Data Privacy and Cybersecurity

SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

By: Charles D. Riely, Shoba Pillay, Alexander J. May, and Hannah E. Schwab

Last week, the SEC proposed rule amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.[1] The proposed rules include an amendment to Form 8-K that would require public companies to disclose a cybersecurity incident within **four business days** following the company's determination that the incident is material to the company. The proposed rules also include a series of new disclosure obligations regarding risk management and governance that appear designed to encourage improvements in what companies are actually doing to address these risks. This alert summarizes the key takeaways from the proposed amendments.

For additional details regarding the proposed amendments, the press release summarizing the proposal and public comment period can be found here and the text of the proposed amendments can be found here.

Background and Obligations Under Current Law

While Regulation S-K and SEC forms such as Forms 10-K and 10-Q mandate a number of specific line item disclosure requirements, the SEC has previously noted that cybersecurity issues are often too fact-dependent to prescribe specific disclosure obligations.[2] The SEC previously issued guidance instructing companies that material cybersecurity incidents should be disclosed and further instructed public companies on the timing of disclosures following a material cybersecurity incident.[3] This guidance provided companies with discretion, within reason, to ascertain the relevant facts to be disclosed, acknowledging that "some material facts may not be available at the time of the initial disclosure," that a company "may require time to discern the implications of a cybersecurity incident," and that "ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident."[4] Ultimately, as the number of incidents increased and the importance of cybersecurity to the typical company's business strategies increased, the SEC elected to propose rules that would provide investors with more timely and standardized information regarding cybersecurity matters.

Summary of the Proposed Disclosure Obligations

The SEC is proposing the following with respect to a public company's cybersecurity disclosures:

- **Material Cyber Incidents Require a Form 8-K Filing:** Item 1.05 of Form 8-K would require companies to disclose information about a cybersecurity incident within **four business days** after the company determines that it has experienced a material cybersecurity incident.[5] The proposed rule also specified that companies would have to provide a number of details in this initial disclosure including when the incident occurred, whether it is ongoing, "[w]hether 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 the incident."[6]
- **Companies Must Update Investors on Material Cyber Incidents:** Proposed Item 106(d) of Regulation S-K would amend Forms 10-Q and 10-K to require companies to provide updated disclosure relating to previously disclosed cybersecurity incidents, and, to the extent known to

management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate.[7]

- **Companies Must Describe Cybersecurity Governance Matters in Additional Detail:** Proposed Item 106 would require a company to disclose the following in their Form 10-K:
  - A company's policies and procedures, if any, for identifying and managing cybersecurity risks, including, but not limited to whether it has a cybersecurity risk assessment program, whether it engages third parties in connection with the program and whether it has a business continuity, contingency, and recovery plan for cybersecurity incidents;[8]
  - A company's cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risks;[9] and
  - Management's role, and relevant expertise, in assessing and managing cybersecurity related risks and implementing related policies, procedures, and strategies.[10]
- **Companies Must Describe Directors' Cybersecurity Experience:** Amended Item 407 of Regulation S-K would require disclosure about whether any member of the company's board of directors has cybersecurity expertise, and if so, the nature of such expertise.[11]
- **XBRL Requirements:** Require that the proposed disclosures be provided in Inline XBRL (eXtensible Business Reporting Language).[12]

Importantly, the SEC is also proposing to add Item 1.05 to the list of Form 8-K items that does not trigger the loss of Form S-3 eligibility, so long as Form 8-K reporting is current at the time the Form S-3. Further, the SEC has also proposed amendments to Exchange Act Rules 13a-11(c) and 15d-11(c) to include Item 1.05 in the list of Form 8-K items eligible for a limited safe harbor from liability under Exchange Act Section 10(b) and Exchange Act Rule 10b5-1.

Impact and Considerations

The proposed amendments represent an important change to existing law and have the potential to change what companies do after a cybersecurity incident or breach and may also impact how companies are managing cybersecurity risks generally.

First, the SEC's proposed requirement that companies disclose a material cybersecurity incident within four days after determining it has experienced a material incident appears designed to help standardize the content and timing of cybersecurity disclosures across companies and industries. As the SEC highlighted in the Proposal Release, companies took a variety of approaches under current law.[13] Some companies filed a Form 8-K, and some described the incident in their next periodic filing. The SEC also observed that it has seen media reports of breaches impacting a company and no corresponding disclosure.[14] Although it is possible that these different approaches were the result of differences in the magnitude of events, the SEC seems to be trying to create a more unified approach and appears to be encouraging earlier and/or specific disclosures.

