Baker McKenzie.

Cybersecurity Forum: From Risk to Readiness

November 8, 2022

ACC Association of Corporate Counsel CHICAGO

Agenda

1. Threat landscape
2. Types of attack
3. Risks/pre-attack preparation
4. Regulatory and Law Enforcement Concerns
5. Cyber Risk Insurance
6. Response
7. Remediation
8. Board level considerations


1
Threat landscape

Trends in cyber attacks

Ransomware example

From: Candidate, Joe <joe.candidate@gmail.com>
Sent: Monday, September 15, 2015 10:58 AM
To: <hrdirector@yourcompany.com>
Subject: Open Position
Attachments: Resume.pdf

Dear HR Director,

Please see my resume attached.

Thanks,

Joe

Trends in cyber attacks

Ransomware example

From:
Sent:
To:
Subject:
Attachments:

Dear HR Director,

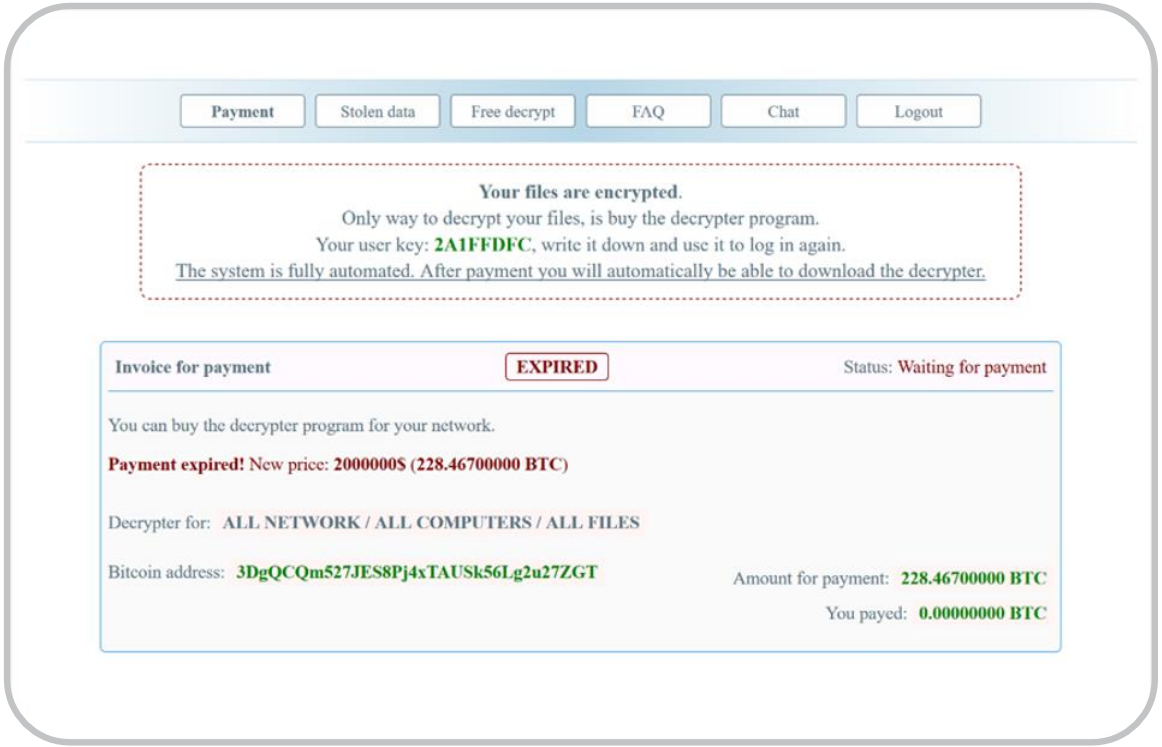
Please see my resume a

Thanks,

Joe

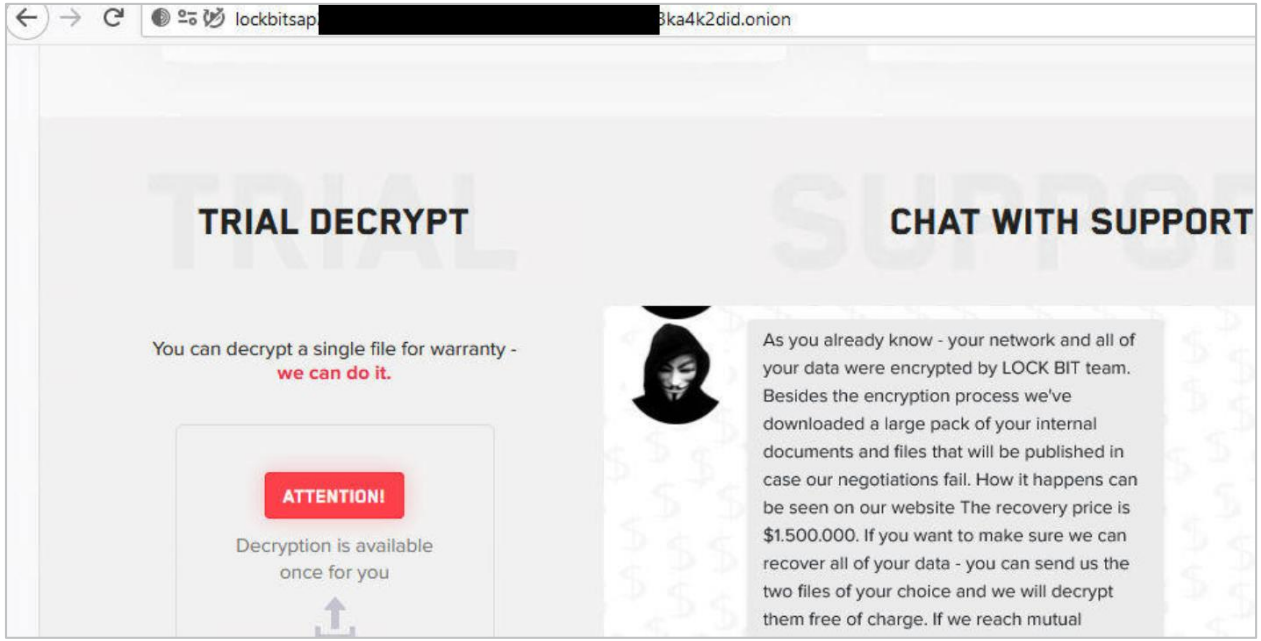
Trends in cyber attacks

More recent ransomware example



