wiley

Cyber Risk in a Changing Environment: Emerging Regulations and Lessons from the Front Lines

May 19, 2022

Agenda

- Where is government headed with new mandates, substantively and in reporting?
- What key outside resources and standards should corporate counsel familiarize themselves with?
- What should be top of mind for internal governance and risk management?
- What should you know about ransomware response and risk management?
- Key lessons and best practices

Regulatory landscape: new obligations emerging

New mandates: DHS CISA Incident Reporting

- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)
  - Signed into law on March 15, 2022 by President Biden
  - Bipartisan legislation requiring owners and operators of critical infrastructure to report cyber incidents to U.S. Dep't of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)
  - Not effective until CISA promulgates rules to define the types of entities and cybersecurity incidents that will be subject to the law

Where is government headed?	Outside resources	Internal governance and risk mgmt.	Ransomware risk and response	Key lessons

DHS CISA Incident Reporting: Who and When?

Required Timing

- **Significant Cyber Incident:** When there is a reasonable belief that a significant cyber incident has occurred, the covered incident must be reported to CISA **within 72 hours**.
- **Ransomware Payment:** When a covered entity has made a ransomware payment, CISA must be notified within **24 hours of ransom payment.**

Who Will Have to Report?

CRITICAL INFRASTRUCTURE	
Chemical	Financial Services
Commercial facilities	Food & Agriculture
Communications	Government Facilities
Critical Manufacturing	Healthcare, Public Health
Dams	Information Technology
Defense Industrial Base	Nuclear Reactors, Materials, Waste
Emergency Services	Transportation
Energy	Water, Wastewater Systems

DHS CISA Incident Reporting: Anticipated Requirements

CISA wants critical infrastructure entities to report the following types of activities to CISA:

1. Unauthorized system access
2. Denial of Service (DOS) attacks that last more than 12 hours
3. Malicious code found on systems, including any variants, if known
4. Targeted and repeated scans against services on systems
5. Repeated attempts to gain unauthorized access to a system
6. Email or mobile messages associated with phishing attempts or successes
7. Ransomware attacks against critical infrastructure, including the variant and ransom details

In the meantime, DHS identifies Top 10 Key Elements to Share Voluntarily

1. Incident date and time
2. Incident location
3. Type of observed activity
4. Detailed narrative of the event
5. Number of people or systems affected
6. Company/Organization name
7. Point of Contact details
8. Severity of event
9. Critical Infrastructure Sector, if known
10. Anyone else the victim informed

How to report cyber incidents today

- CISA Incident Reporting System: Critical infrastructure partners can complete an incident report form which contains a variety of prompts and a convenient way to electronically report.
  - Reports@cisa.gov: Critical infrastructure entities that have never used the CISA Incident Report System or want to expeditiously submit a report, can send an email to Reports@cisa.gov with as much information about the cyber event as they can.
  - Phishing-report@us-cert.gov: Entities can also share phishing information regarding phishing emails, mobile messages, and website locations by sending an email to phishing-report@us-cert.gov.
- FBI's Internet Crime Complaint Center (IC3.GOV): Report Business Email Compromises, Ransomware Attacks, or other scams directly to the FBI. Also contains industry and consumer alerts on cyber threats.
- StopRansomware: the consolidated U.S. Government one-stop for reporting ransomware and contains resources to tackle ransomware more effectively.
- Shields Up: Cyber threat updates, private sector guidance and recommendations, resource links

New Mandates: SEC Public Disclosures

- Current reporting of material cybersecurity incidents and governance covered by 2018 and 2011 SEC guidance
- Proposed amendments to SEC rules (March 2022)
  - Mandatory public disclosure of material cyber incidents within 4 business days of a materiality determination
  - Public disclosure about company policies and procedures to identify and manage cybersecurity risks; BOD oversight of cybersecurity risk; and management's role and expertise in assessing and managing cybersecurity risk
  - Substantial criticism of rule as in tension with other regimes and broader cyber policy
- Builds on investigations SEC has been doing into high profile incidents, like SolarWinds and insider trading