The SEC's Proposal Release does not provide much guidance on when disclosure would be triggered, other than to require disclosure upon determining that the cybersecurity incident was material. The SEC noted that it could come as early as the date of discovery of the incident, and emphasized that if the proposed rule were passed, "we expect registrants to be diligent in making a materiality determination in as prompt a manner as feasible."[15]

The proposed Item 1.05 of Form 8-K would not provide discretion to delay reporting while an internal or external investigation is ongoing. Citing to the 2018 Interpretative Release, the SEC reasoned that while an ongoing investigation might affect the specifics in the company's disclosure, "an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident,"[16] and that any such delay provision could undermine the purpose of proposed Item 1.05. While recognizing that reporting obligations may differ from other state or federal agencies, the SEC noted that "[i]t is critical to investor protection and well-functioning, orderly, and efficient markets that investors promptly receive information regarding material cybersecurity incidents."[17]

Second, the proposed amendments would impose significantly more disclosure obligations on companies. These obligations include disclosures of its cybersecurity policies and procedures and a requirement 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. The rules also require disclosure regarding whether the company has a "cybersecurity risk assessment program" and require parties to describe the program and whether it engages a third party in connection with that program. It also requires disclosure of whether the company has policies and procedures relating to use of third-party service providers. As proposed, the SEC has not provided exemptions for smaller reporting companies, reasoning that smaller companies may have an equal or greater risk than large companies of being attacked.[18]

Third, if the rules are adopted as proposed, companies will need to review and potentially alter their current information governance standards and procedures. The proposed rules would require companies to disclose detailed information about its board members and management team's expertise in cybersecurity and a description of the board's oversight on cybersecurity. This includes:

- Whether members of the board or management have expertise in cybersecurity, including by the member's name and as much detail as necessary to fully describe the nature of the expertise;
- Whether a company has a chief information security officer, their relevant expertise, and where they fit in the organizational chart; and
- A description of the interactions of management and the board of directors on cybersecurity, including the frequency with which the board considers the topic and the frequency with which the relevant experts from the board and management discuss the topic.

Taken together, these new disclosure requirements are likely to lead to additional focus from companies on their cybersecurity practices and governance. While a number of companies provide all or part of this information in their periodic reports and proxy statements, many companies will have to consider these items for the first time should the rules be adopted.

This aspect of the SEC's rules was criticized by Commissioner Hester Pierce, who filed a dissent. She commented that the proposal, although couched in standard disclosure language, guides companies in substantive, if somewhat subtle, ways."[19] She noted, "[s]uch precise disclosure requirements look more like a list of expectations about what issuers' cybersecurity programs should look like and how they should operate."[20]

Finally, the proposed amendments highlight the importance of companies ensuring close coordination and communication between their cybersecurity and information security functions with their disclosure teams. Companies can better defend their approach to cybersecurity disclosures when they are able to show the officers responsible for disclosure and the disclosure committee had all relevant facts.

***

Jenner & Block will continue to monitor the regulatory landscape surrounding the SEC and cybersecurity.

Charles D. Riely, Shoba Pillay, and Alexander J. May are partners, and Hannah E. Schwab is an associate with Jenner & Block LLP.

Contact Us

Charles D. Riely
criely@jenner.com | Download V-Card

Shoba Pillay
spillay@jenner.com | Download V-Card

Alexander J. May
amay@jenner.com | Download V-Card

Hannah E. Schwab
hschwab@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower
Co-Chair
dbitkower@jenner.com
Download V-Card

Madeleine V. Findley
Co-Chair
mfindley@jenner.com
Download V-Card

Kelly Hagedorn
Co-Chair
khagedorn@jenner.com
Download V-Card

Shoba Pillay
Co-Chair
spillay@jenner.com
Download V-Card

[1] Release No. 33-11038, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (Mar. 9, 2022), available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf [hereinafter *Proposal Release*].
[2] *Modernization of Regulation S-K Items 101, 103, and 105*, Release Nos. 33–10825; 34–89670 at 63744 (Oct. 8, 2020), https://bit.ly/3FBJfEd (declining to add a cybersecurity-specific risk factor disclosure).
[3] *CF Disclosure Guidance: Topic No. 2 – Cybersecurity* (Oct. 13, 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [hereinafter *CF Disclosure Guidance*]; *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release No. 33-10459 (Feb. 26, 2018), available at https://www.sec.gov/rules/interp/2018/33-10459.pdf [hereinafter *2018 Interpretative Release*].
[4] *See CF Disclosure Guidance; 2018 Interpretative Release*.
[5] Note that the SEC proposed to add Instruction 1 to proposed Item 1.05 providing that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."
[6] Proposed Item 1.05 to Form 8-K.
[7] Proposed Item 106(d) of Regulation S-K.
[8] Proposed Item 106(b) of Regulation S-K.
[9] Proposed Item 106(c)(1) of Regulation S-K.
[10] Proposed Item 106(c)(2) of Regulation S-K.
[11] Proposed Item 407(j) of Regulation S-K.
[12] Proposed Rule 405 of Regulation S-T.
[13] *See* Proposal Release, at 16.
[14] *Id*.
[15] *Id.* at 22.
[16] *See* 2018 Interpretative Release.
[17] *See* Proposal Release, at 26.
[18] *Id*. at 85.
[19] *See* Dissenting Statement on Cybersecurity Risk Management Strategy, Governance, and Incident Disclosure Proposal of Commissioner Hester M. Pierce (Mar. 9, 2022), available at https://www.sec.gov/news/statement/peirce-statement-cybersecurity-030922.
[20] *Id*.