KING & SPALDING

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Cybersecurity and the Board

December 9, 2020

Phyllis Sumner
Partner & Chief Privacy Officer
King & Spalding

Mary Chapin
Chief Legal Officer, VP & Corporate Secretary
National Student Clearinghouse

Lisa Shemie
Associate General Counsel, Chief Legal Officer
Cboe FX and Cboe SEF

Jerry Howe
Executive Vice President and General Counsel
Leidos

Agenda

Cybersecurity and Threat Landscape

Board Cybersecurity Oversight

Key Board Considerations

Takeaways and Tips

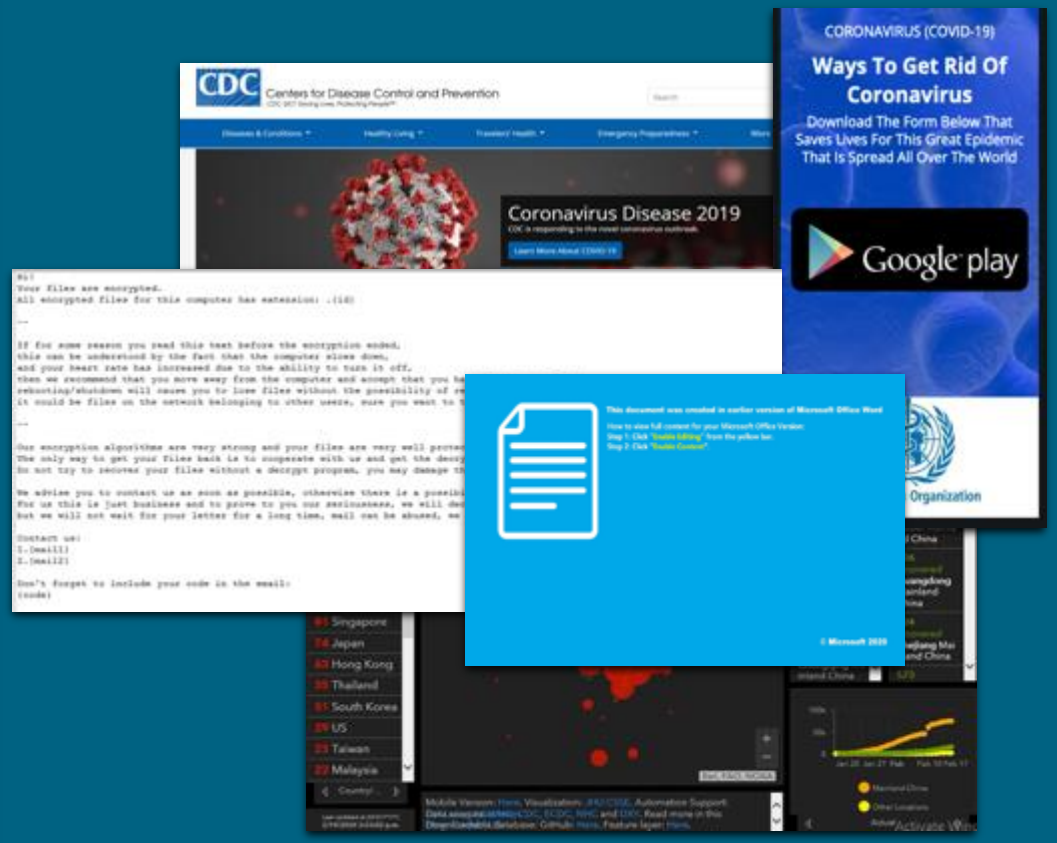
Cybersecurity and Threat Landscape

COVID-19 Cyberthreat Landscape

"Beyond the threat that COVID-19 poses to public health, the pandemic has exposed a massive new risk for global corporations: a debilitating cyberattack."

