CRC**") may prescribe criteria and methods for reporting in the future.

Section 37(4) of the PDPA provides that the data controller shall notify the Office of the Personal Data Protection Committee of any personal data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such personal data breach is unlikely to result in a risk to the rights and freedoms of the persons. The notification and the exemption to the notification shall be made in accordance with the rules and procedures set forth by the Personal Data Protection Committee. There are, however, currently no such rules and procedures announced.

Sectoral laws also impose reporting obligations on specific industries. For example, under the Payment Systems Act, e-payment service providers are required to notify the Bank of Thailand ("**BOT**") of an occurrence of any problem or failure to provide e-payment service as soon as possible, regardless of whether such problem/failure is caused by the occurrence of an Incident. Under the FIBA, the financial institutions are required to report to the BOT any significant problem or incident in relation to technology usage which impacts the service, system or reputation of the financial institutions, including the Incidents.

Under the Securities and Exchange Act 1992 ("**SEA**"), securities companies are required to notify, either by verbal or electronic means, the Securities and Exchange Commission ("**SEC**") without delay upon the acknowledgment of a system disruption, unauthorised access to a system or an Incident that results in damage to the security company's reputation, such as website defacement.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes. Section 37(4) of the PDPA provides that, if the personal data breach is likely to result in a high risk to the rights and freedoms of persons, the data controller shall also notify the data subject of the personal data breach and remedial measures without delay.

The notification shall be made in accordance with the rules and procedures set forth by the Personal Data Protection Committee. There are, however, currently no such rules and procedures announced.

Specific reporting obligations apply to the securities companies under the SEA, and the telecommunication licensee under the TBA.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

(1) Cybersecurity Regulating Committee.
(2) Personal Data Protection Committee.
(3) National Broadcasting and Telecommunications Commission ("**NBTC**").
(4) Bank of Thailand.
(5) The Securities and Exchange Commission.
(6) A police officer – the official who has the authority to initiate an investigation or proceedings relating to a criminal offence, including CCA offences.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

(1) Under the Cybersecurity Act, the CII Organisation that fails to report a cyber threat Incident without reasonable cause would be subject to a fine not exceeding THB 200,000.
(2) Under the PDPA, the penalty for a data controller/data processor not complying with the notice requirements under questions 2.3, 2.4 and 2.5 is an administrative fine not exceeding THB 3,000,000.
(3) Under the SEA, the penalty for securities companies not complying with the notice requirements under questions 2.4 and 2.5 is a fine not exceeding THB 300,000 and a further fine not exceeding THB 10,000 for every day during which the violation continues. The director, manager or any person responsible for the operation of such securities company shall be liable for imprisonment for a term not exceeding six months or to a fine not exceeding THB 200,000, or both, unless it can be proven that such person has no involvement with the commission of the offence by such securities company.
(4) Under FIBA, the penalty for financial institutions that fail to report to the BOT under question 2.4 is a fine not exceeding THB 1 million and, during the incompliance or until such incompliance is rectified, a daily fine not exceeding THB 10,000.
With respect to e-payment service providers under the supervision of the BOT, the penalty for not complying with the notice requirement under question 2.4 is a fine not exceeding THB 1 million or THB 2 million depending on the type of e-payment service provider.
(5) If the Licensee under the TBA fails to comply with the requirement identified under question 2.3 or the prescribed licensing conditions, the NBTC has the power to order the Licensee to: refrain from carrying out the violating act(s); carry out rectification and improvement; or perform actions correctly or appropriately within a specified period of time. If the Licensee fails to comply with the order, the Licensee shall be liable for an administrative fine of not less than THB 20,000 per day and in case the Licensee still fails to perform the actions correctly, or where there is serious damage to the public interest, the NBTC has the power to suspend or revoke the licence.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In 2018, according to media reports, the personal data of around 46,000 users of TrueMove H, Thailand's mobile operator, was leaked into Amazon Web Services' ("**AWS**") cloud storage and the NBTC ordered TrueMove H to solve the Incident and report the result to the NBTC.

In May 2020, the media reported an alleged data leakage of more than 8.3 billion internet usage records of users of Thailand mobile operator, AIS. AIS claimed that such data was not personal data and there was no effect on the AIS users, financially or in any other aspects. The NBTC handed an official warning letter demanding that AIS and its subsidiaries strictly ensure cybersecurity and personal data protection after the incident.

We found no other non-compliance cases taken by the relevant regulators which have been announced to the public.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Not applicable. According to Section 60 of the Cybersecurity Act, the Office is entitled to determine the measures to prevent, cope with, assess, suppress and suspend the cyber threats in each level. As of now, there is no notification regulating the use of beacons to detect and deflect Incidents in Thailand.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Please see the comment provided with regard to beacons above.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Please see the comment provided with regard to beacons above.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

There is no specific provision addressing monitoring or intercepting electronic communications on the ground of preventing or mitigating the impact of cyber-attacks. The provisions under the PDPA and the CCA apply in general, regarding the collection and processing of personal data and the access to and interception of computer data/systems. Please see our comments in question 1.1 above for details.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

There is no specific provision regulating the import or export of technology designed to prevent or mitigate the impact of cyber-attacks.

However, certain types of electronic device or machine may be subject to import-export restrictions, such as:

- the prescribed machine/equipment used in radio communications business under the Radio Communications Act B.E. 2498 (1955); or
- the dual-use items, (i.e. goods, software and technology that can be used for both civilian and military applications) under the Trade Control on Weapons of Mass Destruction Related Items Act B.E. 2562 (2019).

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. Based on Section 50 of the TBA and the notification issued thereof, the Licensee shall put in place protection and security measures pertaining to personal data both in technical and internal organisational management aspects suitable with each type of telecommunications services. The protection and security measures pertaining to personal data in a technical aspect shall be undertaken at least as follows:

(1) the encoding and decoding system which is used to maintain the security of personal data shall be modified at least every three months; and
(2) the level of safety system shall be adjusted suitably in alignment with the risks arising due to technological advancement.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes.

(1) Financial services sector: the financial sector is administered by the BOT. Financial institutions are required to satisfy the requirement regarding IT security measures and risk management under BOT Notification No. SorNorSor. 21/2562 Re: Regulations on Information Technology Risk of Financial Institutions. Moreover, e-payment service providers, regulated under the relevant BOT notifications, are required to have a contingency plan or a backup system for the purposes of continuity of the service and a safety policy or measures for the information system, which must at least meet the standards prescribed in the BOT notifications.
(2) Telecommunications sector: the telecommunications sector is administrated by the NBTC. The NBTC has issued notifications setting out rules and procedures for the management of information technology, and procedures for protecting personal information, rights of privacy and freedom in communication through telecommunications' means. Please see our comments in question 4.1 above for details. Moreover, the NBTC has the power to prescribe specific provisions concerning cybersecurity to each licensed telecommunication operator.
(3) Others: Insurance companies and banks are subject to the notifications of the Office of Insurance Commission ("**OIC**") governing the collection, handling, use, storage, and protection of personal data used for the purposes of insurance. The credit information company shall put in place rules and procedures regarding data management, security of system and preventive measures for any malicious access in accordance with the the Credit Information Business Operation Act B.E. 2545 (2002).

