GIBSON DUNN

SEC Proposes Rules on Cybersecurity Disclosure

Client Alert | March 11, 2022

Click for PDF

On March 9, 2022, the Securities and Exchange Commission ("SEC" or "Commission") held a virtual open meeting where it considered a rule proposal for new cybersecurity disclosure requirements for public companies, primarily consisting of: (i) current reporting of material cybersecurity incidents and (ii) periodic reporting of material updates to cybersecurity incidents, the company's cybersecurity risk management, strategy, and governance practices, and the board of directors' cybersecurity expertise, if any. The proposal passed on party lines and the comment period ends on the later of 30 days after publication in the Federal Register or May 9, 2022 (which is 60 days from the date that the rules were proposed). Below please find a summary description of the rule proposal, as well as certain Commissioner's concerns related to the proposal. **Summary of Proposed Amendments** New Current Reporting Requirements The proposed amendments would require current reporting of material cybersecurity incidents by adding new Item 1.05 to Form 8-K. As is the case with almost all other Form 8-K items, Item 1.05 would require companies to disclose material cybersecurity incidents[1] within four business days. The trigger date for the disclosure is the date of the materiality determination, rather than the date of discovery of the incident, although companies are required to make a materiality determination as soon as reasonably practicable after discovery. Required disclosure would include:

- 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.

According to the release, "[w]hat constitutes "materiality" for purposes of the proposed cybersecurity incidents disclosure would be consistent with that set out in the numerous cases addressing materiality in the securities laws, including: *TSC Industries, Inc. v. Northway, Inc.*,[2] *Basic, Inc. v. Levinson*,[3] *and Matrixx Initiatives, Inc. v. Siracusano*[4]."[5] The SEC noted in the proposed rule that it would not expect companies to disclose technical information about its planned response, cybersecurity systems, related networks and devices, or vulnerabilities "in such detail as would impede the company's response or remediation of the incident."[6] However, Item 1.05 would not allow for a reporting delay when there is an ongoing internal or external investigation related to the cybersecurity incident. Notably, however, an untimely filing of Item 1.05 disclosure on Form 8-K would not result in a loss of Form S-3 and Form SF-3 eligibility and would be covered by the safe harbor for Section 10(b) and Rule 10b-5 liability. With respect to foreign private issuers, the amendments would similarly create a disclosure trigger for cybersecurity incidents on Form 6-K. New Periodic Reporting Requirements *Material Updates to Cybersecurity Incidents.* The proposed amendments would add additional

Related People

Ashlie Beringer

Lori Zyskowski

Thomas J. Kim

Julia Lapitskaya

Matthew L. Dolloff

disclosure requirements to public companies' quarterly and annual reports by introducing new Item 106(d) of Regulation S-K, which would require companies to disclose any material changes, additions, or updates to information required to be disclosed pursuant to proposed Item 1.05 of Form 8-K in the company's Form 10-Q or Form 10-K for the covered period (the company's fourth fiscal quarter in the case of a Form 10-K) in which the material change, addition, or update occurred. Item 106(d) would also require companies to disclose when a series of previously undisclosed individually immaterial cybersecurity incidents becomes material in the aggregate. *Risk Management and Strategy.* In addition, public companies would be required to disclose their policies and procedures, if any, to identify and manage cybersecurity risks and threats. The company would also be required to describe whether it engages assessors or other third parties in connection with its risk assessment and any policies or procedures for risks in connection with the use of third party service providers. The other topics included in proposed Item 106(b) would require disclosure regarding whether the company undertakes to prevent, detect and minimize the threat of cybersecurity incidents; whether the company has business continuity, contingency or recovery plans in the event of cybersecurity incident; whether previous cybersecurity incidents have informed changes in the company's governance, policies and procedures, or technologies; whether and how cybersecurity-related risk and incidents have affected or are reasonably likely to affect the company's results of operations or financial condition; and whether and how cybersecurity risks are considered as part of the company's business strategy, financial planning, and capital allocation. *Governance.* Proposed Item 106(c) of Regulation S-K would require disclosure regarding the role of the board of directors and management in cybersecurity governance. With respect to the board of directors, companies would need to disclose whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks. Disclosure would also need to include a discussion of the processes by which the board is informed about cybersecurity risks, the frequency of discussions on cybersecurity, and whether and how the board or responsible board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight. With respect to management, companies would need to disclose whether certain management positions or committees are responsible for measuring and managing cybersecurity risk and the relevant expertise of such persons. The company would also need to disclose whether it has designated a chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the company's organizational chart, the relevant expertise of any such persons, the processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents, and whether and how frequently such persons or committees report to the board or a committee of the board on cybersecurity risk. *Director Cybersecurity Expertise.* Proposed Item 407(j) of Regulation S-K would require companies to annually disclose (in proxy statements for their annual meetings of shareholders or their annual reports on Form 10-K) cybersecurity expertise of directors of the company, if any. If any member of the board has cybersecurity expertise, the company would be required to disclose the name of any such director, and provide such detail as necessary to fully describe the nature of the director's expertise. Cybersecurity expertise would remain undefined, but the proposed rule would introduce criteria relevant for the determination, such as whether the director has work experience in cybersecurity, whether the director obtained a certification or degree in cybersecurity, and whether the director has knowledge, skills or other background in cybersecurity. Similar to the existing safe harbor with respect to “audit committee financial experts," proposed Item 407(j)(2) would state that a person who is determined to have expertise in cybersecurity will not be deemed an expert for any purpose, including, without limitation, for purposes of Section 11 of the Securities Act of 1933, as a result of being designated or identified as a director with expertise in cybersecurity pursuant to proposed Item 407(j). *Foreign Private Issuers.* Comparable changes would be made to require similar disclosures on an annual basis on Form 20-F. Structured Data Requirements Disclosures required under the proposed rules would need to be tagged in Inline XBRL, which would include block text tagging of narrative disclosures, as well as detail tagging of quantitative amounts disclosed within the narrative disclosures. According to the release, “[t]his Inline XBRL tagging would enable automated extraction and analysis of the granular data required by the

