Freshfields Bruckhaus Deringer

SEC Proposes Cybersecurity Disclosure Rules

Authored by: Brock Dahl, Kimberly Zelnick, Nicholas Caselli
March 12, 2022

On March 9, the Securities and Exchange Commission proposed rules and amendments aimed at enhancing and standardizing disclosures about cybersecurity risk management, strategy, governance, and incident reporting by public companies. The proposal, which follows prior guidance on cybersecurity risks and incidents by the Division of Corporate Finance in 2011 and the Commission in 2018, would broaden the cybersecurity disclosure landscape in two major ways: first, by requiring disclosure of material cybersecurity incidents within four business days of a company determining that it has experienced such an incident, and second, by requiring ongoing disclosures about a company's cybersecurity governance, risk management, and strategy.

Incident Reporting. The Commission first proposes to amend Form 8-K to require all U.S. domestic reporting companies to disclose material cybersecurity incidents within four business days after determining that they have experienced such an incident. Specifically, the Commission would add new Item 1.05 to Form 8-K, which would require disclosure of the following information about material cybersecurity incidents, to the extent that such information is known at the time of the Form 8-K filing:

- When the incident was discovered and whether it is ongoing;
- A brief description of the nature and scope of the incident;
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
- The effect of the incident on the company's operations; and
- Whether the company has remediated or is currently remediating the incident.

New Item 1.05 would be "triggered" on the date on which a company determines that a cybersecurity incident is material, rather than the date of discovery of the incident. Yet, to address any concern that some companies might delay making a materiality determination to avoid the disclosure obligation, the proposed amendment also requires that such a determination be made "as soon as reasonably practicable after discovery of the incident."

The Commission's proposal explains that what constitutes a "material" cybersecurity incident for the purpose of these amendments is consistent with that term's general usage in the federal securities laws—in other words, an incident is material if "there is a substantial likelihood that a reasonable shareholder would consider it important." The Commission advised that companies should "thoroughly and objectively evaluate the total mix of information" and consider "all relevant

facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors," when gauging materiality. For example, even if the probability of an adverse consequence is low, if the magnitude of the loss or liability is high, the incident may be material.

The proposal enumerates a non-exclusive list of examples of cybersecurity incidents, including unauthorized systems access or ransomware attacks, which "may, if determined by the registrant to be material, trigger the proposed Item 1.05 disclosure requirement." Separate from the proposals, but in consideration of their import, companies may wish to begin working now to establish materiality protocols so that they are able to demonstrate the existence of, and their commitment to, a rigorous and serious process for evaluating potential events. Such considerations could include:

- Duration of the incident (and whether the length implies deficient monitoring or large-scale failures);
- Number and nature of the affected users;
- Nature and origin of the incident (in particular, whether there is any implication of broader systemic issues for the company);
- Nature and sensitivity of the affected data;
- Potential regulatory implications and associated legal obligations or triggers;
- Potential business impacts (operational disruptions and revenue impediments); and
- Potential financial impact.

In addition, the Commission proposes that companies be required to periodically update incident information for "material changes, additions, or updates" in quarterly and annual reporting, as necessary. The Commission suggests this as a supplementary measure, recognizing that a company may still have incomplete information within the four-day window for reporting material incidents.

Finally, the Commission also suggests that a series of individually immaterial events could become material in the aggregate. The Commission lays out a list of disclosure requirements in the event such aggregate materiality is determined to exist.

Foreign private issuers are not required to file current reports on Form 8-K and therefore the new 8-K disclosure regarding cybersecurity would not apply to foreign private issuers. Instead, foreign private issuers are required to file on Form 6-K information that the foreign private issuer (i) makes or is required to make public under the laws of its jurisdiction of incorporation, (ii) files, or is required to file under the rules of any stock exchange, or (iii) otherwise distributes to its security holders. Form 6-K includes a list of items which may trigger 6-K disclosure if material, and the SEC is proposing to add a reference to "cybersecurity incidents" among the items that may trigger a current report on Form 6-K. If a foreign private issuer has previously provided disclosure regarding one or more cybersecurity incidents pursuant to Form 6-K, the company would also be required to

disclose in its annual report on Form 20-F any material changes, additions, or updates regarding such incident that occurred during the prior year period.

Governance, Strategy and Risk Management Disclosures. As a second key theme, the proposal would require public companies (both U.S. domestic reporting companies as well as foreign private issuers) to periodically issue disclosures describing their policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the company considers cybersecurity as part of its business strategy, financial planning, and capital allocation. Public companies would also be required to disclose information about their boards' expertise in cybersecurity and oversight of cybersecurity risk, as well as managements' expertise and role in assessing and managing that risk and implementing cybersecurity policies, procedures, and strategies.

This aspect of the proposal reflects pressure from Capitol Hill to require disclosures about cybersecurity expertise on a company's board and among its management, a mandate that is likely to hasten the search for such expertise in boardrooms and executive suites across corporate America. In addition, although relevant to companies across the country, the requirement that companies disclose board and management cybersecurity oversight and expertise may be of special interest to any Delaware corporation with cybersecurity risks who might wish to take prophylactic steps now should it one day face breach of fiduciary duty or lack of oversight claims related to cybersecurity incidents under the state's evolving *Caremark* claim jurisprudence.

This may be an opportune time for public companies to consider their risk management practices, focusing on certain key priorities, such as:

- Reviewing disclosure control procedures for identifying and escalating incidents;
- Conducting periodic reviews of the corporate cyber posture and resourcing;
- Enhancing governance and oversight of mission-critical cybersecurity risks;
- Auditing policy framework and implementation practices; and
- Seeking vulnerability assessment and penetration testing to enable necessary remedial efforts.

Public comment will remain open until the later of May 9, 2022 and 30 days following publication of the release in the Federal Register.