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Yes. It is not unusual in Thailand for third parties to sue directors or officers together with the company for the alleged commission of offences.

Some laws also provide specific provisions on director liability. According to Section 77 of the Cybersecurity Act and Section 81 of the PDPA, where the offence was committed by a company as the result of an order, an act or omission to order or act, by a director or any person in charge of operation of such company who has the duty to order or act, such director or person must be liable for the penalties prescribed for such offence.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(1) There is no requirement regarding CISO under the Cybersecurity Act. However, Domestic Systemically Important Banks ("**D-SIBs**") or financial institutions with high cyber-inherent risk are particularly required to designate a CISO under BOT Notification No. SorNorSor. 21/2562 Re: Regulations on Information Technology Risk of Financial Institutions.
(2) Yes. Section 44 of the Cybersecurity Act requires the CII Organisation to prepare a code of practice and standard framework for maintaining cybersecurity which shall

comprise the plan for examining and assessing risks related to maintaining cybersecurity, as well as the plan for coping with Incidents.

Also, generally under the PDPA, data controllers and data processors shall provide appropriate security measures for preventing the unauthorised or unlawful loss, access to, use, alteration, correction or disclosure of personal data which must be in accordance with the minimum standard specified and announced by the Personal Data Protection Committee.

(3) Yes. Section 54 of the Cybersecurity Act requires the CII Organisation to conduct a risk assessment on maintaining cybersecurity by having an examiner, including examination in the cybersecurity aspect by the information security auditor, internal auditor or external independent auditor, at least once per year.

(4) Yes. Section 56 of the Cybersecurity Act requires the CII Organisation to participate in the assessment on the readiness in coping with the Incidents as held by the Office.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Yes. Securities companies are required to submit an annual report which includes its IT management and occurrence of Incidents to the SEC. Financial institutions and e-payment service providers are also required to prepare information and details as to the provision of services and information technology and make the same available for inspection by the BOT. The BOT has the power to instruct the financial institutions and e-payment service providers to provide any information in relation to its services, including information on the occurrence of Incidents.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Where the data controller or the data processor violates or fails to comply with the PDPA, which results in damage to the data subject, the party in breach is bound to compensate the data subject for damages suffered, regardless of whether such operation is performed intentionally or negligently.

Apart from actual compensation, the Court may order the party in breach to pay punitive damages as the court deems fit, but not exceeding two times the actual compensation amount.

In addition, issues relating to Incidents are generally governed by the Civil and Commercial Code ("**CCC**") under the section relating to a "wrongful act" (i.e. Section 420 of the CCC). If any Incident, whether wilfully or negligently, unlawfully damages or injures another person's life, body, health, liberty, property or any right, the party in breach is said to have committed a wrongful act and is bound to pay compensation for damages suffered. The general guidance from Thailand's Supreme Court decisions is that the injured party is entitled to claim actual damage suffered, with the burden of proof being on the claimant.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There are limited cases on Incident-related issues and most publicly available cases are criminal cases. Please note that only the Supreme Court cases can be accessed by the public.

According to the media, in 2016, the accused was arrested in connection with the attacks that caused some government websites to be blocked and non-public files to be leaked. The legal status of the accused and the progress of the case are not yet available to the public.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes. Please see our comments on "wrongful acts" in question 6.1 above.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. There are no regulatory limitations for the organisations to take out insurance against Incidents in Thailand.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

In coping with and to remedy damage from a cyber threat at a critical level, the CRC has the power to order any relevant person to: (i) monitor the computer or computer system; (ii) examine the computer or computer system to find an error, analyse the situation, and evaluate the effects from the cyber threat; (iii) conduct a measure rectifying the cyber threat; (iv) maintain the status of the computer data or computer system to operate the computer forensic science; and (v) provide access to the relevant computer data or other information related to the computer system.

CRC also has the power to order a competent official to do the following: (i) enter into a place to examine; (ii) access the computer data, computer system or other data, copy, or filter/screen information data or computer program; (iii) test the operation of the computer or computer system; and (iv) seize or freeze a computer, a computer system, or any equipment.

For the benefit of an investigation, if there is reasonable cause to believe that there is the commission of an offence under the CCA, or there is a request by the inquiry official, the competent official is empowered to acquire evidence to prove an

offence and to identify the accused, for example, by: (i) issuing an inquiry letter to any person related to the commission of an offence to give statements, forward written explanations or any other documents, data or evidence in a comprehensible form; (ii) requiring computer traffic data related to communications from a service user via a computer system or from other relevant persons; (iii) instructing a service provider to (a) deliver user-related data that is required to be retained under the CCA requirements or that is in the service provider's possession or control to the competent official, or (b) keep the data for later; or (iv) seizing or attaching a computer system for the purposes of obtaining details of the offence and the person who committed the offence.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes. In relation to criminal offences in violation of the CCA or any other laws committed against any persons by using a computer system, computer data or equipment storing computer data, which is a composition or part of the commission of the offence or has computer data relating to a commission of any offence under another law, the competent official is empowered to decrypt any person's computer data or order a person related to the encryption of the computer data to decrypt it, or cooperate with the competent official to decrypt it.

Supawat Srirungruang is a Partner in the Corporate & Commercial Practice of R&T Asia (Thailand) Limited, the Bangkok office of Rajah & Tann Asia. Supawat graduated with a Bachelor of Laws (with honours) from Thammasat University (1998), and has a Master of Laws from California Western School of Law (2001) and University of Sydney (2002). Prior to joining Rajah & Tann, Supawat spent more than 14 years working for leading American- and Australian-based international law firms in Thailand. Supawat focuses his practice on technology, media & telecommunications matters, regulatory compliance, administrative law, dispute resolution, anti-bribery, competition law, labour law issues, merger and acquisitions, customs regulation, project development, and international trade laws.

R&T Asia (Thailand) Limited
973 President Tower, 12th Floor Units 12A–12F
Ploenchit Road, Lumpini, Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 656 1991
Email: supawat.s@rajahtann.com
URL: www.rajahtannasia.com

Saroj Jongsaritwang is a Partner in the Corporate & Commercial Practice of R&T Asia (Thailand) Limited, the Bangkok office of Rajah & Tann Asia. Saroj graduated with a Bachelor of Laws from Thammasat University in 1999, and is a licensed Thai lawyer.
Prior to joining Rajah & Tann, Saroj was a legal counsel (AVP) at a leading Thai consumer finance business, and before that he was in private practice at a local Thai law firm. Saroj has several years' experience in advising on corporate, commercial and consumer finance matters (including personal loans, credit cards and insurance) and agreements relating to the consumer finance business.

