Davis Polk

SEC outlines new cybersecurity disclosure mandates

March 14, 2022 | Client Update | 6-minute read

Proposed rules would require cybersecurity incident and risk management disclosures and may compound compliance costs and enforcement risks.

On March 9, the SEC proposed cybersecurity disclosure mandates for public companies designed to provide "consistent, comparable, and decision-useful" information to investors. The proposal would require disclosures regarding cybersecurity risk management and material cybersecurity incidents in filings on Forms 8-K, 6-K, 10-Q, 10-K and 20-F, and is likely to spur additional compliance costs and enforcement risks as the SEC steps up its policing of public company cybersecurity management and reporting. The proposal is open for public comment through May 9.

- **Broad definition of "cybersecurity incident"**: The proposal defines "cybersecurity incident" as "*an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.*" This broad definition does not focus on the identity of the bad actor (whether internal or external) or the particular tools (whether electronic or otherwise) used by the bad actor to access or compromise a company's information systems.
- **Current reporting**: Since 2011 the SEC has encouraged public companies to file a Form 8-K or 6-K upon the occurrence of a material cybersecurity incident. The proposal would turn the guidance into a mandate for Form 8-K. Form 6-K would be revised to emphasize that material cybersecurity incidents fall within the categories of information disclosable by foreign private issuers when otherwise reported under local law.
  - *Timing*—Form 8-K reporting under new Item 1.05 must happen within four business days after the company determines that it has experienced a material cybersecurity incident. This determination must be made "as soon as reasonably practicable" and disclosure cannot be delayed during the pendency of an investigation, even if delay would otherwise be permissible under laws governing cyber incident reporting. (In a bit of good news, the failure to make a Form 8-K disclosure on time would not cost Form S-3 eligibility.)
  - *Substance*—Form 8-K disclosure must include when the incident occurred, its impact and the state of remediation.
  - *Updates*—disclosure must be updated in subsequent Forms 10-Q, 10-K and 20-F. The proposal provides broad, non-exhaustive examples of required updates, including "any changes in the registrant's policies and procedures" as a result of the incident. The proposal does not specify an end date for updates.
- **Annual reporting**: The proposal would require additional cybersecurity risk management disclosures in Forms 10-K and 20-F, including:
  - *Policies and procedures*—whether the company has policies and procedures for cybersecurity risk assessment, third-party service provider risk management, incident response, disaster recovery, and programmatic improvements in response to incidents.
  - *Role of management*—management's cybersecurity expertise and its role in assessing and managing cybersecurity risk and implementing policies and procedures, including details on the company's chief information security officer such as internal reporting lines.

- *Governance*—whether, how and how frequently the board is informed of and considers cybersecurity risk, and whether and how the board considers cybersecurity risks as part of its business strategy, risk management and financial oversight.
- *Identification of board cybersecurity experts*—perhaps most problematically, similar to requirements to name board members with financial expertise, the proposal would require companies to identify any board member with expertise in cybersecurity along with "such detail as necessary to fully describe the nature of the expertise." (This disclosure would be a new Form 10-K or 20-F requirement, although a 10-K filer would be able to present this information in the proxy statement.)

The considerations for whether a board member has cybersecurity expertise include:

– whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner;

– whether the director has obtained a certification or degree in cybersecurity; and

– whether the director has knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.

Although many companies have directors who are qualified to assess cybersecurity oversight, in our experience directors usually do not have the specific technical background that the proposal seems to envision, like prior experience as an incident response manager. Because many companies today may not have a director who would meet the SEC's stated expertise criteria (or who would be comfortable being so named), this novel disclosure requirement may impact boards' thinking on composition and refreshment issues at a time when multiple competing priorities are also at play.

The SEC does not have general authority to regulate corporate governance, which is a matter of state law. Therefore, this is a disclosure requirement only, and not a mandate that companies have a director with the specified cybersecurity expertise. But the proposal is consistent with other ways the SEC effectively seeks to mandate governance through disclosure on the assumption that, for example, no company would want to disclose that it does not have a code of ethics or a financial expert on its audit committee. Presumably, the SEC is expecting that most companies will similarly not want to disclose that they do not have a board cybersecurity expert.

However, we view the topic of cybersecurity quite differently—it is clear to investors why a company should have a financial expert on its audit committee and a code of ethics that binds its officers, but it is much less clear that a company with a qualified CISO and robust IT infrastructure must also have an IT expert on its board with the specific technical background that the proposal contemplates. For this reason, and given the narrow definition that the SEC has proposed for board-level cybersecurity expertise, we think many companies will conclude, depending on the particular company's business and the adequacy of its cybersecurity capability at the management level, that it is not imperative to have a board member who is able satisfy the SEC's particular definition of cybersecurity expertise.

Potential compliance implications

– **Incident response may be more costly and complicated**
  - Companies will need to quickly determine cybersecurity incident materiality and make disclosures within four business days of the determination—an aggressive timeline, as compared to most other federal and state breach notification laws. The SEC also rejects delayed notification while investigating an incident, as permitted in most breach notification laws.
  - The proposal acknowledges the complexity of materiality determinations, and provides examples of potentially material incidents including data exfiltration, ransomware, and system outages. But the breadth of these examples illustrates the potential complexity of timely materiality decisions.
  - Companies will need to track incident response and remediation to make required updates in subsequent Form 10-Q, 10-K and 20-F filings.

– **De facto minimum standards for cybersecurity policies and procedures**
  - In requiring a discussion of specific cybersecurity policies and procedures in Forms 10-K and 20-F, the SEC is effectively signaling minimum standards for what these policies and procedures should cover.

- In her dissent from the proposal, Commissioner Peirce characterized the SEC as moving towards more direct regulation of public companies, “cloaked as a disclosure requirement.” To her point, and in addition to our observations above about board composition, the proposal would require companies to disclose practices akin to those the SEC directly requires of registered investment advisers and investment companies, including in proposed rules announced last month.

Increased enforcement risk

The proposed disclosure requirements come at the same time the SEC has stepped up cybersecurity disclosure enforcement, including recent actions involving the disclosure of hypothetical cybersecurity risks when actual events had occurred, and disclosure controls and procedures around cybersecurity event reporting. The proposal would heighten enforcement risk, including:

- for failure to provide timely or adequate notice of a material cybersecurity incident in Form 8-K or in subsequent filings,
- for failure to adequately disclose, or for overstating, the nature of the company’s policies and procedures, management and governance of cybersecurity risks, and
- increasing the likelihood of an SEC finding that the company lacks adequate cybersecurity controls because it does not maintain some of the policies and procedures described in the proposal.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Micah G. Block
+1 650 752 2023
micah.block@davispolk.com

Ning Chiu
+1 212 450 4908
ning.chiu@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

Joseph A. Hall
+1 212 450 4565
joseph.hall@davispolk.com

Michael Kaplan
+1 212 450 4111
michael.kaplan@davispolk.com

Emily Roberts
+1 650 752 2085
emily.roberts@davispolk.com