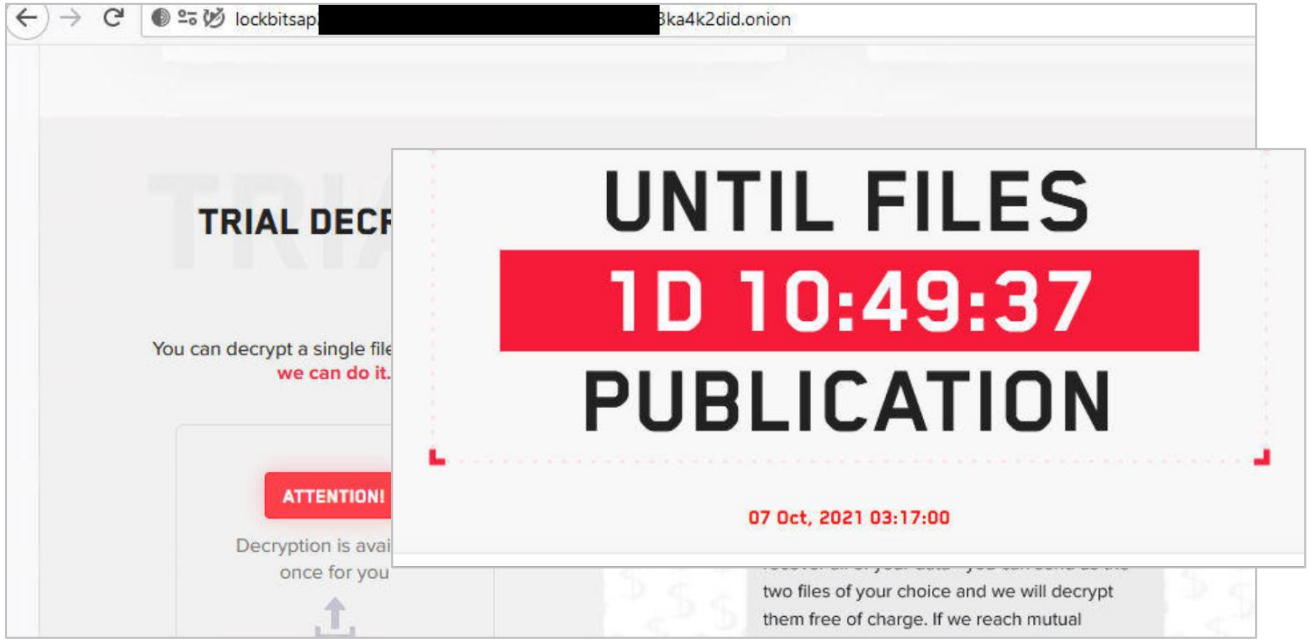
Trends in cyber attacks

Current ransomware example



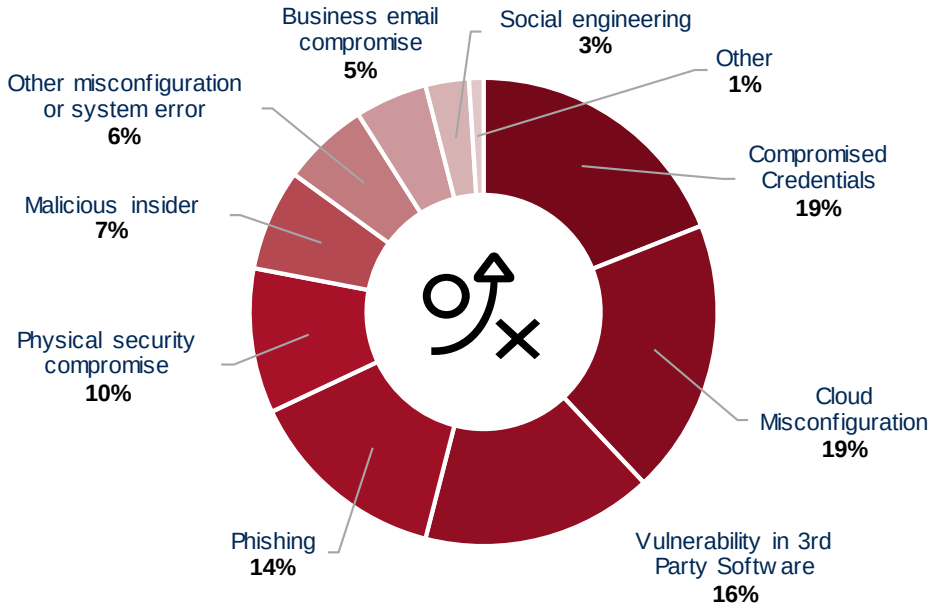
Trends in cyber attacks

Current ransomware example



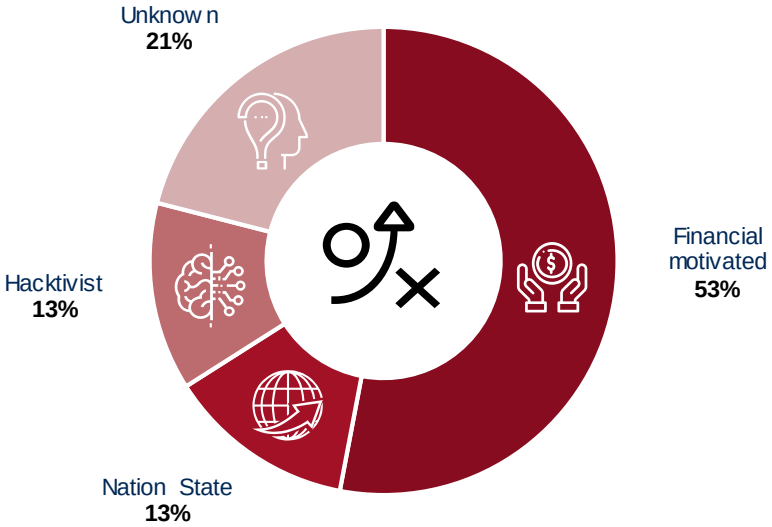
Threat landscape

Malicious attack threat vectors

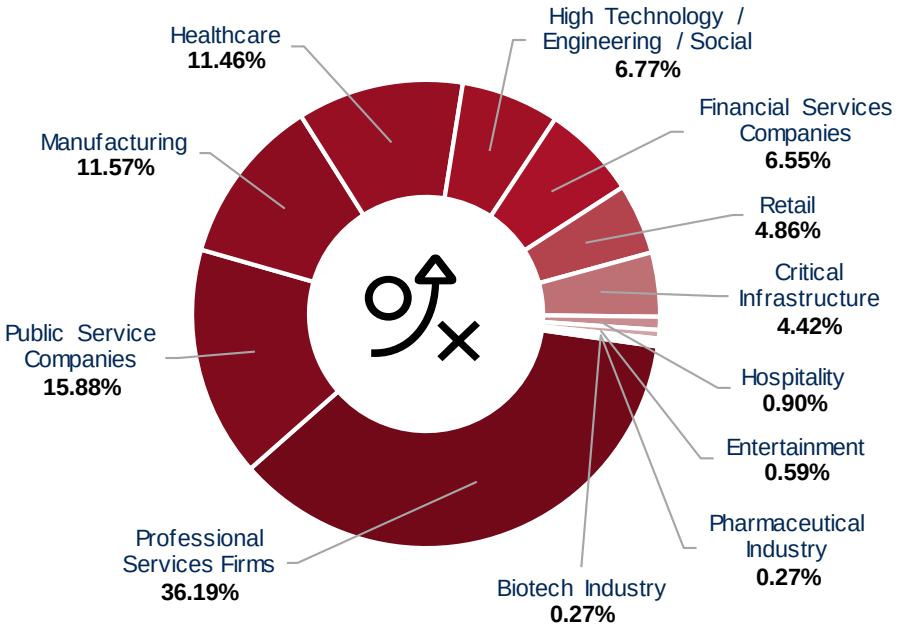


Threat landscape

Threat actors



Industries targeted by ransomware



Source: 2500+ Arete Cases


2
Types of attack

Types of cyber attacks

Phishing

- Fraudulent attempt to steal personal information
- Business Email Compromise (BEC): usually through personalized targeted emails which impersonate a legitimate email sender
- Often used as an entry point to a network to then deploy malware

Malware

- Code with malicious intent during a cyber attack
- E.g., viruses, worms, Trojans, spyware etc.
- Often multiple malware types deployed for different purposes during an attack