R&T Asia (Thailand) Limited
973 President Tower, 12th Floor Units 12A–12F
Ploenchit Road, Lumpini, Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 656 1991
Email: saroj.jongsaritwang@rajahtann.com
URL: www.rajahtannasia.com

R&T Asia (Thailand) Limited, based in Bangkok, has an impressive base of international, regional and local clients.
We have many years of experience in advising on a range of Thai law matters, including representing clients in civil, criminal or administrative proceedings, international and domestic arbitration, government investigations and compliance proceedings, structuring foreign direct investment and mergers and acquisitions involving private or listed companies, and general corporate commercial matters for foreign investors in Thailand.
The team has a particular expertise in representing clients in highly regulated industries, such as oil & gas, petrochemical, telecoms, tobacco, food & beverage, insurance and manufacturing, and can provide full support in large-scale litigation, transactions and investigations.
The team comprises a majority of Thai nationals who are qualified to advise on Thai law. Our Thai lawyers are fluent in Thai and English and are fully conversant with the practical application of the law within Thailand's business and cultural landscapes.

www.rajahtannasia.com

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

United Arab Emirates


Hamdan Al Shamsi


Helen Tung

Hamdan AlShamsi Lawyers & Legal Consultants

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
The law incriminates hacking and provides various penalties depending on: the way in which electronic information was hacked; the content of what was hacked and what result the hack brought about; and whether information was destroyed or stolen. The basic sentence for accessing an electronic database or software or programme without rights and privileges to do so is imprisonment and a fine of AED 100,000 to AED 300,000. The sentence would be higher if the act affected a government entity or otherwise a company. If the hacking results in any damage, or destroys, amends or deletes any data, the penalty increases to imprisonment for at least six months and a fine of up to AED 750,000.

It should be noted, with the introduction of the DIFC Data Protection Law, No. 5 of 2020 (DIFC DPL), that whilst there are no criminal offences in place, there could well be administrative fines applicable as per Art. 62 as a consequence of a breach. The laws and regulations are administered by the Commissioner and personal data are either kept and/or processed by the Controller or Processor. The onus lies within the remit of the Controller or Processor within an organisation. Such administrative fines are listed in Schedule 2 of the Data Protection Laws, ranging from US$25,000 to US$100,000. It is foreseeable that each breach is likely to be assessed on the facts.

Denial-of-service attacks
Denial of service attacks are punishable under UAE law. They are punishable by a fine of AED 100,000 to AED 300,000 and/or imprisonment.

It should be noted, with the introduction of the DIFC DPL, No. 5 of 2020, that whilst there are no criminal offences in place, there could well be administrative fines applicable as per Art. 62 as a consequence of a breach. See "Hacking (i.e. unauthorised access)" above.

Phishing
If the phishing was directed at obtaining passwords or security information to log in or gain access to systems, then the perpetrator can be subject to jail and/or a fine of between AED 100,000 and AED 500,000. If the perpetrator was able to obtain banking information or credit card information, they would be subject to jail and fines depending on whether they committed the crime to misappropriate money or not. In the case where they had the intention but did not necessarily appropriate the money, they would be subject to a minimum sentence of six months and a fine of between AED 100,000 and AED 300,000. If the perpetrator was able to actually misappropriate money, they would be subject to a minimum sentence of one year's imprisonment and a fine of between AED 100,000 and AED 1,000,000.

It should be noted with the introduction of the DIFC DPL, No. 5 of 2020 that whilst there are no criminal offences in place, there could well be administrative fines that come in place, that come under Art. 62 as a consequence of a breach. See "Hacking (i.e. unauthorised access)" above.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infecting a server, electronic system or data with any type of malware, virus or program is punishable with a minimum of five years' imprisonment and a fine of between AED 500,000 and AED 3,000,000. The penalty is reduced if the act did not cause any harm or change, or take information.

If such infection results in a breach of the data protection rules in the form of disclosed personal emails and details, then it is likely it would trigger further fines and liabilities as per Schedule 2 of the DIFC DPL.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
The distribution, sale or offering for sale of hardware, software and tools could be legal in principle. However, allowing such tools to "commit" cybercrimes suggests that it may well be illegal. Notwithstanding, clearly any breach of the DIFC DPL would result in fines and/or liabilities.

Possession or use of hardware, software or other tools used to commit cybercrime
Any person who creates, sells, markets or otherwise makes available for sale any tools to commit cybercrimes shall be subject to imprisonment and/or a fine of AED 100,000 to AED 500,000. The law also punishes any person who may have a website or database that carries and possesses something illegal with knowledge of its illegality or who has not removed it after being directed to do so by the authorities.

Identity theft or identity fraud (e.g. in connection with access devices)
Any person found guilty of fraud, using someone's identity for his own benefit, will be subject to a minimum of one year's imprisonment and a fine of between AED 150,000 and AED 1,000,000.

Moreover, the DIFC DPL raises the importance of personal data, thereby giving rise to greater responsibility for companies, especially those designated as Controllers/Processors, to ensure there is consent. Hence in scenarios where such consent is not present, and the data is breached, one can envisage fines/liabilities flowing from that.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Any person who obtains and uses confidential information illegally, through his employment, can be subject to imprisonment for a minimum of six months and a fine of between AED 500,000 and AED 1,000,000.

Moreover, the DIFC DPL raises the importance of personal data, thereby giving rise to greater responsibility for companies, especially those designated as Controllers/Processors to ensure there is consent, and hence in scenarios where such consent is not and moreover, their data is breached, one can envisage fines/liabilities flowing from that.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
This is a difficult question, because the ultimate question in the context of the DIFC DPL is whether there is consent at the time the information is supplied. If such unsolicited penetration testing would preclude divulgence of such personal data, whether or not it is part of a simulation exercise, then arguably one could say no harm was done.

If, however, such unsolicited penetrating testing results in data being released to the public, with or without the person's consent, then there may be a broader issue as to breach of the DIFC DPL rules, which may result in fines/liabilities the extent of which would most likely require assessment on a case-by-case basis.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
There are many additional crimes listed that are punishable under UAE law, including intercepting any correspondence or calls and recording them. Other crimes punishable include blackmailing using the internet or through other electronic means, insulting or verbally assaulting anyone using electronic means, money laundering, using any electronic means for terrorism and collecting any charity without a licence to do so. It is punishable by law if electronic means are used to threaten the security of the country.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The law does have extra-territorial application for any breaches of the law by any offenders, except in connection with a database or electronic property related to the government or its departments.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Currently, there appears to be none. In fact, if we were to look at the DIFC DPL, there appears to be greater opportunities for development and scope especially when we look at the Codes of Conduct (Art. 48) and potential Certification Schemes. It would be fair to say that there is no current accepted standard under which such "ethical hacking" can be accepted; however, that is not to say that may not change in the near future.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The laws that relate to cybercrime are Cybercrime Law no. 5 of 2012, replacing Cybercrime Law no. 2 of 2006, and the DIFC DPL 2020.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

It would be useful to see where the DIFC DPL does not apply, including in personal or household activity that has no connection to a commercial purpose. If that were the case, and assuming critical infrastructure and operators of essential services have a commercial purpose, then on the face of it the DIFC DPL would apply. To what extent, and what legal ramifications apply, would most likely need to be assessed on a case-by-case basis.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

There are no laws that require organisations to take measures to monitor, detect, prevent or mitigate cybercrimes; however, regulators in certain industries will set out regulations to require organisations to deal with cybercrimes and prevent them. One example of such is the central bank, which issues circulars and instructions to banks for dealing with cybercrimes.