proposed rules, allowing investors and other market participants to more efficiently perform large-scale analysis and comparison of this information across registrants and time periods."[7] For additional information on the proposed amendments, please see the following links:

- Press Release
- Proposed Rule
- Fact Sheet

Commissioner Concerns The Commission voted three to one in support of the proposed amendments, with Commissioner Peirce dissenting. Chair Gensler supported the proposed rules noting that "companies and investors alike would benefit if this disclosure were required in a consistent, comparable, and decision-useful manner."[8] Chair Gensler emphasized two ways in which the proposed rules would enhance cybersecurity disclosure and allow investors to assess cybersecurity risks more effectively, by requiring (i) ongoing disclosures regarding companies' governance, risk management, and strategy with respect to cybersecurity risks and (ii) mandatory, material cybersecurity incident reporting. Commissioner Peirce expressed some reservations about the proposal. Specifically, Commissioner Peirce voiced concern that: (i) the governance disclosure requirements could be viewed as substantive guidance for the composition and functioning of both the boards of directors and management of public companies; (ii) the policy disclosure requirements may pressure companies to consider adapting their existing policies and procedures to conform to the Commission's preferred approach; and (iii) the Commission is not best suited to design cybersecurity programs to be effective for all companies. Although Commissioner Peirce was more supportive of the cybersecurity incident reporting requirements, stating that they provided guideposts for companies to follow in reporting material cybersecurity incidents, she was critical of the proposed rule's inflexibility with regard to whether temporary relief from the disclosure requirements would best protect investors in cases of ongoing investigations. For the published statements of the Commissioners, please see the following links:

- Chair Gensler
- Commissioner Peirce
- Commissioner Crenshaw

As mentioned above, the comment period ends on the later of 30 days after publication in the Federal Register or May 9, 2022 (which is 60 days from the date that the rules were proposed). Comments may be submitted: (1) using the SEC's comment form at https://www.sec.gov/rules/submitcomments.htm; (2) via e-mail to rule-comments@sec.gov (with "File Number S7-09-22" on the subject line); or (3) via mail to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090. All submissions should refer to File Number S7-09-22. **Takeaways** The proposed rule contemplates extensive changes to current reporting requirements, and many of the disclosure topics act as guidance with respect to the SEC's expectations for public companies' cybersecurity risk management, strategy, and governance. In light of these changes, public companies should consider the following:

- ***Incident Disclosure Obligations Take Priority Over All Other Considerations.*** As noted by Commissioner Peirce, proposed Item 1.05 of Form 8-K does not provide companies with flexibility with respect to the timing of disclosing material cybersecurity incidents, even when it may be beneficial to delay disclosure. Under the proposed rule, companies would be required to report material cybersecurity incidents within four business days of the materiality determination, even when doing so may hinder the efforts of law enforcement to investigate the extent of the incident or apprehend wrongdoers. The disclosure mandate would also effectively override any deferral provided under state and local law, as companies will still need to timely file the required Form 8-K even where a

state or local law would permit a delay in notifying the public about the incident. In addition, the proposed rule does not distinguish ongoing incidents from past or remediated incidents in the reporting requirements, which could result in required disclosure of cybersecurity incidents that still have active vulnerabilities. In these instances, disclosure could exacerbate the severity of the incident, as wrongdoers could become aware of and seek to exploit current vulnerabilities in the company's systems. In essence, the proposed rule does not allow companies to take into account any other considerations on whether to disclose material cybersecurity incidents. The proposing release justifies the rule by stating that it is “critical to investor protection and well-functioning orderly and efficient markets that investors promptly receive information regarding material cybersecurity incidents."[9] However, the SEC does not demonstrate that the inflexibility of the rule is necessary for the functioning of the markets or that such other considerations are less critical to investor protection than strict adherence to the proposed reporting regime. Moreover, the mere fact that the trigger date for the disclosure requirement is the date of the materiality determination does not provide companies with flexibility given the rule's expectation that companies will make such determination as soon as reasonably practicable after discovery of the incident.