Ransomware

- Encrypts files until a ransom is paid
- Modern ransomware now attempts to exfiltrate data – double threat ransomware
- Third parties are often also ransomed – triple threat ransomware

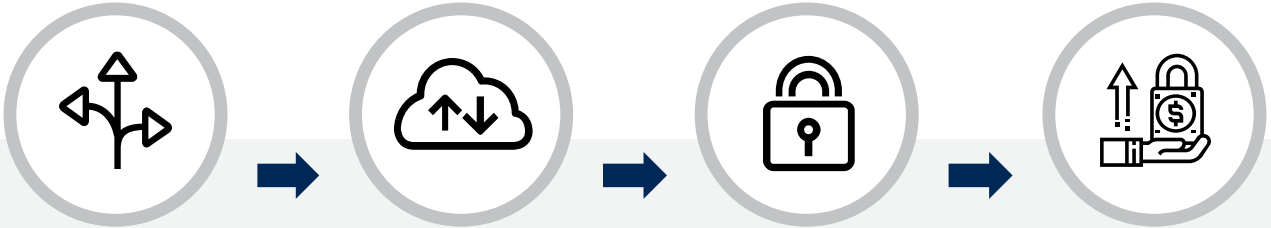
Denial-of-Service attacks

- Focuses on disrupting the service to a network
- Occurs by sending high volumes of data or traffic through the network until it becomes overloaded and can no longer function
- Can be used to disguise / enable other attacks

Ransomware

How it works

Ransomware is a form of malware that encrypts files – making them inaccessible without the encryption key



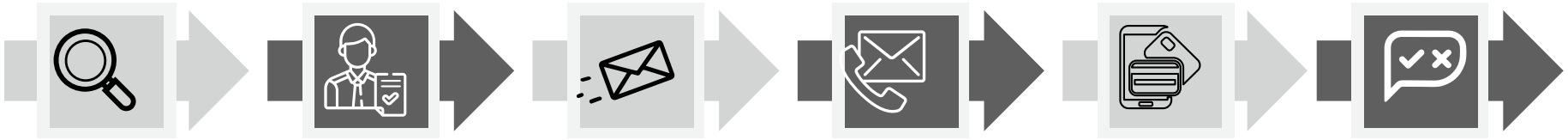
Access, escalation, and mapping

Potential theft of data

Execution of malware to encrypt files

Ransom demand

Misdirected funds scam



Surveillance of target company

- Public information
- Inside information (phishing/ hacked)

