CORPORATE BOARDS USA

Boardroom Fundamentals 301
Module 5: Cybersecurity

Prepared by
Linda Iannone

CORPORATE BOARDS **USA**

Cybersecurity

Cybersecurity risk has increasingly become a focus of boardroom oversight responsibility. Because of its complexity and evolving nature, oversight can be challenging. Best practices include the following:

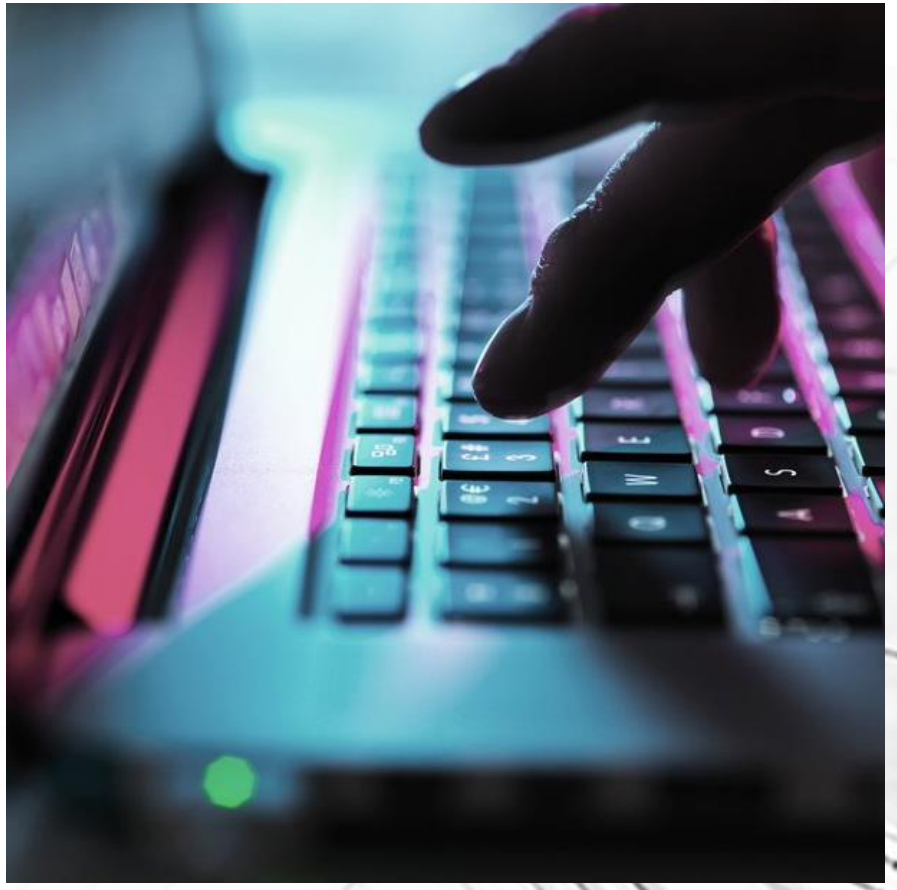
- Set the "tone at the top" to establish an organization-wide expectation that cybersecurity is important and that the board is paying attention
- Ensure that cyber risk is part of the enterprise risk management framework
- Require periodic reporting by the executive charged with implementing cyber controls, such as the Chief Information Security Officer or other IT leader
- Review results of risk assessments, penetration testing, tabletop exercises and internal audits
- Obtain cyber risk insurance and assess its adequacy on a regular basis
- Inquire about the adequacy of resources and budget to safeguard cyber assets
- Understand the company's cybersecurity strategy, priorities and policies
- Ascertain the company's internal process and response plan for reporting cybersecurity and privacy breaches to customers and regulatory authorities
- Consider appointing a technology expert to the board

CORPORATE BOARDS USA

Cybersecurity

Questions Board should ask Management

- What is the organization's cybersecurity framework and strategy?
- Where are the company's most significant vulnerabilities and what controls are in place?
- What training (and how frequently) is given to employees about cyber risks and how to protect against cyber breaches?
- Are the company's key assets protected?
- Does the company have a plan to respond to malicious attacks, including ransomware? If so, how often is it tested?



CORPORATE BOARDS USA

Cybersecurity

Current SEC Guidance on Cybersecurity Disclosure

While no specific SEC regulation requires disclosure of cybersecurity risks, a 2018 Interpretive Release explained how current rules may impact disclosures about cyber risks, governance and incidents including:

- How the board administers its risk oversight function if cybersecurity risk is material to a company's business
- The impact of costs associated with cybersecurity incidents on the company's financial condition
- Material pending legal proceedings relating to cybersecurity issues
- The design of reporting control systems to ensure that the financial impact of cyber incidents is incorporated into the financial statements
- Risk factors specifically relating to cybersecurity

CORPORATE BOARDS **USA**

Cybersecurity

Proposed SEC Regulations

In March 2022, the SEC issued proposed rules that would require expanded disclosure about cybersecurity risk management, strategy and governance, specifically:

- Reporting cybersecurity incidents within four days of determining that the breach was material
  - Information is material if a reasonable shareholder would consider it important in making an investment decision or
  - If it significantly alters the total mix of information made available
- Cybersecurity governance, including policies and procedures and the board's oversight function
- Management expertise in cybersecurity
- Identification of any board member with cybersecurity expertise

CORPORATE BOARDS USA

Questions?

Contact Linda via email → **lindaiannone35@gmail.com**

End of Module 5