- ***Companies May Need to Revisit their Cybersecurity Policies and Procedures.*** The proposed rule would require companies to disclose many facets of their cybersecurity policies and procedures, such as whether there are procedures for overseeing cybersecurity risk arising from the use of third party service providers. These disclosure topics are likely to incentivize companies to revisit their policies and procedures in order to ensure that they address such topics, as companies will want to avoid disclosure of policies that lack features that the SEC focuses on or that appear less robust than those of their peers. In addition, it will be important for companies revisiting their cybersecurity policies to ensure that they provide for effective disclosure controls and procedures that include communication between the cybersecurity team, or those responsible for cybersecurity, and the legal team. These channels of communication will be necessary for the prompt assessment and escalation of detected cybersecurity incidents, which serves the purposes of providing for proper oversight and complying with the proposed disclosure requirements. Communication will need to be maintained through the conclusion and remediation of cybersecurity incidents, given the requirement to provide material updates to the disclosure and to disclose any series of previously undisclosed, immaterial incidents that become material in the aggregate. Companies without a chief information security officer, or equivalent, should consider whether such a position should be created in light of the requirement to disclose whether the company has such an officer.
- ***Boards May Need to Revisit Their Oversight Role and Structures.*** While many companies already include disclosure on the board's role in overseeing cybersecurity risk in their proxy statements, the proposed rule introduces a broad set of discussion topics that will need to be addressed. In particular, boards that have not delegated responsibility for overseeing cybersecurity disclosures to a specific board committee will need to consider whether it is appropriate to do so. Companies should also consider the channels through which cybersecurity information is communicated to the board (or designated committee) and evaluate whether such channels provide effective and timely communications. Boards will also need to assess whether the amount of time spent addressing cybersecurity during meetings is appropriate given the requirement to disclose the frequency of discussions on the topic.
- ***Director Cybersecurity Experience will be at a Premium.*** Requiring disclosure of whether any of a company's directors have cybersecurity expertise will likely pressure companies to prioritize candidates with cybersecurity experience as part of their search process in order to avoid appearing behind on cybersecurity compared to their peers. Given that companies will need to describe such expertise in their annual disclosure, directors with substantive cybersecurity

experience may be highly sought after. In addition, many companies include cybersecurity in director skill matrices in their proxy statements. Should the rules be adopted as proposed, those companies will need to consider whether their assessments of experience align with the criteria proposed by the SEC, or risk potentially confusing investors with two different standards for cybersecurity expertise.

---

[1] Cybersecurity incident is defined to mean an unauthorized occurrence on or conducted through a company's information systems that jeopardizes the confidentiality, integrity, or availability of a company's information systems or any information residing therein.

[2] TSC Indus. v. Northway, 426 U.S. 438, 449 (1976).

[3] Basic Inc. v. Levinson, 485 U.S. 224, 232 (1988).

[4] 563 U.S. 27 (2011).

[5] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release, No. 34-94382 (Mar. 9, 2022) at Part II.B.1, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

[6] Id.

[7] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release, No. 34-94382 (Mar. 9, 2022) at Part II.G, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

[8] Chairman Gary Gensler, “Statement on Proposal for Mandatory Cybersecurity Disclosures" (Mar. 9, 2022), available https://www.sec.gov/news/statement/gensler-cybersecurity-20220309.

[9] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release, No. 34-94382 (Mar. 9, 2022) at Part II.B.3, available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

This alert was prepared by Alexander H. Southwell, Ashlie Beringer, Lori Zyskowski, Thomas J. Kim, and Julia Lapitskaya.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work in the firm’s Privacy, Cybersecurity and Data Innovation and Securities Regulation and Corporate Governance practice groups, or the following authors:

Alexander H. Southwell – New York (+1 212-351-3981, asouthwell@gibsondunn.com)

S. Ashlie Beringer – Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)

Lori Zyskowski – New York (+1 212-351-2309, lzyskowski@gibsondunn.com)

Thomas J. Kim – Washington, D.C. (+1 202-887-3550, tkim@gibsondunn.com)

Julia Lapitskaya – New York (+1 212-351-2354, jlapitskaya@gibsondunn.com)

We would like to thank Matthew Dolloff in our New York office for his work on this article.

advice.

Related Capabilities

Privacy, Cybersecurity, and Data Innovation

Securities Regulation and Corporate Governance