Identify key individuals

- CEO
- CFO
- Financial Controller
- Bank customers
- Bankers

Fraudulent email requesting transfer

- Appears legitimate
- From similar/ same address
- From hacked account
- Timing

Pressure emails/ follow-up calls

- Further email exchanges/ calls with imposter

Transfer to fraudster's account

- Overseas account
- Money moved again (hard to trace)

Further requests

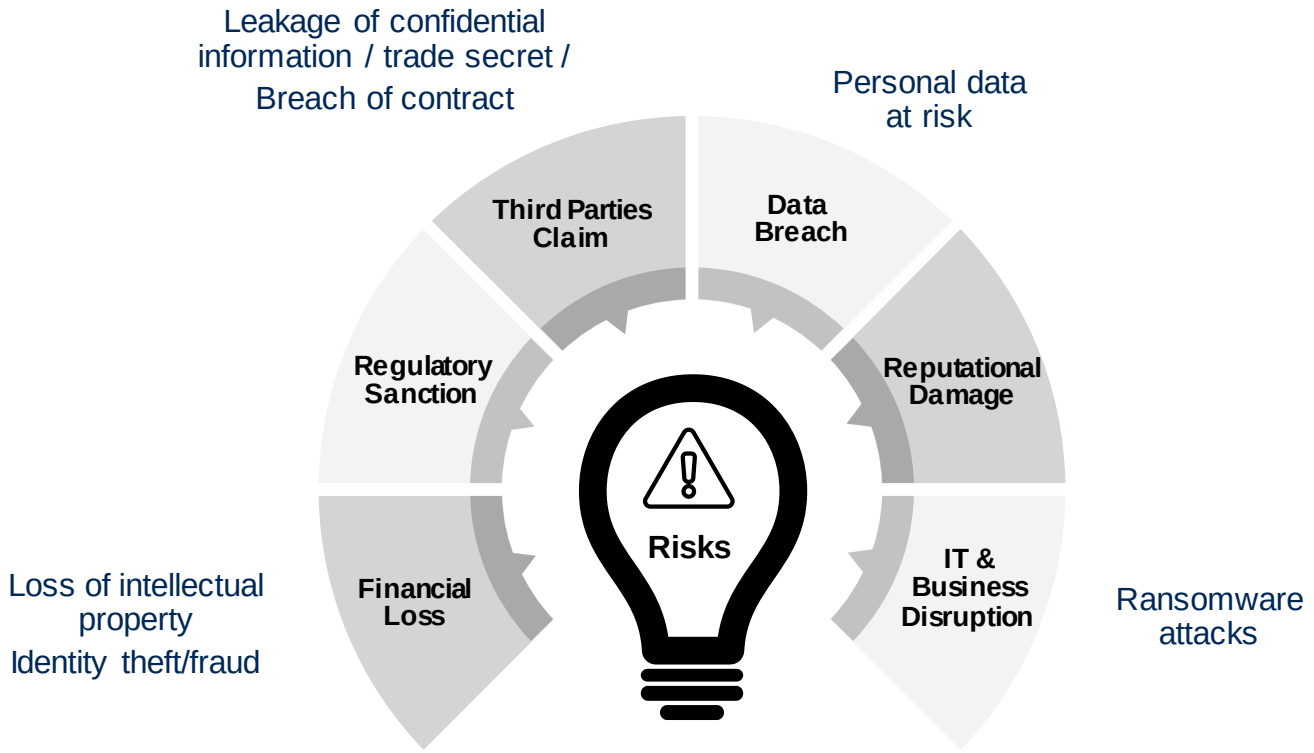
- Often successful
- Not worried about being caught

> Mary, I have an urgent secret investment that requires you to transfer payment to Hong Kong. It's a rare opportunity arising from the COVID-19 situation. The responsible lawyer will send you the transfer details shortly.

> Tom, the supplier for surgical masks requires us to re-direct our payment to a company in Hong Kong. Please arrange for payment urgently as I need to secure the shipment. Here are the remittance instructions.


3
Risks/pre-attack preparation

Cybersecurity risks



Pre-Attack Preparation

- What InfoSec/Privacy preparations should be done?
- What decisions / engagements should be made upfront?
- Incident response plan and testing

Attack Response

- Internal communications
- Technical response
- Outward response
- Project/crisis management
- Legal / risk response

Post-Attack Remediation

- Addressing regulator & enforcement inquiries
- Possible litigation
- PR issues
- Technical response

Pre-Attack Preparation

Action Items

Data Security Incident Response Plan and Trainings

Avoidance

- Back-up systems segregated sufficiently?
- Operational recovery plan practiced?
- Back-up communications solutions in place?
- Business continuity plan?
- "Crown jewels" assessments

Engagement of Response Providers

- Baker McKenzie
- Forensic Investigators
- eDiscovery Providers
- Public Relations / Crisis Management
- Credit Monitoring / Identity Theft Protection / Call Center
- Ransom Negotiators / Payors

Insurance

- Review and understand scope of cyber insurance coverage

Pre-Attack Preparation

Decision Points

Moral / PR / Corporate Decisions

- Is the company against paying ransoms?
- PR considerations
- Different approaches for different business segments?

Operational Issues

- Who pays and how (e.g., from what accounts)?
- Insurance requirements?
- Who/how to engage with attacker?