To the extent that any incidents give rise to breach of the DIFC DPL, then it may well be recommended that organisations have a plan to address such issues. For example, under Part 7 of the DIFC DPL, there is a requirement for any personal data breaches to be notified to the Commissioner and Data Subject, so it would be advisable for organisations to have a plan of action ready in case such breaches were to occur.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

(a) In the context of the DIFC DPL, the circumstances would most likely be a breach of personal data in some shape or form.
(b) The Commissioner would need to be notified as well as the Data Subject.
(c) Presumably, basic information, depending on the circumstances/impacts and consequences.
(d) Under the DIFC DPL, there are certain provisions if the Data Subject had withdrawn their rights, or attempts have been made to contact them that such further information ought to be taken into account.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under Art. 42 of the DIFC DPL, there is an obligation to notify the Data Subject if it is likely there is a high risk to the security or rights of the Data Subject. The key phrase is "high risk", which may well mean that there is a chance, yet the event has yet to occur, which means that the burden is placed on the company with such information.

The nature and scope of scope of such information would need to be provided in clear and plain language and, where possible, recommendations ought to be made to mitigate any potential adverse effects.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The Commission is in charge, who is appointed by the President. The President shall consult the DIFCA Board of Directors in that regard (Art. 43 of the DIFC DPL).

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Fines/liabilities can be imposed. Please see Schedule 2 of the DIFC DPL.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

The question of enforcement is not stated explicitly; however, there is reference under Art. 59, which refers to "seek[ing] Judicial Review by the Court", which presumably allows for appeal or assessment of how the law is applied. It is yet to be seen whether such decisions are enforceable.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Beacons may be used; however, if by using the beacon information an IP address is obtained and such was used for committing a crime, then it would not be allowed, and it would be considered illegal.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Honeypots are permitted.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
If it is used only for the organisation's own IP addresses, then sinkholes are permitted, but if it happens to result in diverting traffic away from other organisations then it may breach cybercrime law.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

To the extent that there may be a breach and mitigation is required, one can safely presume the answer is yes; however, the circumstances would be very limited.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Such import/export is likely to be assessed on a case-by-case basis.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice differs from one industry to another. As explained, different industries have different regulators, who may have requirements and instructions to companies in that specific industry.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

The financial sector is regulated by the central bank of the UAE. The central bank issues circulars that may include instructions for banks to deal with cybersecurity. The telecommunications sector is regulated by the Telecommunications Regulatory Authority (TRA), which may communicate certain instructions to them too. Whilst there may not be any laws specific to these sectors, the regulators and authorities may communicate instructions to the companies in such industries.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Managers and directors can be found liable under the laws of the UAE. This is dealt with in the general rules of responsibility for damage caused (tort) and other articles that deal with the responsibilities of managers and board of directors towards their companies. Managers and directors who may be seen to have omitted or acted in a wrongful way, which caused harm to a company, may find themselves liable for losses and damages.

With the DIFC DPL, the role of a Controller/Processor is important to the extent that a fine may be imposed. It is anticipated that, as the law is still in a nascent stage, through case law and evolution of practice, we are yet to see what the best practices are. Currently, the DIFC DPL makes clear what potential fines and liabilities companies may be subject to and so it gives a sense of what and the seriousness of any breach could result in significant financial penalties.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Companies generally are not required to appoint a CISO and neither do they have to by law establish an incident response plan or policy, conduct periodic cyber risk assessments or perform tests unless required and instructed by a regulator for a specific industry; for example, the central bank or the TRA.

However, in the context of the DIFC DPL, the approach very much relies on the Controller/Processor in ensuring details are captured, processes are in place and therefore quite naturally one can see assessments and performance penetration tests or the like being performed. The new law gives impetus to organisations to think proactively rather than reactively in how to tackle and prevent data protection breaches.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There is no law requiring such disclosures; however, certain regulators may have instructed companies in certain industries to do so, save for in relation to the DIFC DPL.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Any civil action may be brought if a claimant can prove that an act through the internet or electronic means caused harm to the claimant. The claimant would need to prove causation and damages.

In relation to the DIFC DPL, there are directions under Art. 59 which allow for complaints to be addressed to Commissioners. It is still too early to understand how this would work on a practical level, though it is safe to say that should reasonable measures be taken, then matters could potentially be resolved. If not, we may see new developments via case law.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There are no incidents that can be disclosed.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The UAE has a concept similar to tort in which a claimant may claim against any person who, through such act, caused harm to a claimant. Such a concept would apply to incidents in cyberspace.

Under the DIFC DPL, there are fines/liabilities as per Schedule 2.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, they are permitted.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no limitations. Insurance companies may exclude or

include clauses in their policies with insured persons. There are no legal limits for these types of insurance cover.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

By law, the authorities have certain powers in relation to cybercrimes, including contacting service providers for information, requesting access to information, reviewing information and other general powers of investigative bodies. Likewise, in relation to the DIFC DPL, the Commissioner has a right to conduct such investigations.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no requirements for such; however, the authorities may, by law and as part of their mandate, instruct and require cooperation from persons in the country. However, it may well be in the interests of companies to consider implementing backdoors, as the fines/liabilities for any breach of the DIFC DPL are not insignificant.

Hamdan Al Shamsi has built one of Dubai's most reputable and respected law practices, and is widely regarded as a top litigator in the Dubai Courts with immeasurable experience in corporate, banking & finance, and insurance law. Hamdan advises both local and international companies as well as governmental entities in cases involving complex litigation. He appears regularly before both the Appeals Court and the Court of Cassation, as well as the UAE's Federal Supreme Court.

Hamdan AlShamsi Lawyers & Legal Consultants
Office 107
Bay Square, BLD- 07
Marasi Drive, Business Bay, Dubai
United Arab Emirates

Tel: +971 4 346 9262
Email: hamdan@alshamsilegal.com
URL: www.alshamsilegal.com

Helen Tung, LL.B. (Hons) is a UK-trained Barrister with 11 years of post-qualification experience. Helen attended the University of Sheffield, Tilburg University and the University of Law, where she obtained her law degrees. Helen furthered her studies at the University of Greenwich for Ph.D. studies (completed coursework only) in maritime security and international law and undertook Directed Studies on International Private Law at The Hague Academy.
Helen works in the DIFC department, specialising in commercial disputes including banking, bankruptcy, construction, and shipping.
Prior to joining HAS, Helen worked in reinsurance, maritime law and commercial disputes in London and advised clients globally. Helen also had experience working as a policy legal advisor for the UK Maritime Coastguard, was an advocate for the Home Office with experience in the Court of Appeals and had secondments with leading shipping law firms in Seoul and Shanghai. Helen has also advised the European Commission, METI and UAE Space Agency in relation to space law and policy.
Helen is a member of the Dubai Courts of the Future Working Group, a founding member of the Maritime Autonomous Regulatory Systems Working Group (MARSWG) and a member of the SmartShip ISO standards committee. Helen is also a committee member of the Knowledge Management group of the International Bar Association addressing the role of AI and emergent technologies in law.
Helen is also part of 7 Pillars law working in space law, and the Founder of NewSpace2060.