Where is government headed?	Outside resources	Internal governance and risk mgmt.	Ransomware risk and response	Key lessons

Increasing regulatory oversight

- Substantive and reporting obligations imposed on sectors
  - Pipeline security directives (covered entities must (1) report confirmed and potential cybersecurity incidents to CISA; (2) designate a Cybersecurity Coordinator to be available 24 hours a day, seven days a week; (3) review current practices; (4) identify any gaps and related remediation measures to address cyber-related risks and report the results to TSA and CISA within 30 days.)
  - Security directives for surface transportation, SD 1582-01 (owners and operators must (1) designate a cybersecurity coordinator; (2) report cybersecurity incidents to CISA within 24 hours; (3) develop and implement a cybersecurity incident response plan to reduce the risk of an operational disruption; complete a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems.)
- Department of Justice announced intent to use False Claims Act to pursue civil fraud against contractors who misstate or fail to disclosure cyber incidents
- DoD leadership conducts oversight of the DoD supply chain for DFARS cyber clause compliance.

Key resources and standards

What should be top of mind for internal governance and risk management?

- How is your working relationship with your CISO and senior management?
- Has the team practiced your incident response plan?
  - Have you mapped potential reporting obligations?
- Is it clear when legal will be involved and how you will assert and protect privilege?
  - Not just for incident response, but also for vulnerability assessments and compliance tasks
- Is there an identified recipient of government alerts and advisories?
- Do you have vendors (forensic, ransomware) lined up?

How does insurance affect governance and risk management?

- Insurance considerations
- How to get insurance
- How to use your insurance

Key ACC resources can help

- Cybersecurity checklists
  - NIST Cybersecurity Framework: A Quick Start Guide (https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide)
  - FINRA (https://www.finra.org/compliance-tools/cybersecurity-checklist)
  - TitanFile's Top 5 (https://www.titanfile.com/blog/cybersecurity-checklist/)
  - Secure Community (https://cdn.fedweb.org/fed-91/2/Cybersecurity_Checklist_v2.pdf)
- Existing materials published by ACC

Key third-party resources and standards

- SANS 20 Critical Security Controls, also known as the Center for Internet Security's *Critical Security Controls Version 8*, https://www.cisecurity.org/controls/v8
- ISO/IEC 27001:2013 certification; ISO 27001 consists of 114 controls and 10 management system clauses that support implementation and maintenance of an information security management system.
  - ISO 27701 is an add-on to on the requirements and controls of the widely adopted information security management standard ISO 27001 and provides and extension to ISO 27001 through privacy-specific requirements and controls.
- SOC 2, from American Institute of CPAs (AICPA), offers criteria for managing customer data using five "trust service principles"—security, availability, processing integrity, confidentiality and privacy. https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations
  - Type I describes a vendor's systems and whether their design is suitable to meet relevant trust principles.
  - Type II details the operational effectiveness of those systems.

Where is government headed?	**Outside resources**	Internal governance and risk mgmt.	Ransomware risk and response	Key lessons

Key government resources for corporate counsel

- NIST Framework for Improving Critical Infrastructure Cybersecurity (under revision)
  - Informative resources, https://csrc.nist.gov/projects/olir
  - Associated mappings relevant to your sector
- Key NIST Publications on IoT, Risk Management Framework, Zero Trust (SP 800-207), and ransomware (NISTIR 8374)
- DHS CISA
  - Playbooks on Incident and Vulnerability Response
  - Critical infrastructure performance goals https://www.cisa.gov/control-systems-goals-and-objectives
- Federal Trade Commission guidance
  - Cyber insurance underwriting guidance https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