JANE HOLL LUTE, FORMER DEPUTY SECRETARY OF HOMELAND SECURITY

- Phishing lures
- Malicious apps
- Denial-of-service attacks
- Advanced persistent threats
- Ransomware
- Novel threats



Cybersecurity and Threat Landscape

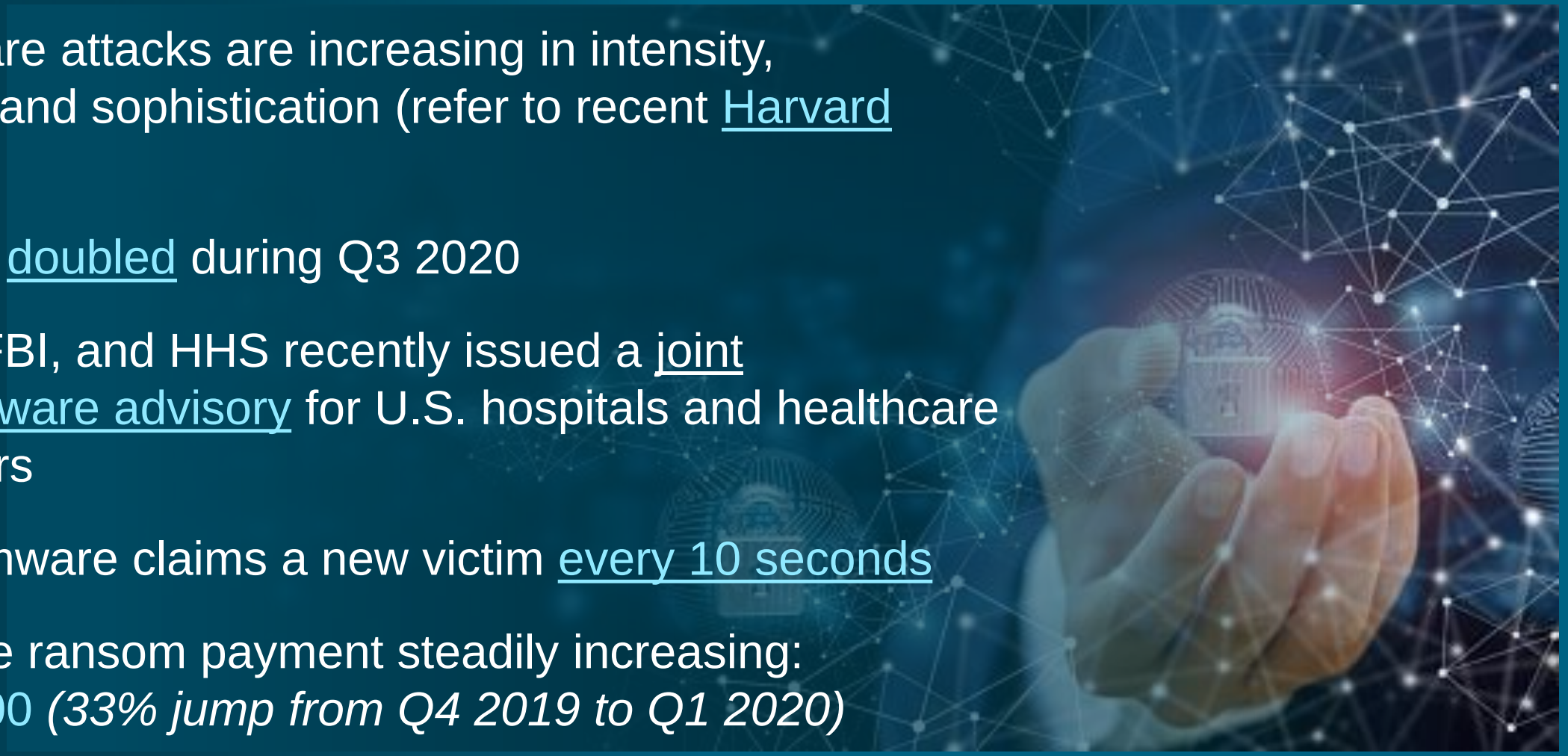
Amplified Attack Vectors

- Fake alerts from the CDC
- Solicitations ostensibly from legitimate charitable organizations
- Flood of “stimulus payment” scam opportunities
- Fake streaming service sites designed to steal payment and PII

Ransomware

Ransomware attacks are increasing in intensity, frequency, and sophistication (refer to recent Harvard article)