Hamdan AlShamsi Lawyers & Legal Consultants
Office 107
Bay Square, BLD- 07
Marasi Drive, Business Bay, Dubai
United Arab Emirates

Tel: +971 4 346 9262
Email: htung@alshamsilegal.com
URL: www.alshamsilegal.com

Established in 2011, Hamdan AlShamsi Lawyers & Legal Consultants has adapted and expanded, paving the path for our diverse range of legal experience and clientele. Based in the UAE, our legal practice provides sector expertise at both the local and international levels. Hamdan Al Shamsi is not only known for his successful cases that have been internationally recognised, such as the Al Khorafi Swiss Banking accomplishment, but also his litigation expertise and especially copyright experience. Hamdan is known by reputation throughout the UAE for not only his position as Senior Partner of leading firm Hamdan AlShamsi Lawyers, but also as the CEO, heading a team of international lawyers. The firm's areas of legal litigation and consultancy expertise include, but are not limited to: Banking & Finance; Construction; Corporate, Criminal; Family; Maritime; Employment (Labour); Real Estate; and Intellectual Property Law.

www.alshamsilegal.com

HAMDAN ALSHAMSI
LAWYERS & LEGAL CONSULTANTS

USA

Edward R. McNicholas

Kevin J. Angle

Ropes & Gray LLP

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. The federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, is the primary statutory mechanism for prosecuting cybercrime, and it provides for both criminal and civil penalties. The CFAA prohibits: (1) unauthorised access (or exceeding authorised access) to a computer and obtaining national security information; (2) unauthorised access (or exceeding authorised access) to a computer that is used in interstate or foreign commerce and obtaining information; (3) unauthorised access to a non-public computer used by the United States government; (4) knowingly accessing a protected computer without authorisation with the intent to defraud; (5) damaging a computer either intentionally or recklessly; (6) trafficking in passwords; (7) transmitting threats of extortion, specifically threats to damage a protected computer and threats to obtain information or compromise the confidentiality of information; and (8) cyber-extortion related to demands of money or property. Depending on the specific offence, penalties can range from one to 20 years in prison. The U.S. Supreme Court is considering the scope of this statute in *Van Buren v. U.S.*, case no. 18012024, which will likely be argued in the fall of 2020.

Other relevant laws include the Electronic Communications Protection Act ("ECPA"), which provides protections for communications in storage and in transit. Under the Stored Communications Act (Title II of the ECPA), 18 U.S.C. § 2702, it is a criminal violation to intentionally access without authorisation (or exceed authorised access) a facility that provides an electronic communications service ("ECS"), which could include, among others, email service providers or even employers who provide email addresses to their employees. Personal computers are not considered facilities providing an ECS. Violations are subject to penalties ranging from up to one year for first time violations without an improper purpose (i.e. violations that are not committed for commercial advantage, to cause malicious destruction or damage or the like) to up to 10 years for repeat violations for an improper purpose. Intentionally intercepting electronic communications in transit is prohibited by the Wiretap Act (Title I of the ECPA), 18 U.S.C. § 2511, with exceptions for law enforcement, some service providers and others (including, potentially, employers). Penalties for violations can include imprisonment for up to five years.

In addition to federal statutes, numerous states have passed statutes prohibiting hacking and other computer crimes, some of which are broader than the federal statute. New York, for example, prohibits the knowing use of a computer with the intention to gain access to computer material (computer trespass), N.Y. Penal Law § 156.10, with penalties of up to four years' imprisonment, and knowing unauthorised use of a computer, N.Y. Penal Law § 156.05, 156.20 *et seq.*, with penalties of varying ranges up to 15 years' imprisonment, depending on the severity of the offence. New York is merely one example; dozens of such state laws exist. The specification of which statute is applicable depends on several factors.

Hacking could violate, among other statutes, the CFAA, 18 U.S.C. § 1030(a)(1) (national security information, imprisonment up to 10 years), (2) (obtaining information, imprisonment up to one year, or five if aggravating factors apply), (3) (government computers, imprisonment up to one year), and (4) (accessing to defraud, imprisonment up to five years).

Denial-of-service attacks

Yes, a DOS attack could violate CFAA, 18 U.S.C. § 1030(a)(5)(A) (intentionally damaging through knowing transmission, imprisonment up to 10 years), as well as state computer crime laws.

Phishing

Yes, among other statutes, phishing could violate the CFAA, 18 U.S.C. § 1030(a)(5)(A) or constitute wire fraud under 18 U.S.C. § 2702, which carries a potential sentence of up to 20 years' imprisonment.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes, planting malware would violate CFAA, 18 U.S.C. § 1030(a)(5)(A) (intentionally damaging through knowing transmission, imprisonment up to 10 years), as well as state computer crime laws.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Whether distribution of hacking tools would constitute a crime would depend on whether the actor intended for them to be used for illegal purposes. If there were evidence of criminal intent and the distribution assisted another party in committing a hacking offence, a person may be liable for aiding and abetting the violation of the CFAA, 18 U.S.C. § 1030(a)(5)(A), or related computer crime laws. With respect to federal statutes, aiding and abetting is subject to the same sentence as commission of the offence.

Possession or use of hardware, software or other tools used to commit cybercrime
As with distribution, mere possession of hacking tools would be difficult to prosecute in the absence of intent to use them for illegal purposes. If there were evidence of criminal intent and some overt act taken towards that end, a person may be liable for an attempt to violate the CFAA, 18 U.S.C. § 1030(a)(5)(A), or related computer crimes laws. With respect to federal statutes, attempt is subject to the same sentence as commission of the offence.

Identity theft or identity fraud (e.g. in connection with access devices)
Yes, identity theft could be charged under the federal identity theft statute, 18 U.S.C. § 1028, as well as numerous state laws.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Yes, electronic theft could violate CFAA, 18 U.S.C. § 1030(a)(2) (obtaining information, imprisonment of up to one year, or five if aggravating factors apply). It may also, or alternatively, violate the Economic Espionage Act, 18 U.S.C. § 1831–1839, which creates two crimes based on the theft of trade secrets; the first makes it a crime to acquire, without authorisation, trade secrets in order to benefit a foreign government, and the second if the theft will create economic benefit for others and will injure the target of the theft.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Yes. Unsolicited penetration testing could constitute a violation of the CFAA if the tester obtains data as a result or causes damage. To the extent information was obtained from the systems tested, such testing could violate 18 U.S.C. § 1030(a)(1) (national security information, imprisonment up to 10 years), (2) (obtaining information, imprisonment up to one year, or five if aggravating factors apply), or (3) (government computers, imprisonment up to one year). If the penetration tester causes damage, e.g. by impairing the integrity or availability of a system or data, the action could constitute a violation of § 18 U.S.C. § 1030(a)(5).