Regulatory Issues

- Diligence requirements for payments
- OFAC guidance
- SEC and market regulators

Law enforcement notification strategy

4

Regulatory and Law Enforcement Concerns

OFAC Advisory on Ransomware Payments

Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.[2]

OFAC will also consider a company's full and ongoing cooperation with law enforcement both during and after a ransomware attack — e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible — to be a significant mitigating factor.

OFAC strongly encourages all victims and those involved with addressing ransomware attacks to report the incident to CISA, their local FBI field office, the FBI Internet Crime Complaint Center, or their local U.S. Secret Service office as soon as possible.

Cooperation with Law Enforcement

From: [redacted]@gmail.com>
Sent: Sunday, May 30, 2021 9:41 PM
To: [redacted]@fbi.gov>
Subject: [EXTERNAL EMAIL] - Sodinokibi

[redacted]

My name is [redacted] and I am General Counsel for JBS USA Food Company, a subsidiary of JBS SA, the world's largest food company.

Today we suffered a cyber attack and ransom demand by Sodinokibi. I understand you are the lead Agent handling issues with this threat actor.

If you could please give me a call on my cell as soon as possible (number below), I would very much appreciate it.

Thank you,
[redacted]
General Counsel
[redacted]

On May 31, 2021, at 11:23 AM, [redacted]@fbi.gov> wrote:

Hello [redacted]

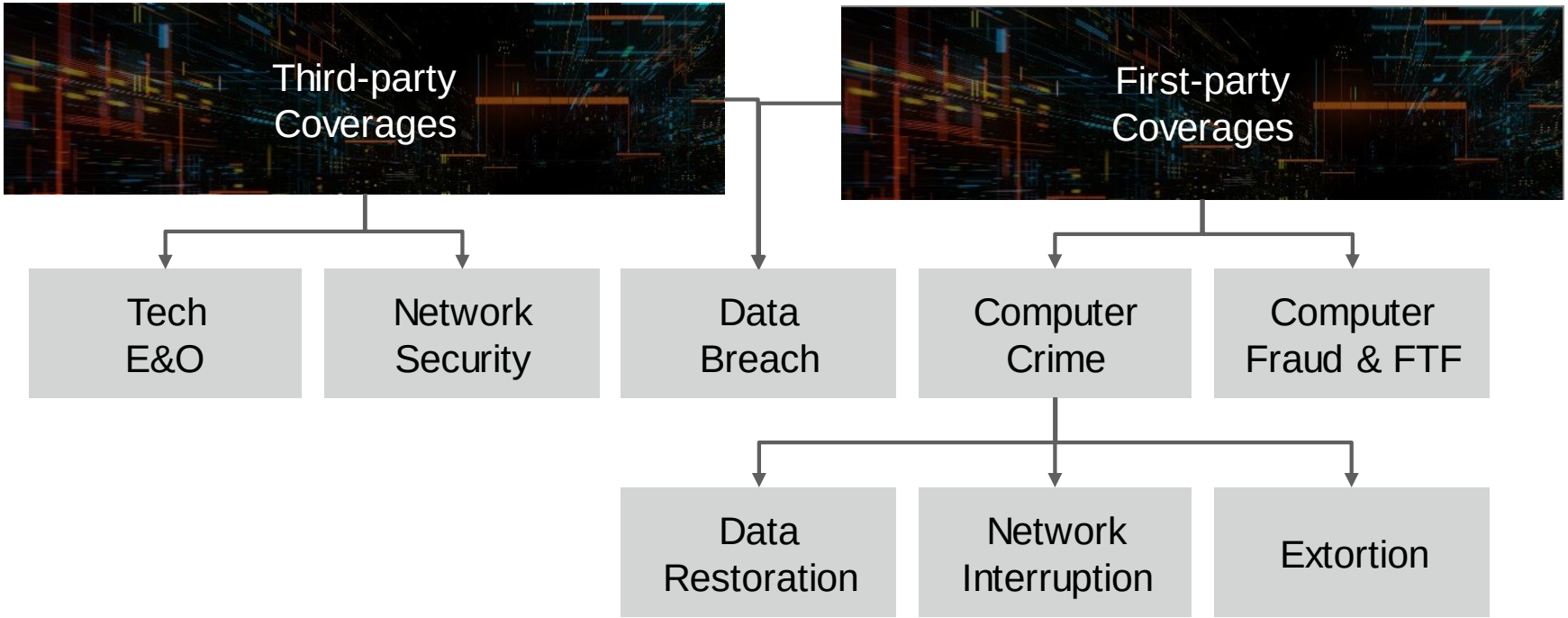
My apologies for the delay in replying. I am not the case Agent for Sodinokibi. The lead case Agents for Sodinokibi are SA's [redacted] (copied). Please feel free to go direct with either of them.

Special Agent [redacted]
Federal Bureau of Investigation
[redacted]

