Articles + Publications | March 10, 2022

SEC Proposes New Rules to Enhance Cybersecurity Disclosures and Incident Reporting

WRITTEN BY

David I. Meyers | Betty Linkenauger Segaar | Adrianna C. ScheerCook | Joseph A. Goldman

On February 9, the Securities and Exchange Commission (SEC) proposed new rules to enhance and standardize registrants' disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting. While existing SEC disclosure requirements do not explicitly reference cybersecurity risks or incidents, the SEC has twice issued interpretative guidance (in 2011 and 2018), urging companies to consider the materiality of cybersecurity risks and incidents when preparing required disclosures under existing SEC rules. While the SEC's prior guidance identified existing Regulations S-K and S-X as provisions that may require disclosure about cybersecurity risks, governance, and incidents, the proposed rules would put in place a suite of requirements that are cybersecurity-specific.

In its proposal, the SEC noted that the majority of registrants reporting material cybersecurity incidents do so via a press release, Form 8-K or other periodic report, but that the nature of cybersecurity incident disclosures varies widely. Furthermore, the SEC observed that companies often blend cybersecurity disclosures with other unrelated disclosures, making it more difficult for investors to analyze the information provided. The SEC's proposed rules are intended to remedy registrants' disclosures of both material cybersecurity incidents and cybersecurity risk management and governance, which it views as inconsistent, untimely and difficult to locate.

The public comment period for the proposing release will remain open for 60 days following its publication on the SEC's website, or for 30 days following its publication in the Federal Register, whichever period is longer.

If approved as proposed, the new rules would effect significant changes, including:

Reporting of Cybersecurity Incidents on Form 8-K

The proposal would require registrants to disclose material cybersecurity incidents in a current report on Form 8-K within four business days after the registrant determines that it has experienced a material cybersecurity incident. Notably, the trigger date for such disclosure would be the date on which a registrant determines that a cybersecurity incident it has experienced is *material* (applying traditional materiality standards) — not the date the incident was discovered.

If adopted as proposed, Form 8-K would be amended to add a new Item 1.05 that would require a registrant to disclose the following information about a material cybersecurity incident:

- 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 registrant's operations; and
- Whether the registrant has remediated or is currently remediating the incident.

Like other Form 8-K items that require materiality determinations, the proposal provides that an untimely filing under proposed new Item 1.05 would not result in a loss of Form S-3 eligibility. In any case, registrants should review and update their disclosure controls and procedures to ensure that they are able to timely comply with the new Form 8-K trigger, if adopted, and make the required materiality determination. This may prove to be challenging in cases where the extent of a cybersecurity breach is difficult to assess from the outset and requires some time to determine whether or not it is material. Additionally, registrants will need to weigh the desire to get the information about a material breach into the public sphere as soon as possible to prevent potential litigation against the desire to not disclose a breach that ends up not being material prematurely.

For registrants that are banking organizations, including U.S. bank holding companies, insured state nonmember banks, and national banks, these rules would apply in addition to those approved in November 2021 by the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, which go into effect May 1, 2022. These rules require a banking organization to notify its primary federal regulator of a cyber incident no later than 36 hours after determining that such an incident has occurred, which could materially disrupt, degrade, or impair the viability of the banking organization's operations, its ability to deliver banking products and services to its customers, or the stability of the financial sector. Banking organization registrants will need to ensure that their disclosure controls and procedures facilitate compliance with both sets of rules if the SEC's rules are adopted as proposed.

Disclosure About Cybersecurity Incidents in Periodic Reports

Proposed Item 106(d)(1) of Regulation S-K would require registrants to disclose any material changes, additions, or updates to information, which must be disclosed pursuant to new Item 1.05 in the registrant's Form 10-Q or Form 10-K, as applicable. The following are examples of the types of disclosure that should be provided, if applicable, pursuant to proposed Item 106(d)(1):

- Any material impact, or any potential material future impacts, of the incident on the registrant's operations and financial condition;
- Whether the registrant has remediated or is currently remediating the incident; and
- Any changes in the registrant's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes.

In addition to serving as a supplementary disclosure to an initial Form 8-K filing, proposed Item 106(d)(1) would also require disclosure when a series of previously immaterial cybersecurity incidents becomes material in the aggregate (*e.g.,* a malicious actor engages in a number of smaller but continuous cyber-attacks against the registrant that collectively are either quantitatively or qualitatively material).

Disclosure of Risk Management, Strategy, and Governance Regarding Cybersecurity Risks

Proposed Item 106(b) of Regulation S-K would require a registrant to disclose its policies and procedures, to the extent it has any, to identify and manage cybersecurity risks and threats, including: operational risk; intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk. Proposed Item 106(b) would require disclosure of several items that the SEC believes benefit investors by providing greater transparency as to a registrant's policies to manage cybersecurity risks.

Proposed Item 106(c) of Regulation S-K would require disclosure of a registrant's cybersecurity governance, including the board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks; the relevant expertise of such management; and its role in implementing the registrant's cybersecurity policies, procedures, and strategies. A registrant would be required to include a discussion of the following in connection with the board's oversight of cybersecurity risk:

- Whether the entire board, specific board members, or a board committee, is responsible for the oversight of cybersecurity risks;
- The processes by which the board is informed about cybersecurity risks, and the frequency of the board's discussion on cybersecurity risks; and
- Whether, and how, the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

Disclosure Regarding the Board of Directors' Cybersecurity Expertise

The SEC proposes to amend Item 407 of Regulation S-K by adding paragraph (j) to require disclosure about the cybersecurity expertise of members of the board, if any. If any member of the board has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s) and fully describe the expertise of the director(s). Notably, proposed amended Item 407 does not require a registrant to disclose why it does not have a board member with cybersecurity expertise like existing Item 407(d)(5) does with respect to an "audit committee financial expert." In addition, unlike the required "audit committee financial expert" disclosure, the proposal would require disclosure of any details necessary to describe the nature of the cybersecurity expertise. The proposed new Item 407(j) disclosure would be included in Part III of Form 10-K, meaning it would typically be disclosed in a registrant's proxy statement.

Given the prominence of cybersecurity risks facing public companies today, many companies have already

prioritized strengthening board cybersecurity expertise in connection with their board refreshment efforts. However, for companies that have not, the proposed rules may serve as motivation to begin doing so.

Inline XBRL Tagging Requirement

The proposed rules would also require registrants to tag the information specified by new Item 1.05 of Form 8-K and new Items 106 and 407(j) of Regulation S-K in Inline XBRL in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual. The proposed structured data requirement is consistent with the SEC's recent adoptions regarding Inline XBRL requirements to improve the quality and usability of data for investors.

Currently, the proposed rule has the support to pass on a 3-1 vote. The dissenting Commissioner characterized the proposed disclosure requirements as "an unprecedented micromanagement by the [SEC] of the composition and functioning of both the boards of directors and management of public companies." The Commissioner also criticized the SEC for overstepping its authority, stating that the proposal "flirts with casting [the SEC] as the nation's cybersecurity command center, a role Congress did not give [the SEC]." However, the Commissioner stated that a "bright spot" of the rule is its "sensible guideposts for companies to follow in reporting material cybersecurity incidents," which are "[p]roperly rooted in materiality…."

In his accompanying statement, SEC Chair Gary Gensler noted that this is the third rulemaking proposal that implicates cybersecurity — the two prior proposals addressed government securities trading platforms and registered investment advisers and funds. Chair Gensler also flagged the prospect of future cybersecurity regulation proposals regarding broker-dealers.

RELATED INDUSTRIES + PRACTICES

- Corporate