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
The CFAA, 18 U.S.C. § 1030(a)(2), and wire fraud statute, 18 U.S.C. § 2702, as well as numerous state laws apply to a wide variety of criminal conduct online.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, the USA PATRIOT Act amended the CFAA and Access Device Fraud statute, 18 U.S.C. § 1029, to expressly apply them extraterritorially.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The nature of the crime, whether it was intentional or unintentional, whether it was committed for economic benefit or malice or ethical hacking, and the number of past offences may impact the severity of any penalty. The existence of a robust corporate compliance program, as well as cooperation with law enforcement, may help to mitigate any penalty or influence prosecutorial discretion.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Numerous federal and state laws include cybersecurity requirements. The Federal Trade Commission ("FTC") has been particularly active in this space and has interpreted its enforcement authority under § 5(a) of the FTC Act, applying to unfair and deceptive practices, as a means to require companies to implement security measures. Since 2002, the FTC has brought more than 80 enforcement actions against companies it alleges failed to implement reasonable security measures.

The Cybersecurity Information Sharing Act ("CISA") has two primary impacts. First, it allows companies to monitor network traffic, including taking defensive measure on their own systems. Second, it encourages the sharing of cyber-threat information between companies and with the government.

Some federal laws, however, are sector-specific or extend only to public companies. For example, the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations require "financial institutions" to implement written policies and procedures that are "reasonably designed" to ensure the security and confidentiality of customer records, and protect against anticipated threats and unauthorised access and use. The Health Insurance Portability and Accountability Act ("HIPAA") includes cybersecurity requirements applicable to protected health information in the possession of certain "covered entities" and their "business associates".

At the state level, several states have passed laws imposing security requirements. Most of these statutes require some form of "reasonable security". Massachusetts regulations impose specific security requirements on companies that own or licence personal information, including the implementation of a written security program and encryption of data in transit across public networks and on all portable devices. New York recently passed its SHIELD Act, requiring reasonable security for personal information and specifying specific measures that may satisfy that standard. The California Consumer Privacy Act ("CCPA") creates a data breach right of action for Californian residents with statutory penalties of $100 to $750 per consumer and per Incident if plaintiffs prove that the impacted business failed to implement and maintain reasonable security procedures and practices, appropriate to the nature of the information, to protect the personal information.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The Cybersecurity and Infrastructure Security Agency Act created CISA, a component of the Department of Homeland Security, and the federal agency responsible for protecting

critical infrastructure in the United States. CISA coordinates between government and private sector organisations in protecting critical infrastructure. The federal government has issued sector-specific guidance for critical infrastructure operators and the nuclear, chemical, electrical, government contracting, transportation and other sectors have detailed statutory and regulatory requirements.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Generally, yes. U.S. cybersecurity laws exist at both the federal and state levels and vary by commercial sectors. For instance, several federal statutes have data breach notice provisions, but each state and four territories also have data breach laws. Many regulators expect regulated companies to have implemented "reasonable" security measures, taking into account factors such as the sensitivity of the data protected. In light of the proliferation of standards, many companies rely on omnibus cybersecurity frameworks like the NIST Cybersecurity Framework, which recommends that companies take steps to identify and assess material foreseeable risks (including with vendors), design and implement policies and controls to protect the organisation in light of those risks, monitor for and detect anomalies and realised risks, respond promptly and adequately to Incidents and then recover from any Incident.

In addition to general reasonable security requirements, some U.S. laws are much more prescriptive. For example, Massachusetts' cybersecurity regulations and the New York SHIELD Act contain detailed information security requirements at the state level, and the New York Department of Financial Services (which regulates entities such as banks and insurance companies) has further additional requirements.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, all states and four territories have requirements for the reporting of Incidents and most of these statutes require reporting to state regulators. The nature and scope of the information that is required to be reported varies by state or territory. For example, Massachusetts requires that organisations reporting a breach to state regulators must include information about (i) the nature of the breach of security or unauthorised acquisition or use, (ii) the number of residents of Massachusetts affected by the Incident, (iii) any steps taken to address the Incident, (iv) the name of the organisation reporting and experiencing the breach, (v) the person responsible, if known, (vi) the type of personal information potentially compromised, (vii) whether the organisation maintained a written information security program, as required by Massachusetts regulations, and (viii) whether the organisation is updating that program in response to the Incident.

These state requirements are in addition to federal requirements that are sector-specific. For example, the Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") requires covered entities and business associates to report certain Incidents involving Protected Health Information ("PHI").

Timeframes for reporting vary by state or agency, with most requiring notification around the same time that individuals are notified (or sometimes in advance). Vermont requires any notification to its Attorney General to be sent within 15 days. Covered financial institutions are required to report breaches to the New York Department of Financial Services within 72 hours. At the request of law enforcement agencies, however, some notifications may be delayed.

Information about cyber threats generally need not be reported, although the federal government encourages participation in Information Sharing and Analysis Centers ("ISAC"s) or Information Sharing and Analysis Organizations ("ISAO"s) where threat intelligence is shared within sector-specific groups of companies.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

All 50 U.S. states and four territories have now passed breach notification statutes with varying requirements. Typically, breach notification statutes require notification be sent to individuals whose electronic Personal Information, as defined therein, was acquired in an Incident, though some states require notification based on access to such information alone. State definitions of Personal Information triggering data breach notification generally apply to the first name or first initial and last name in combination with another identifier, when not encrypted or redacted, such as social security number, driver's licence or identification card number, or account number, or credit card or debit card number in combination with any required security code, access code or password that would permit access to the individual's account. Increasingly, states are also including in the definition of Personal Information, health and biometric information, as well as usernames and passwords that provide access to an online account. Many states also require that notice be sent to Attorney Generals or other state agencies, often depending on the number of individuals impacted. Most states allow for consideration of whether there is a risk of harm to the data subjects, but some states do not allow for such consideration.

Timeframes for notification vary by state; however, 30 days is a common standard.

Additionally, some sector-specific laws provide notification requirements. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400–414, requires HIPAA-covered entities and business associates to provide notifications in the event of certain Incidents impacting PHI.