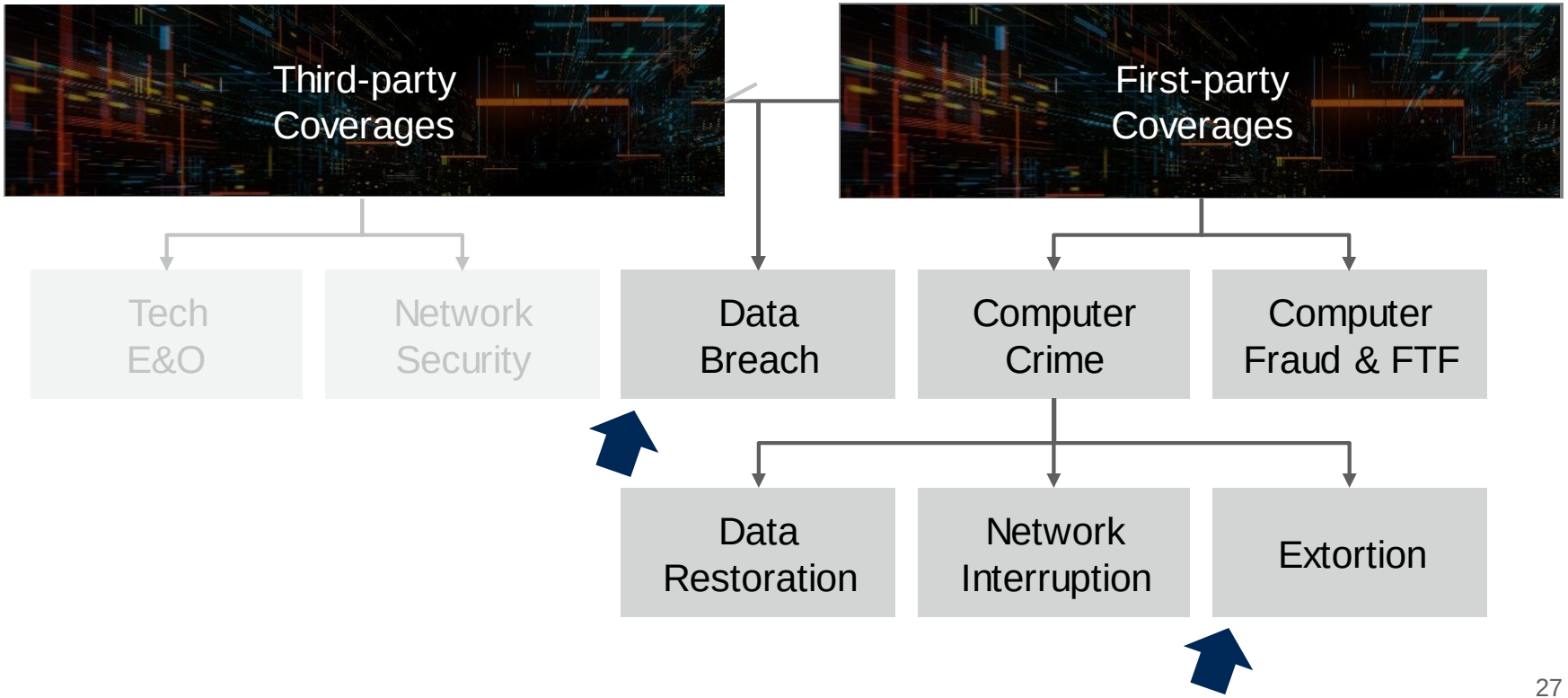

5
Cyber Risk Insurance

Cyber Risk Insurance:
An Evolving Landscape

Cyber Insurance: Types of Coverages



Cyber Insurance: Types of Coverages



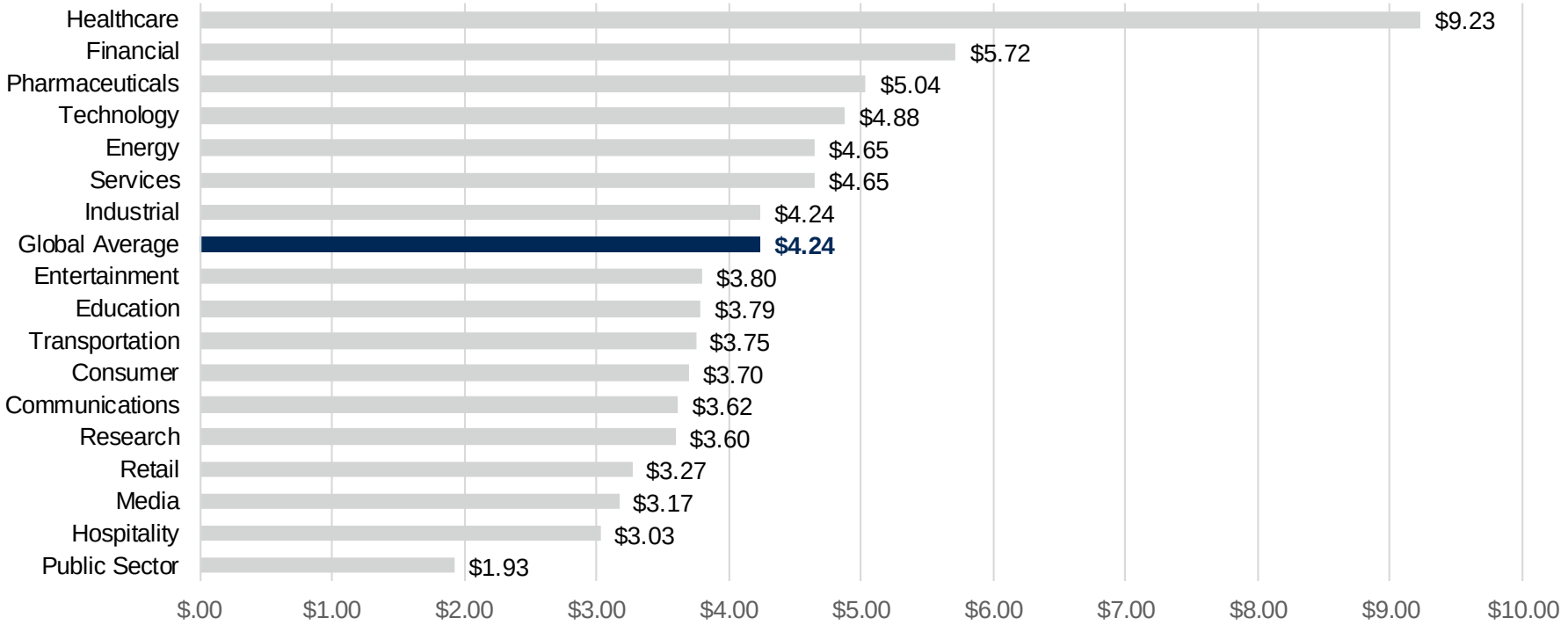
Cyber Insurance: Watch for Sub-limits

Third Party Liability Insuring Agreements			
Coverage	Limit of Insura	Retention	Retroactive Date
		$10,000	08/10/2017
		$10,000	08/10/2017
	ed	Not Purchased	Not Purchased
	ed	Not Purchased	Not Purchased

