ADVANCED
CYBER
SECURITY
CENTER

Cyber Risk Governance

Briefing Summary

Session 1 of 4: Getting Ahead of the Regulators

March 2023

TRUSTED NETWORKS.
ADVANCING CYBER STRATEGIES.

ADVANCED
CYBER
SECURITY
CENTER

Overview

Regulators are raising the stakes for board cyber governance. Collaboration between CISOs, risk officers and legal counsels is now vital. In this first of our four-part series, members discussed the issues and challenges every organization will face with respect to coming cybersecurity regulations. The day's findings are organized into three thoughtful sections:

- A succinct overview of where Cyber Risk Governance is heading, SEC disclosure requirements, and the governance landscape (courtesy of Foley Hoag)
- Top 3 priorities (and 10 steps) to prepare boards of directors and senior management to respond to emerging cyber regulation
- Top 5 considerations for effectively communicating cyber risk to boards and senior mgmt

Properly preparing for emerging regulatory challenges builds trust with boards and senior management.

1. Where is cyber governance heading?

Where is Cyber Governance heading?

- **Increasing White House Action.**The Biden Administration has issued a number of Executive Orders regarding cybersecurity practices. While these affect federal agencies, they have trickle-down effects on government contractors.
- **Increasing Agency Regulation.** New proposed SEC rules place greater cybersecurity governance requirements on companies. Other agencies are also increasingly involved in governance of cybersecurity (FTC, CFPB).
- **Increasing State Regulation and Oversight.** States are creating new comprehensive privacy laws (CA, CO, CT, VA, UT). Some states are also updating robust cybersecurity regulations (NY).
- **Increasing International Regulation.** EU, UK, India, China, Australia.

SEC Disclosures and the Cyber Governance Landscape

2. What disclosures will the SEC require?

- **Governance and Oversight.** How the Board is informed of cyber risks and incidents. How the Board integrates cyber risk and incident response into its overall risk management framework.
- **Risk Assessment and Management.** How management establishes and implements cybersecurity policies and procedures. Management's role and expertise in uncovering, assessing, and addressing cyber risks. Incident response.

3. What does the cyber governance landscape look like for boards and senior management?

- **SEC Trendsetting.** Although multiple federal and state agencies are involved, the SEC's new rules will have an outsized impact.
- **The Courts.** Expect a Delaware Chancery Court Caremark duty of care standard for boards involving cybersecurity.
- **Global Scope.** Increasing convergence toward some common principles, driven in part by GDPR, but also by global scope of cyber threats.
- **Training and Competency.** Build high level competency for cyber risk governance.
- **Best Practices.** Collaboration of cybersecurity, risk, legal and privacy. Robust data management. Updated policies. Continuous auditing. Building resiliency.

Top 3 priorities (10 steps) to prepare boards and senior management to respond to emerging cyber regulation

1. INTERACTING WITH REGULATORS

- **Multiple regulatory bodies and jurisdictions make it complicated.** Organizations face challenges in navigating and complying with multiple regulatory bodies and jurisdictions, which can complicate decision-making and resource allocation. There needs to be a clear minimum standard of security to create harmony and reciprocity across jurisdictions.

- **What will 'interaction' from regulators look like?** Many auditors and regulators haven't caught up to modern technology. They often are not well-versed in cybersecurity. Where there aren't a lot of rules or interaction from regulators, create your own and expect to be held accountable to them. Regulations are headed towards corporate liability. This could be a sweeping change. Expect to apply the same level of rigor and compliance to a company's cybersecurity program that is required for SOX financial reporting.

2. FRAMING THE ISSUES. PREPARING THE BOARD.

- **'Business risk' is too broad.** Define it at least one level deeper: reputation risk, regulatory/legal risk, and of course, financial risk. Identify impact vs. likelihood.

- **Boards will want to know if the risk identification process is working.** There will always be plenty of evidence of activity – but was the activity successful? How is success measured? Do you know what risk you are accepting? Use backwards planning: We want this outcome and here is how we'll get there. Looking back from an after-action report can reveal lessons learned and the need for new policies. Support this with data and analytics. Show that you are identifying risk at a strategic level, not just at an operational level.

- **Boards cannot usually act in real time.** Set up a process that defines when to engage the board. Is notification by phone call, email, text? Establish a briefing meeting with a clear decision goal. Consider attorney-client privilege, as it is important to keep comms open. Organize comms, internally and externally. Use Sharepoint, Boardvantage, etc. for capture.