2.6 Responsible authority(ies): Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The regulator varies by sector, law and state. The FTC is the principal U.S. federal privacy regulator covering most for-profit businesses not overseen by other regulators. The SEC regulates many financial institutions and the OCR is primarily responsible for enforcing HIPAA. State Attorney Generals have broad authority regarding enforcement of cybersecurity matters. In addition, federal and state regulators in particular sectors, such as insurance, have further enforcement powers.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

The U.S. has no single framework for non-compliance with notice requirements and penalties will depend heavily on the relevant law and regulator. In addition to regulatory penalties, private plaintiffs may file actions alleging non-compliance with relevant laws. For example, the CCPA provides for statutory damages of between $100 to $750 per consumer and per Incident in the event of a data breach caused by the failure to have in place reasonable security measures.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Hundreds of actions have been brought for non-compliance. For instance, Equifax agreed to pay at least $575 million as part of a settlement with the FTC, CFPB and 50 U.S. state Attorney Generals, or other state regulators charged with overseeing data security, related to its 2017 data breach allegedly impacting approximately 147 million people. Government authorities alleged that Equifax failed to have in place reasonable security for the information it collected and stored.

Typical of the FTC's enforcement is a case involving Uber in which it entered into an expanded settlement with Uber arising from a 2016 data breach, which the FTC alleged was not disclosed to the FTC for more than a year. The FTC had previously settled allegations related to an earlier 2014 breach. The FTC had alleged that Uber failed to live up to statements that access to rider and driver accounts were closely monitored, which, the FTC alleged, was not the case, rendering the statements false or misleading.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Generally, yes.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Generally, yes.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Generally, yes.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes, the CISA provides broad authorities to monitor network traffic, and employers can generally monitor employee communications where they first provide transparent notice of the monitoring and obtain consent from their employees.

Although the CISA may pre-empt them, state torts such as invasion of privacy may also limit an employer's ability to monitor employee communications, but tort law claims can be overcome where an employer can show that the employee did not have a reasonable expectation of privacy in the communication. Notices and consents to monitoring should be carefully drafted to ensure compliance.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Yes. Export Administration Regulations restrict the export of certain strong dual-use encryption technologies; however, licence exceptions may be available for exports.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Cybersecurity laws in the United States vary significantly by business sector. There is currently no single U.S. cybersecurity law of general application other than, arguably, restrictions of "unfair" trade practices. Most businesses must comply with sector-specific federal and states laws. Healthcare organisations, for example, may need to comply with the Health Information Portability and Accountability Act ("HIPAA"), and many financial institutions are required to comply with the Gramm-Leach-Bliley Act ("GLBA"). Related state laws impose additional requirements.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Financial Services: Financial services organisations must comply with the GLBA and its implementing regulations (which vary depending on the organisation's functional regulator). The SEC, other regulators and industry groups, such as FINRA and the NFA, have published cybersecurity guidance that should be carefully reviewed. Red Flag Rules published by regulators require covered firms to adopt written programs to detect, prevent and mitigate identity theft. The Fair Credit Reporting Act ("FCRA") and Fair and Accurate Credit Transactions Act ("FACTA") impose requirements with respect to credit reports.

The FTC's Disposal Rule, 16 C.F.R. § 682, issued pursuant to FACTA, requires certain practices for the destruction of certain information contained in or derived from a credit report. State regulators sometimes impose very significant further regulations, particularly in New York.

Telecommunications: The Communications Act, as enforced by Federal Communications Commission ("FCC") regulations, requires telecommunications carriers and providers of Voice over Internet Protocol ("VoIP") services to protect "customer proprietary network information". Substantial fines and penalties can be assessed for failure to ensure adequate protections.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Public company boards of directors and officers owe shareholders fiduciary duties, including the duties of care and loyalty. To fulfil these duties, among other things, boards and officers must ensure that they are properly informed regarding the company's cybersecurity risks and the efforts the company has made to address them.

In the event of an Incident, boards and officers may face scrutiny and potentially litigation relating to their oversight of the company's cybersecurity. For example, in the Yahoo! data breach, individual board members and officers faced a shareholder derivative action alleging that they failed to exercise their fiduciary duties, failed to ensure that proper security measures were in place, failed to adequately investigate the Incident and made misleading statements. The allegations were ultimately settled for a reported $29 million. In that same Incident, the Securities and Exchange Commission issued a $35 million fine.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Federal and state laws may impose specific cybersecurity requirements that depend on the entity's functional regulator and the residence of the data subject. For example, the New York Department of Financial Services has issued regulations requiring covered financial institutions (which include banks and insurance companies) to, among other things, designate a CISO (or equivalent), establish a written Incident response plan and conduct a periodic risk assessment, annual penetration testing and biannual vulnerability assessments. Massachusetts information security regulations, likewise, require organisations that collect certain Personal Information from Massachusetts residents to implement a comprehensive information security program that, among other things, identifies and assesses reasonably foreseeable internal and external risks to the security, confidentiality and integrity of such information. The New York SHIELD Act deems companies as compliant with its reasonable security requirement if they implement specified administrative, technical, and physical safeguards, including appointing an employee responsible for coordinating its cybersecurity program and regularly testing the effectiveness of key controls, systems, and procedures. While not expressly required by regulation, the Securities and Exchange Commission has identified measures such as risk assessments, Incident response plans and penetration testing as elements of a robust cybersecurity program for public companies and SEC registrants.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Public companies are required to publicly report material cybersecurity risks, including material past Incidents. Even if a past Incident is not material, companies should consider them in evaluating their disclosures regarding cybersecurity. The SEC has issued guidance regarding the factors public companies should report with respect to cybersecurity. Private companies do not have the same public disclosure obligations but may need to inform potential investors or purchasers regarding past Incidents or cybersecurity risks.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Organisations that publicly announce Incidents involving a large amount of Personal Information will often confront class action litigations filed by plaintiffs whose information was impacted by the Incident. Typically, these actions involve several theories, including breaches of express or implied contracts, negligence, other common law tort theories, violations of federal or state unfair or deceptive acts or practices statutes or violations of other state and federal statutes, such as the CCPA.

Contract theories may involve claims of breach of contract where there is a written agreement between the plaintiff and the defendant that contains an express promise of reasonable security measures to protect personal information. Even if such a term is not included in the contract, many plaintiffs will assert a claim of implied contract, arguing that the receipt of a plaintiff's personal information implies a promise to protect the information sufficiently. Tort theories may involve negligence or other common law theories such as invasion of privacy, bailment, misrepresentations with respect to cybersecurity or unjust enrichment. Each of these theories may prove challenging to fit to the data breach context; for example, bailment claims are typically dismissed because plaintiffs cannot allege that they transferred any "property" to the defendant, that the defendant promised to return the "property" or that the defendant wrongfully retained such information.

Consumer protection theories are often alleged, claiming that a victim of a data breach committed unfair or deceptive acts or practices. Deception claims are typically premised on an alleged misrepresentation about the security practices of an organisation. Plaintiffs may also allege that a failure to protect information is "unfair"; although many courts will require a showing of substantial injury or widespread and serious consumer harm. Plaintiffs may also allege violations of other statutes such as the federal Fair Credit Reporting Act or other state laws.