First Party Insuring Agreements		
Coverage	Limit of Insurance	Retention
E. Incident Response Coverage Inside the Aggregate Limit of Insurance		
1. Breach Consultation	$5,000,000	$10,000
2. Data Forensics	$5,000,000	$10,000
3. Breach Response – In addition to the Aggregate Limit of Insurance	50,000 Individuals	$10,000
4. Public Relations	$5,000,000	$10,000
F. PCI Expenses Coverage	Not Purchased	Not Purchased
G. Network Extortion Coverage	$5,000,000	$10,000
H. Cyber Crime Coverage	$100,000	$10,000
1. Social Engineering Fraud Coverage	$100,000	$10,000
2. Telecommunications Fraud Coverage	$100,000	$10,000
3. Funds Transfer Fraud Coverage	$100,000	$10,000
I. Data Restoration Coverage	$5,000,000	$10,000

Average total cost of a data breach by industry

Measured in U.S.$ millions



Source: Ponemon 2021 Cost of a Data Breach Report

Cyber Insurance: Underwriting Process

PRIVACY CONTROLS

6. Indicate whether the Applicant currently has the following in place:

a.	A Chief Privacy Officer or other individual assigned responsibility for monitoring changes in statutes and regulations related to handling and use of sensitive information	☐ Yes	☐ No
b.	A publicly available privacy policy which has been reviewed by an attorney	☐ Yes	☐ No
c.	Sensitive data classification and inventory procedures	☐ Yes	☐ No
d.	Data retention, destruction, and recordkeeping procedures	☐ Yes	☐ No
e.	Annual privacy and information security training for employees	☐ Yes	☐ No
f.	Restricted access to sensitive data and systems based on job function	☐ Yes	☐ No

Cyber Insurance: Underwriting Process

NETWORK SECURITY CONTROLS

7. Indicate whether the Applicant currently has the following in place:

a. A Chief Information Security Officer or other individual assigned responsibility for privacy and security practices	☐ Yes	☐ No	
b. Up-to-date, active firewall technology	☐ Yes	☐ No	
c. Up-to-date, active anti-virus software on all computers, networks, and mobile devices	☐ Yes	☐ No	
d. A process in place to regularly download, test, and install patches	☐ Yes	☐ No	
If Yes, is this process automated?	☐ Yes	☐ No	
If Yes, are critical patches installed within 30 days of release?	☐ Yes	☐ No	
e. Intrusion Detection System (IDS)	☐ Yes	☐ No	
f. Intrusion Prevention System (IPS)	☐ Yes	☐ No	
g. Data Loss Prevention System (DLP)	☐ Yes	☐ No	
h. Multi-factor authentication for administrative or privileged access	☐ Yes	☐ No	☐ N/A
i. Multi-factor authentication for remote access to the Applicant's network and other systems and programs that contain private or sensitive data in bulk	☐ Yes	☐ No	☐ N/A
j. Multi-factor authentication for remote access to email	☐ Yes	☐ No	☐ N/A
k. Remote access to the Applicant's network limited to VPN	☐ Yes	☐ No	☐ N/A
l. Backup and recovery procedures in place for all important business and customer data	☐ Yes	☐ No	
If Yes, are such procedures automated?	☐ Yes	☐ No	
If Yes, are such procedures tested on an annual basis?	☐ Yes	☐ No	
m. Annual penetration testing	☐ Yes	☐ No	
If Yes, is such testing conducted by a third party service provider?	☐ Yes	☐ No	
n. Annual network security assessments	☐ Yes	☐ No	
If Yes, are such assessments conducted by a third party service provider?	☐ Yes	☐ No	
o. Systematic storage and monitoring of network and security logs	☐ Yes	☐ No	
p. Enforced password complexity requirements	☐ Yes	☐ No	
q. Procedures in place to terminate user access rights as part of the employee exit process	☐ Yes	☐ No	

Cyber Insurance: Watch for Exclusions

A. **EXCLUSIONS APPLICABLE TO ALL INSURING AGREEMENTS**

This Policy does not cover **Loss**, **Breach Consultation**, **Breach Response**, **Public Relations Costs**, **Data Forensics**, **PCI Expenses**, **Network Extortion Expenses**, **Social Engineering Fraud Loss**, **Telecommunications Fraud Loss**, **Funds Transfer Fraud Loss**, **Digital Assets Restoration Costs**, **Business Interruption Costs**, or **Cyber Expenses**:

* * *

3. alleging, arising out of, or based upon war, invasion, acts of foreign enemies, nations, groups or natural persons, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power; provided, however, that this Exclusion shall not apply to **Cyberterrorism**.


6
Response

Key Response Elements

Key Initial Decisions and First Steps

Engagement of Law Enforcement?