- **Boards will need more expertise and systems thinkers capable of governing cyber risk.** Regulators are asking for evidence that boards are challenging management. Boards must ensure alignment and collaboration between different organizational functions for effective cyber risk management. Proposals for Board training: Drive towards a cyber knowledge baseline first. Use 1:1 training and 1:1 debriefs if possible. Recruit an audit committee to help train the full board. Focus on risk/risk reduction and preparation for response. Ensure board members understand the chain of accountability.

3. ORGANIZING FOR GOVERNANCE AND MANAGEMENT

- **Cyber risk management must be viewed as a collective responsibility.** It must involve the entire organization and simply cannot be relegated to, or limited to, the IT department.

- **3rd party risk is real.** Managing third-party risks is essential, and organizations must maintain visibility into their vendors' security postures to ensure end-to-end security.

- **Regulatory compliance and security investment balance is key.** Pursuing harmonization in regulations and investing in security can streamline compliance efforts and improve overall cybersecurity resilience. But it won’t be easy. Regulatory compliance costs are increasing. Regulatory harmonization is likely years out due to independence of regulatory entities like NSPM-33, FEDRAMP, state-level regulatory bodies.

- **Cybersecurity insurance is needed, but also far from mature.** The underwriting process should include CISO, Privacy and legal to properly identify and quantify risk. Policies are likely to require an extension of fiduciary duties, increased cyber competency and understanding of regulations at board level. Consider self-insurance: escrows, reciprocals, and captives.

Top 5 considerations for effectively communicating cyber risk to boards and senior management

- **Make it easy to consume.** Use the same format at each meeting. Dashboard reporting works with business executives. Consistent one-page executive summaries focusing on primary global risks. Reference an established framework, e.g., NIST, with trends over time. Use 3-5 most important measurements, maturity indicators.

- **Less jargon. More business impact clarity.** Translate technical terms/concepts into direct impact financials - a perspective that management and boards understand. Express findings in terms of $, business impact, reduced insurance premiums, etc.

- **Communicate your immediate and multi-year plans.** Don’t sugar coat it, tell them where you have gaps, but don’t make it all doom and gloom either. Give the board assurances, e.g., we meet expectations here and we are short of targets there. Missing resources? Skill sets? CISO/CEO alignment, etc. Provide de-risk options/plans by resource expense and urgent/non-urgent priority.

- **Organize material around clear topics and challenges.** Make it obvious how to perform regulatory and cyber risk oversight. Condense to threat risk - regulatory/non-regulatory, compliance gaps, lines of business maturity, cyber competency, training metrics, etc.

- **Translate threat risk into meaningful dimensions and establish benchmarks.** Scale/scope, nation state vs. private, likelihood, impact, effort/cost/ROI to de-risk. Look at other industries. Reference exemplars, even if unregulated. Boards will always ask “how do we compare?”

Closing Thoughts

The emerging regulatory challenge roundtable presented valuable insights into the direction of Cyber Risk Governance and forthcoming cybersecurity regulations.

Proper preparation for regulatory management builds trust and influences support for resource requests. By taking the necessary steps to prepare for emerging regulations, organizations can avoid undesirable consequences.

More importantly, these measures can help companies improve overall cybersecurity risk management, incident handling and executive stewardship.

Member Participants

- Aptiv
- Commonwealth of Massachusetts
- Commure
- Dell
- Everbridge
- Federal Reserve Bank of Boston
- Foley Hoag
- Harvard University
- The Jackson Laboratory
- John Hancock/Manulife
- MIT Lincoln Laboratory
- Munich Re
- Northeastern University
- Point32Health
- Schneider Electric
- VHB

Research Partners

- Black Kite
- CyberGRX
- CyberSaint
- SimSpace
- Tenable
- Threat Warrior

Special Thanks to Presenters

- Rob Knake, The White House
- Jason Snyder, Commonwealth of MA
- Lavonne Burke, Dell
- Mahi Dontamsetti, State Street
- Pat Ford, Schneider Electric
- Anne Margulies and Chris Perretta - ACSC and corporate board members

Event Sponsor

CyberSaint SECURITY

Event Host

FOLEY HOAG

Contact us ☎ (617) 584-0581 ✉ jdinneen@acscenter.org