In addition to establishing the elements of their claims, plaintiffs filing in federal court are required to show that they suffered injury-in-fact sufficient to establish standing. Even where an injury alleged is sufficient for standing, it may not be

sufficient to state a claim for damages. Some damages theories that plaintiffs attempt to assert, with varying success, include risk of future identity theft, credit monitoring costs, other costs related to mitigating risks related to an Incident and overpayment for the products and services associated with the Incident.

While most class actions involve plaintiffs whose information was allegedly compromised, there has been an increase in shareholder derivative and securities fraud actions arising from Incidents as well. In shareholder derivative actions, plaintiffs will typically allege that a company's officers and board of directors breached their fiduciary duties, wasted corporate assets or committed other mismanagement in failing to ensure that the company maintained what the plaintiffs consider appropriate security. As a preliminary step to any derivative action, plaintiffs must first either ask the board of directors to bring the action and, should the board refuse, prove that its refusal was contrary to the board's reasonable business judgment. Alternatively, they must prove that such a request would be futile. Both theories are difficult to prove.

Plaintiffs may also allege securities fraud. To do so, plaintiffs must allege that the company made materially false or misleading statements, typically regarding the state of its cybersecurity posture, and that the company knew about the falsity of such statements.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

As noted, the public announcement of an Incident will frequently result in class actions and other lawsuits being filed against the impacted organisation. Hundreds of actions have been filed over the years; some recent prominent examples include the following:

- Altaba (formerly known as Yahoo!): After announcing an Incident allegedly impacting up to 200 million people, faced consumer class action, shareholder derivative action and securities fraud action, in addition to regulatory investigations, which it ultimately agreed to settle.
- Home Depot: Suffered an Incident related to its payment card terminals. Home Depot settled actions brought by consumers and banks, which alleged that Home Depot had failed to implement adequate security measures. Home Depot also faced a derivative action, which was dismissed. On appeal, the action was settled after Home Depot agreed to adopt certain security procedures.
- Target: Suffered an Incident related to payment card data at its retail stores. Target faced consumer and shareholder actions and also an action brought by banks related to the theft of payment card data.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes, plaintiffs in data breach actions will often accuse the defendant of negligence or other tort law violations. A preliminary question any plaintiff must answer is whether there is any duty to protect the plaintiffs' information. The answer to that question may vary by state. Courts in several states have found no common law duty to protect personal information, while courts in other states have found such a duty under particular facts and circumstances. In *Dittman v. UPMC d/b/a The University of Pittsburgh Medical Center*, for example, the Pennsylvania Supreme Court found that an employer owes a duty to employees to use reasonable care to safeguard what the court described as the employee's "sensitive" personal data when storing it on an internet-accessible computer system.

The CCPA creates a data breach right of action for Californian residents with statutory penalties of $100 to $750 per consumer and per Incident if plaintiffs prove that the impacted business failed to implement and maintain reasonable and appropriate security practices.

In some states, defendants may assert the economic loss doctrine, which generally provides that contracting parties seeking damages for purely economic losses must seek damages in contract rather than in tort.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Standalone cyber insurance policies typically cover both third-party liabilities arising from the defence and settlement of Incident-related claims, along with first-party cover for the policy holder's own losses, which could include investigation costs, legal fees, notification costs and the costs incurred in providing credit monitoring and identity theft services. Cyber insurance policy forms are typically not standardised and vary significantly from carrier to carrier.

General liability or other policies may, in some instances, cover cyber-related losses, but costs related to Incidents are often excluded.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations specific to cyber insurance, but some states do not allow for insurance against certain violations of law.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Law enforcement retains numerous powers to investigate Incidents. In addition to standard warrant and subpoena powers, law enforcement may seek records stored by electronic communication services or remote computing services through the Stored Communications Act, intercept communications in transit through the Wiretap Act or obtain dialling or routing information through the Pen Register statute. The CLOUD Act authorises law enforcement to access certain information held by a United States-based service provider, even if the data is located in another country.

For Incidents involving national security or terrorism, law enforcement may have additional powers. Under the Foreign Intelligence Surveillance Act ("FISA"), the government can obtain information, facilities or technical assistance from a broad range of entities. National Security Letters ("NSLs") offer an additional investigative tool for limited types of entities.

Federal regulatory authorities such as the FTC, SEC and the OCR have powers to investigate Incidents within their respective jurisdictions. State regulators may also investigate Incidents to determine whether any state laws were violated.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Under the Communications Assistance for Law Enforcement Act ("CALEA"), law enforcement requires certain telecommunications carriers and manufacturers to build into their systems or services necessary surveillance capabilities to comply with legal requests for information.

No general U.S. laws expressly require organisations to implement backdoors in their IT systems or provide law enforcement authorities with encryption keys. Under the All Writs Act, some courts in some instances have ordered reasonable assistance, including in one notable case, requiring Apple to provide assistance in circumventing security features – which Apple successfully resisted until it was moot.

Edward R. McNicholas is a co-leader of Ropes & Gray's privacy & cybersecurity practice. He represents technologically sophisticated clients facing complex data, privacy and cybersecurity issues. His clients include financial institutions, insurance companies, branded pharma companies, technology communications companies and select retailers. He is lead editor of the PLI Treatise, *Cybersecurity*. Recognised by the *National Law Journal* as a "Cybersecurity & Data Privacy Trailblazer", Ed has defended companies in dozens of significant data breaches. Mr. McNicholas previously served as an Associate Counsel to President Clinton, where he advised senior White House staff regarding various investigations. Mr. McNicholas received his J.D. from Harvard Law School, where he was an editor of the *Harvard Law Review*. He received his A.B. from Princeton University and served as a clerk at the U.S. Court of Appeals for the Fourth Circuit.

Ropes & Gray LLP
2099 Pennsylvania Ave, NW.
Washington, D.C. 20006-6807
USA

Tel: +1 202 508 4779
Email: Edward.McNicholas@RopesGray.com
URL: www.ropesgray.com

Kevin J. Angle is counsel in the Ropes & Gray's privacy & cybersecurity practice. He represents a broad range of companies on privacy and cybersecurity compliance matters, incident response and transactional diligence. Kevin helps clients to anticipate and address potential areas of legal exposure and to structure privacy programs to minimise potential liability. Kevin graduated from Columbia Law School and was an editor of the *Columbia Law Review*. After law school, he completed a clerkship for then Chief Judge Carol Bagely Amon of the U.S. District Court for the Eastern District of New York.

Ropes & Gray LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
USA

Tel: +1 617 951 7428
Email: Kevin.Angle@RopesGray.com
URL: www.ropesgray.com

Ropes & Gray is a leader in helping clients navigate the increasingly complex legal landscape surrounding data. Veterans in managing global advisory matters and responding to litigation and investigations stemming from security incidents and alleged privacy violations, the team is particularly distinctive in its innovative work advising on transactions involving the acquisition and management of data.

www.ropesgray.com

ROPES & GRAY

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by: global legal group