Key government cyber resources

- Attorney General's Cyber Digital Task Force (https://www.justice.gov/archives/ag/page/file/1076696/download)
- DOJ's Best Practices for Victim Response and Reporting of Cyber Incidents (https://www.justice.gov/criminal-ccips/file/1096971/download)
- DOJ/DHS Guidance to assist the private sector with sharing cyber information (https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf)
- NIST Cybersecurity Framework https://www.nist.gov/cyberframework)
- InfraGuard: FBI's partnership with the private sector (https://www.infragardnational.org/)
- National Counterintelligence and Security Center: cybersecurity, insider threat, supply chain threats, physical security (https://www.dni.gov/index.php/ncsc-what-we-do)
- National Cyber-Forensics and Training Alliance (NCFTA): companies, government, and academia working together to neutralize cyber crime (https://www.ncfta.net/)
- DOJ's Intellectual Property Victim Guide (https://www.justice.gov/criminal-ccips/file/891011/download)
- SEC Cybersecurity (https://www.sec.gov/spotlight/cybersecurity)
- CLOUD Act Resources (https://www.justice.gov/dag/cloudact)

Government resources: advisories and alerts

- Companies should have a way to monitor and consider acting on the varied government alerts about cyber and geopolitical risk
  - CISA Shields Up Latest Updates (https://www.cisa.gov/shields-up)
  - CISA/US-CERT Alerts (https://www.cisa.gov/uscert/ncas/alerts)
  - FBI IC3 Industry Alerts (https://www.ic3.gov/Home/IndustryAlerts)
  - NSA Cybersecurity Advisories and Guidance (https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/)

- Supply chain risk is harder to track but companies need a way to stay on top of developments
  - Sanctions and export controls
  - Supply chain advisories
    - C-SCRIP out of NTIA on supply chain risks
    - NDAA Section 889 prohibition, along with Federal Acquisition Supply Council, FCC and DoD lists of companies associated with nation-state adversaries

Working with the government

- Building relationships in advance
  - Contact your local FBI field office (https://www.fbi.gov/contact-us/field-offices)
  - Contact the FBI's Office of Private Sector (https://www.fbi.gov/about/partnerships/office-of-private-sector)
  - Contact CISA for a cyber hygiene assessment (https://www.cisa.gov/cyber-hygiene-services)

Working with the FBI

- FBI's goal: find the bad actors and get them out of your systems
- FBI is committed to treating cyber attack victim as crime victim
  - Tries not to disturb business by using investigative measures that avoid computer downtime or displacing company employees
  - Works discretely to not cause unwarranted disclosure of information
    - Protects information from release (e.g., FOIA, CISA 2015)
    - Obfuscates identity in legal documents whenever possible
    - Doesn't share information with regulators
  - Is interested in technical details re intrusion – not sensitive internal communications
- Benefits of cooperation
  - May recover ransom payments
  - Can help mitigate damage and recovery quickly
  - Can work with foreign partners to recover data stolen overseas