- Attacks doubled during Q3 2020
- CISA, FBI, and HHS recently issued a joint ransomware advisory for U.S. hospitals and healthcare providers
- Ransomware claims a new victim every 10 seconds
- Average ransom payment steadily increasing: $112,000 *(33% jump from Q4 2019 to Q1 2020)*



Board Cybersecurity Oversight

Rules and Guidance

SEC – A company should disclose the extent of its board of directors' role in overseeing cybersecurity risk

NYDFS – CISO must submit written risk report to full board at least annually (not audit committee)

FTC – Companies must present their Board with written information security program

Board Oversight

- Oversight and monitoring responsibilities
- Enterprise-wide risk-based approach to cybersecurity
- Internal alignment on expectations
- Access to experience
- Preparedness
- Accountability

Board Cybersecurity Oversight

Pervasive digital transformation means no element of business is unaffected

Heightened privacy requirements increase risks

Pressure from many sources

Changes in vendor management

D&O Litigation

Recent lawsuits involving directors:

- LabCorp (Delaware Chancery 2020)
- Capital One (EDNY 2019)
- FedEx (SDNY 2019)
- Zendesk (NDCA 2019)

Key Board Considerations

Key Board Considerations

Risk Management
is the
Great Equalizer

Risk Management is the Great Equalizer

"Cyber is fundamentally different because it is fundamental. It touches so much — relationships, processes, infrastructure. It permeates in a way that is different from other risks. What you provide to others through your business and your product. It's different than what boards look at with other risks."

— Director

Risk Management Is the Great Equalizer

- Significant changes and forced digital transformations — increase need for risk assessments
- What is the risk appetite?
- Strategic boards will be thinking more holistically (see governance article)

Risk Management Is the Great Equalizer

Strategic boards will be asking management teams about managing the “new future normal”

Grounding discussions in the parlance of risk can bridge the gap of competing interests

Key Board Considerations

We’re All Insiders Now

We’re All Insiders Now

“The mantra: prevent, detect and respond … a conversation you have to keep alive at every point.”

— Director

We’re All Insiders Now

Both the “new normal” and the “new future normal” change the dynamic for protecting assets

Shift from “hacker hunter” to “internal threat” paradigm

Business email compromise, phishing, impersonation, and account-takeover gambits becoming more commonplace

We’re All Insiders Now

Board Guidance

- Ask probing questions about the “new normal” and “new future normal”
- Retain focus on privacy implications of adjustments
- Understand how employee activity is monitored

Key Board Considerations

Incident Response Preparedness

Incident Response Preparedness

"A key part of response isn't just policies and processes, but testing those processes, including engaging the board. In some companies, the CISOs only engage the CEO and direct reports."

— Director

Incident Response Preparedness

- What is the board's role in incident response?
- How to ensure that board and management are aligned on incident reporting and escalation?
- How are Boards involved in costs and resources, including insurance?
- How are Boards balancing risks with protecting the brand?

Incident Response Preparedness

- What are the trends in board-level Incident Response tabletop exercises?
- How are boards assessing management capabilities and talent for cybersecurity?
- How are boards assessing whether IT and Security are overwhelmed?

Key Board Considerations

Regular Reporting and Monitoring

Regular Reporting and Monitoring

"Boards have to be aware of what they're asking for. If you give too much data to the board, it's a problem."

— Director

Regular Reporting and Monitoring

Maintain specific processes and procedures for Committee/Board communication with management

CISO is a critical liaison between the Committee/Board and management

Pervasive digital transformation means that other leaders are critical — e.g. heads of internal audit, supply chain, logistics, etc.

Regular Reporting and Monitoring

Consider level-setting for the board as a whole, including review of fundamentals

Regularly ask about maturity of cybersecurity program, third party risk management and incident response preparedness

Discuss resource allocation

Regular Reporting and Monitoring

- Challenge management to perform tabletop exercises to analyze what works and what doesn’t
- Review ongoing security model and vulnerability report, including high-risk vulnerabilities identified

Key Takeaways and Tips

King & Spalding

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Questions?

