BCLP. Client Intelligent

BCLPSecCorpGov

CYBER-READY BOARDS: A GUIDE TO EFFECTIVE CYBERSECURITY BRIEFINGS FOR DIRECTORS

May 01, 2026

Cybersecurity continues to be a significant risk facing public companies, with different threats constantly emerging. A cyber intrusion may, among other things, be disruptive to business or even bring it to a temporary halt, be extremely expensive to remediate, result in litigation and regulatory exposure and attract media attention. For domestic public reporting companies, a material cybersecurity incident also generally requires public disclosure of material aspects of the incident on a Form 8-K within four business days after the event is determined to be material, and may require Form 6-K disclosure for foreign private issuers.

Additionally, annual reports on both Form 10-K and 20-F require a description of board or committee oversight of risks from cybersecurity threats and the process by which such body is informed about the applicable risks. Disclosure of insufficient processes may result in negative attention from the investor community, and may impact a company's ISS QualityScore (ISS indicated that it gathers information for the QualityScore from, among other sources, a company's annual report). ISS disclosed that it considers multiple factors relating to information security in determining its score for a company, including the frequency of board briefings on information security.

Given the stakes involved, it is incumbent on the board to remain aware of the company's cyber risks, infrastructure and overall cyber landscape. This remains true even where the board delegates oversight responsibility to a committee.

This bulletin provides a high-level outline of topics that may be addressed in board cyber briefings (either in a single presentation or as part of periodic board updates). The frequency of board briefings may depend in part upon the company's cyber risk exposure, the requirements of the company's incident response plan and broader reporting policies and procedures of the company. It is likely appropriate for the company's chief information security officer (CISO) to be significantly involved in the presentation, and/or representative(s) of a third-party business that assists the company with its cybersecurity.

Recommended topics for inclusion in the cyber briefing include:

1. Threat Landscape/Risk Profile

- The most significant risks facing the company and its broader industry
- Potential impact of risks on the company's financial results, operations, reputation and regulatory exposure
- Changes in risk profile since the last update

2. Potential Impact of AI

- Potential threats:

i. Risks associated with the disclosure of confidential or sensitive personal information in publicly available large language models

ii. Sophisticated attacks using deep fake or other AI generated threats

- Potential use for risk mitigation for cybersecurity risks through use of AI tools and platforms (or bad actor use for probing vulnerabilities)

3. Overview of legal and regulatory landscape

- Violations of applicable data breach laws and potential regulatory enforcement
- SEC disclosure requirements
- Ongoing class action risk for data breaches

4. Overview of Company Cybersecurity Program

- Governance Structure - Board and committees (oversight responsibility generally and for time sensitive issues)
- Risk management and strategy overview

i. Adequacy of resources (people, budget, expertise)

ii. Role of external providers (e.g., cybersecurity monitoring)

iii. Identification and status of any priority initiatives

iv. Alignment with recognized frameworks (e.g., the NIST Cybersecurity Framework)

v. Amount and coverage of cyber insurance

- Third-party risk evaluation and mitigation

i. Critical vendors and dependencies

ii. Oversight approach for third-parties

iii. Contractual, insurance, or remediation considerations

5. Description of Maintenance/Improvement Activities

- Training

i. Security training/education

ii. Tabletop exercises

iii. Third-party audits

6. Topics for Board Approval - Key decisions, approvals, or oversight actions requested of the board

As part of periodic board briefings, it may be beneficial for the board or committee charged with overseeing cybersecurity to have private sessions with the CISO to discuss topics of material importance away from other management. Interaction between the board and CISO may build trust between the parties, which is critical in the event of a material cyber incident.

In addition to board briefings, a company may also encourage its directors to take continuing education classes on cybersecurity topics, as well as participate in the company's tabletop exercises to get a better understanding of how significant cybersecurity incidents may be addressed.

Regular, well-structured cybersecurity briefings are essential to enabling the board to fulfill its oversight responsibilities and allowing the organization as a whole to respond effectively in the event of a material cyber incident. By maintaining an informed and engaged board, companies can strengthen their overall cybersecurity posture, enhance regulatory compliance and better protect shareholder value.

RELATED CAPABILITIES

- Securities & Corporate Governance
- Data Privacy & Security

MEET THE TEAM

Andrew S. Rodman

Counsel, New York

andrew.rodman@bclplaw.com
+1 212 541 1197

Amy de La Lama

Partner; Chair – Global Data Privacy and Security Practice; and Global Practice Group Leader – Technology, Commercial & Data, Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Robert J. Endicott

Partner and Leader, Securities and Corporate Governance, St. Louis

rob.endicott@bclplaw.com
+1 314 259 2447