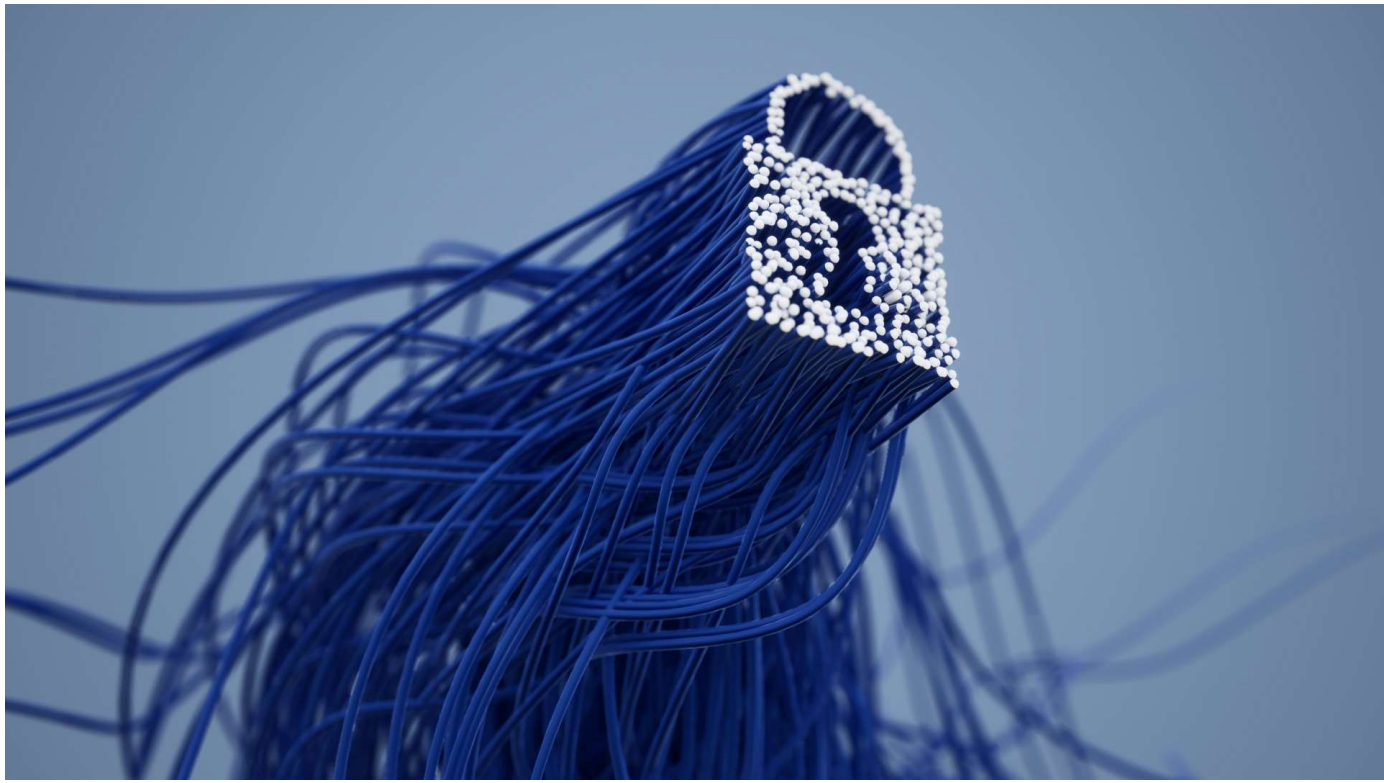
Current cyber threat picture

- Cyber threats are widespread
  - **Criminals** pursue cyber-enabled crime for **financial gain**
  - **Nation-state actors** conduct computer intrusions targeting proprietary information
  - **Combination** of the two (bad actors moonlighting for nation-states)
- Cyber-attacks are becoming more commonplace, dangerous, and sophisticated no matter the actor or motivation
- FBI estimates potential losses of $6.9 Billion from cyber crime in 2021 for a total of $18.7 Billion in losses in the last 5 years (2017-2021)
- Ongoing upward trend in the growth of phishing attacks, cybercriminal services-for-hire, and ransomware losses in 2022

Common crimes and online risks

- **Business email compromise (BEC)** scams exploit the fact that so many of us rely on email to conduct business—both personal and professional—and it's one of the most financially damaging online crimes.
- **Identity theft** happens when someone steals your personal information, like your Social Security number, and uses it to commit theft or fraud.
- **Ransomware** is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.
- **Spoofing and phishing** are schemes aimed at tricking you into providing sensitive information to scammers.
- **Malware** to harvest credentials through phishing emails or fake bank sites.

Ransomware



What is ransomware?

- Ransomware is a form of malware that targets your critical data and systems for the purpose of extortion.
- Ransomware affects organizations of all types and sizes.
- “Commodity” ransomware has relatively low extortion demands.
- “Big game hunting” may have demands ranging from several hundred thousand to more than $20 million.