Decision to Pay

Engagement with Insurance

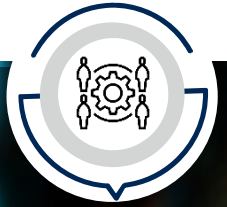
Incident Investigation and Litigation Preparation

Responding to an Attack

Gather information / Contain the breach

Report to Enforcement Authorities / Regulators

Court injunctions



Recovery actions

Dealing with third party recipients

Breach notification obligations

Notification to Banks

Bank Disclosures

Corporate / employee investigations

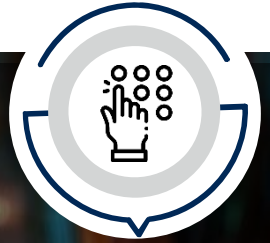
Training and Cybersecurity Advice

7

Remediation

Post-Attack Remediation

Investigations



Technical response

Notifications and Responding to Inquiries

Post-Attack Remediation

Technical Response

Systems Response

- Decryption of systems
- Restarting systems
- Verification that systems are clean
- Deployment of enhanced security measures
- Scanning for additional / latent threats
- Patching
- Ongoing monitoring

Post-Attack Remediation

Investigation

- Forensics
  - Understand the scope of the issue
  - Confirmation/identification of exfiltrated information
  - Examination of impacted/exfiltrated information
- Determination of legal requirements
- Determination of remediation elements

Post-Attack Remediation

Notifications and Responding to Inquiries

- Notification obligations
  - Regulators
  - Enforcement authorities
  - Customers
  - Individuals
- Regulator/Enforcement authority inquiries
- Customer inquiries
- Individual inquiries
- Litigation preparation/response

8

Board level considerations

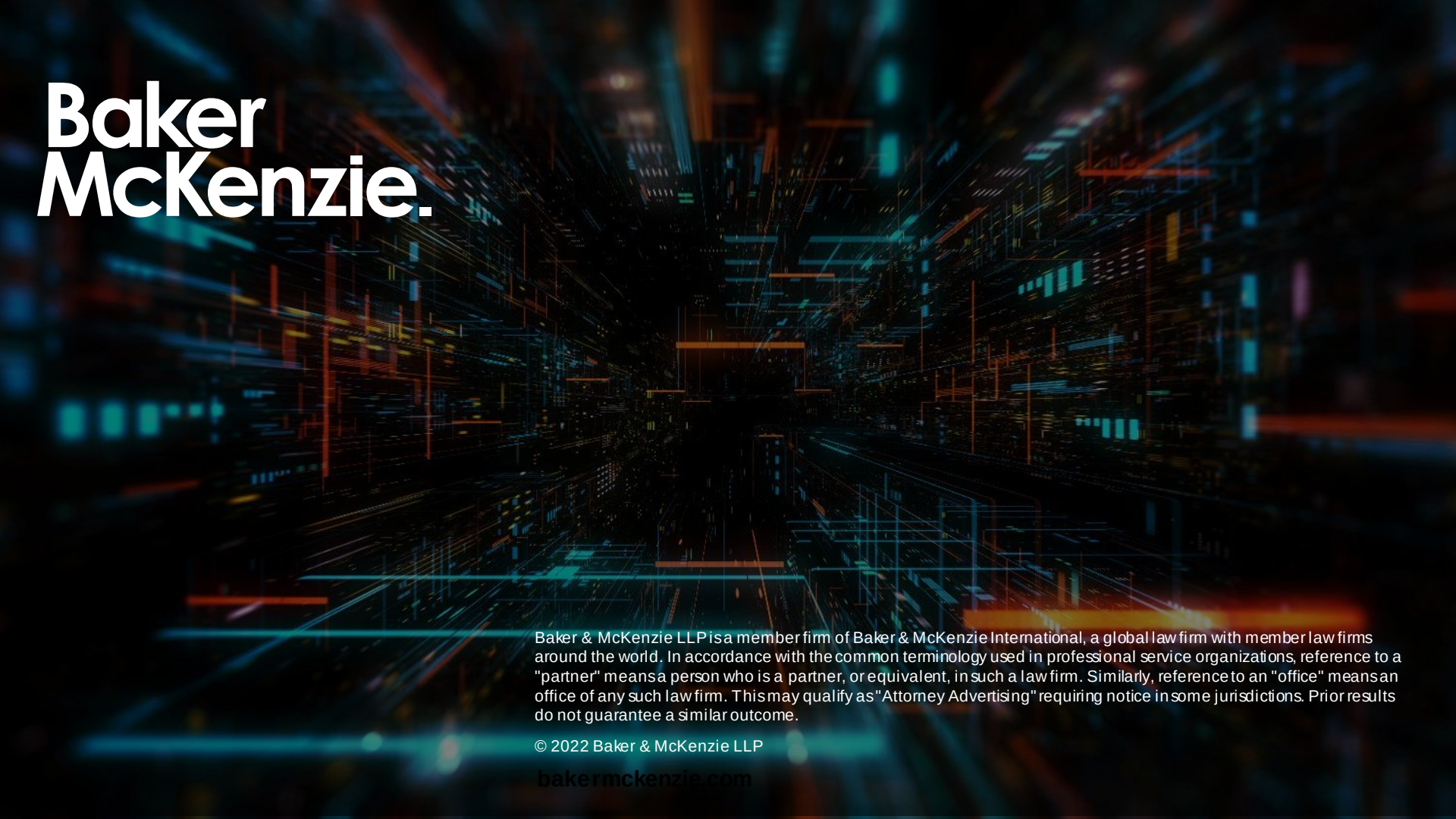
Cybersecurity

Board level issues

Is the board confident that:

- All key information assets have been identified and their vulnerability to attack thoroughly assessed?
- Responsibility for the cyber risk has been allocated appropriately?
- Cybersecurity is featured on the risk register?
- A written data breach incident procedure and information security policy is in place, which is championed by the board and supported through regular staff training?
- The entire workforce understands and follows the company's breach procedure and security policy?

Cybersecurity risk impacts share value, mergers, pricing, reputation, culture, staff, information, process control, brand, technology, and finance



bakermckenzie.com