Phyllis Sumner
Partner & Chief Privacy Officer
King & Spalding

Mary Chapin
Chief Legal Officer, VP & Corporate Secretary
National Student Clearinghouse

Lisa Shemie
Associate General Counsel, Chief Legal Officer
Cboe FX and Cboe SEF

Jerry Howe
Executive Vice President and General Counsel
Leidos

Appendix: Rules and Guidance

Under Section 500.04(b), can the requirement that the CISO report in writing at least annually "to the Covered Entity's board of directors" (the "board") be met by reporting to an authorized subcommittee of the board?

No. The Department emphasizes that a well-informed board is a crucial part of an effective cybersecurity program and the CISO's reporting to the full board is important to enable the board to assess the Covered Entity's governance, funding, structure and effectiveness as well as compliance with or other applicable laws or regulations.

Via New York Department of Financial Services (NY DFS) FAQs

Appendix: D&O Litigation

“A shareholder filed a lawsuit against LabCorp and 12 of its executives and directors - including the medical testing company's CIO - over two data breaches, including the 2019 breach of one of its vendors, American Medical Collection Agency, which affected millions of patients.” – via Bank Info Security

“As discussed here, on October 2, 2019, a plaintiff shareholder filed a securities class action lawsuit in the Eastern District of New York against Capital One and certain of its directors and officers.” – via The D&O Diary

“As discussed here, the securities class action lawsuit filed in the Northern District of California in October 2019 against Zendesk and certain of its directors and officers combined allegations involving the company’s earnings miss in the prior financial reporting quarter along with allegations relating to a data breach the company had announced.” – via The D&O Diary

“The securities class action lawsuit filed in June 2019 against FedEx (discussed here) involved adverse cybersecurity developments in the company’s European operations.” – via The D&O Diary

Appendix: Cyber Risk and the Corporate Response to COVID-19 *(article)*

Successes and Difficulties in Transition to Remote Work

- Investments in technology infrastructure and people paid off
- Persistent challenges remain and new risks have appeared
    - Intensified cyber attacks
    - Insufficient controls around the digital infrastructure
    - Relaxation of operational controls
    - Weakened social cohesion and potential increased insider risk

Appendix: Cyber Risk and the Corporate Response to COVID-19 *(article)*

Reviewing Risks that Surfaced in the Crisis

- Control of physical and digital assets
- Visibility across endpoints
- Insufficient segmentation
- Monitoring data flows
- Insider threats
- Envisioning a post-pandemic future

Third-Party Risks

- Teams forced to consider the level of third-party risk they are willing to accept

Appendix: Cyber Risk and the Corporate Response to COVID-19 *(article)*

Increased Adoption of Cloud Services

- Cloud services can be a key enabler as companies move beyond the limits of legacy systems, but the security challenges are significant, and many management teams must update their skills.

Balancing Tighter Security Against Collaboration and Innovation

- Is the castle-and-moat model becoming obsolete?
- Should zero trust be the goal in a post-pandemic future?

"We're heading into a scenario where the pandemic has made it more important to do all these things because the risks have gone up. From a corporate perspective, asset inventories, data mapping, access controls—already crucially important before the crisis and always difficult to get an organization's arms around—have become even more important today."

Appendix: Cybersecurity – An Evolving Governance Challenge *(article)*

A New and Different Challenge for Boards

- Cyber risk is tough to characterize and measure
- What makes cyber risk unique?
    - directors' lack of familiarity with the issues; and
    - companies' near-total dependence on the internet.
- Who will manage cyber risk?
    - *"Until recently, many senior executives and outside directors tended to assume that management of cyber risk could be delegated to a firm's information technology (IT) professionals. However, as it has become increasingly clear that attacks present potentially existential risks, these top leaders are trying to engage more deeply in cyber matters."*

Appendix: Cybersecurity – An Evolving Governance Challenge *(article)*

A Wide Variety of Oversight Structures

- Oversight by the audit committee
- Oversight by other existing committees
- Oversight by a cybersecurity committee
- Oversight by the whole board

Complex Interactions Between Directors and Management

- In many risk areas, directors have found practical ways to assure themselves that management is aware of exposures and has put mitigation and recovery mechanisms in place. Building this confidence is never easy in a large global firm, but most directors and committees—risk and audit, for example—know which executives they need to be in dialogue with.