Ransomware tactics are evolving

Ransomware Today is a Three Punch Combination:

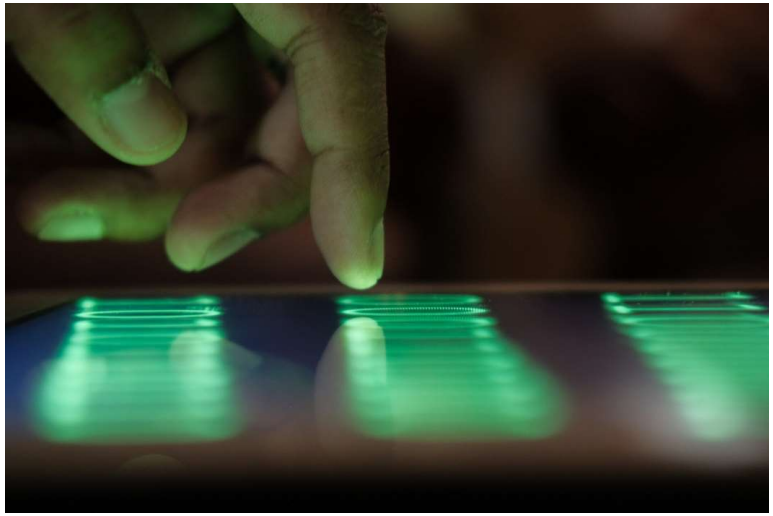
- Encryption and Disruption
- Disclosure of Confidential, Personal, and Health Information
- Aftermath: Recovery, Restoration, and Business Impact

What does a ransomware attack look like in practice?

- Initial triage
- Ransomware-specific decision points
- Recovery
- Communication
- Remediation and avoidance of future threats

Managing the Risk of Ransomware

- Risk can be managed from a technological or process perspective.
- Risk can also be managed from a financial perspective.
  - Indemnification
  - Insurance
- Insurance is available to address certain aspects of the risk, but the market is developing.



Where is government headed?	Outside resources	Internal governance and risk mgmt.	**Ransomware risk and response**	Key lessons

Managing the Risk of Ransomware

Technology/Process Risk Management:

- Incident response plans
- Identify and educate key stakeholders and their roles in the event of a ransomware incident
- Identify critical infrastructure, applications, data, and their internal owners
- Understand internal/external competencies and limitations and assign internal owners
- Identify key legal, forensics, notification, public relations, crisis management, negotiation, and payment vendors
- Set expectations about cost, time, resources

Managing the Risk of Ransomware

Financial Risk Management:

- A stand-alone cyber insurance policy is often viewed as the foundational financial risk management tool.
- The market is changing.
  - "Hard" market
  - Ransomware sub-limits
  - Coinsurance
- Traditional insurance may be available.
  - But data security risks are being addressed

Where is government headed?	Outside resources	Internal governance and risk mgmt.	**Ransomware risk and response**	Key lessons

Third-party risk

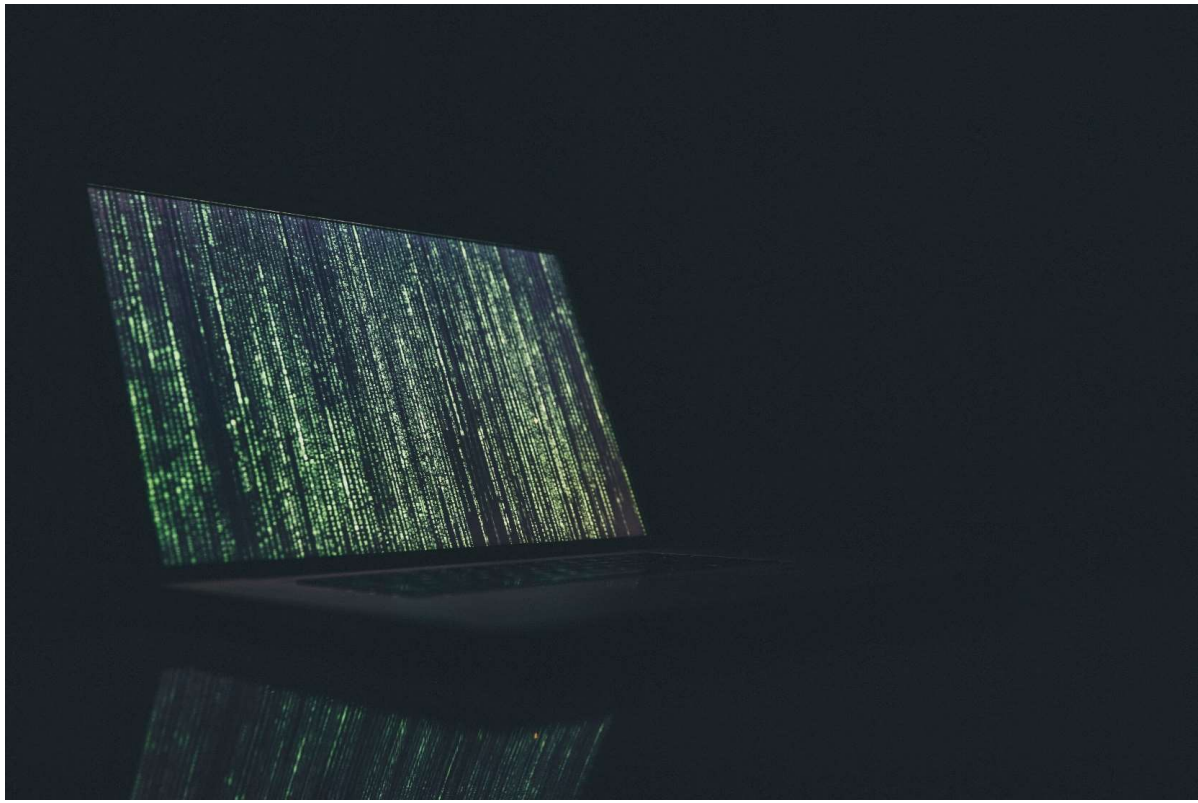
Supply chain and third-party risks

- Cyber risk can come from third parties, suppliers, vendors and customers
  - Misconfigured cloud applications
  - Software vulnerabilities
  - Downstream clients with access to your IT systems
  - Managed Service Providers (MSPs) are oft-targeted victims, see May 11 advisory from US, UK, New Zealand: https://www.cisa.gov/news/2022/05/11/joint-cybersecurity-advisory-protect-msp-providers-and-customers

Supply chain risk management

- Review third party risk management (TPRM) programs
  - TPRM programs often cover financial risk and sanctions but should include cyber
    - NIST SP 800-53: Supply Chain Risk Management (SCRM) Controls
- Consider contract provisions and requirements, as well as oversight
- Planning and preparedness
  - Develop contingency plans if a supplier is impacted (e.g. Kaseya, Wolters Kluwer)
  - Consider physical impacts from third party ransomware events (e.g. Colonial Pipeline)
  - NIST Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (May 2022) https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2022/may/cs2022_0102.pdf

Takeaways and lessons learned



Key lessons

- Regulatory and security risk are increasing for organizations of all sized and types
- Corporate counsel play a vital role as risk managers
- Whatever the level of maturity, organizations can constantly evolve
- Incident preparedness requires a plan and regular practice
- Line up outside counsel, forensic consultant, crisis management firm (establish privilege!)
- It is important to build relationships with peers and government beforehand (e.g., FBI, DHS/CISA)
- Review insurance coverage

Presenters

Lyn Brown
Special Counsel
Wiley
E: jfbrown@wiley.law
T: 202.719.4114

Megan Brown
Partner
Wiley
E: mbrown@wiley.law
T: 202.719.7579

Ted Brown
Partner
Wiley
E: erbrown@wiley.law
T: 202.719.7580

Susanna McDonald
VP and CLO
Association of
Corporate Counsel
E:
T: