Westlaw Today
powered by Reuters

SEC proposes new rules for cybersecurity risk management, strategy, governance and incident disclosure

By Brian V. Breheny, Esq., Raquel Fox, Esq., Marc S. Gerber, Esq., and William Ridgway, Esq., Skadden, Arps, Slate, Meagher & Flom LLP*

MARCH 16, 2022

On March 9, 2022, the Securities and Exchange Commission (SEC) proposed rules[1] that are intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy and governance, as well as cybersecurity incident reporting, by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934.

Specifically, the SEC's proposed amendments would require companies to disclose:

- "Material cybersecurity incidents" on Form 8-K;
- Updates regarding previously reported cybersecurity incidents on Forms 10-K and 10-Q;
- The company's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board's oversight of cybersecurity risks on Form 10-K; and
- Whether any board member has cybersecurity expertise in proxy statements and annual reports.

The SEC is concerned that cybersecurity threats and incidents pose an ongoing and escalating risk to public companies, investors and market participants.

The proposed rules also would require similar disclosures for foreign private issuers on Form 6-K and new Item 16J of Form 20-F.

Companies must tag cybersecurity disclosures with Inline eXtensible Business Reporting Language (Inline XBRL).

Background

To date, the SEC's Division of Corporation Finance issued 2011 staff guidance[2] and the SEC issued its 2018 interpretive release[3] expressing views on how and when companies should make disclosures regarding cybersecurity incidents. In January 2022, noting the economic and national security threats posed by cyberattacks, SEC Chair Gary Gensler announced[4] that he had asked SEC staff to make recommendations for the SEC's consideration regarding companies' cybersecurity practices and cyberrisk disclosures.

As explained in the proposing release, the SEC is concerned that cybersecurity threats and incidents pose an ongoing and escalating risk to public companies, investors and market participants, and cyber criminals are using increasingly sophisticated methods to execute attacks. The SEC noted that cybersecurity incidents can result in adverse consequences that can affect long-term shareholder value, including business disruption costs and lost revenues, ransom payments, remediation and restoration costs, increased cybersecurity protection costs, litigation and legal risks, harm to employees or customers, and damage to the company's reputation and competitiveness. In light of these risks, the SEC believes investors would benefit from greater availability and comparability of disclosures regarding cybersecurity risk management, strategy and governance practices.

Key requirements of proposed incident disclosure rules

Incident reporting. The proposed rules would amend Form 8-K to add new Item 1.05 to require companies to provide disclosure within four business days after the company determines that it has experienced a material "cybersecurity incident" as defined in proposed Regulation S-K Item 106(a). Materiality for purposes of the proposed rules would be consistent with the standard established by case law.

The 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.

Importantly, the proposed rule defines the trigger for Item 1.05 of Form 8-K as the date on which the company determines that a cybersecurity incident it has experienced is material, rather than the date of discovery of the incident.

Updating disclosure and incidents material in the aggregate. Proposed Item 106(d) of Regulation S-K would require companies to disclose in the company's quarterly report on Form 10-Q or annual report on Form 10-K for the period in which it occurred, (i) any material changes, additions or updates to a previous disclosure under Item 1.05 of Form 8-K and (ii) any individually immaterial cybersecurity incidents not previously disclosed that become material in the aggregate. Such disclosure would include the same information required by proposed Item 1.05 of Form 8-K.

Cybersecurity risk management, strategy and governance disclosure

Risk management. Proposed Item 106(b) of Regulation S-K would require companies to disclose, as applicable, whether:

- The company has a cybersecurity risk assessment program and, if so, a description of the program;
- The company engages assessors, consultants, auditors or other third parties in connection with any cybersecurity risk assessment program;
- The company has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider;
- The company undertakes activities to prevent, detect and minimize the effects of cybersecurity incidents;
- The company has business continuity, contingency and recovery plans in the event of a cybersecurity incident;
- Previous cybersecurity incidents have informed changes in the company's governance, policies and procedures, or technologies;
- Cybersecurity-related risks and incidents have affected or are reasonably likely to affect the company's results of operations or financial condition and, if so, how; and
- Cybersecurity risks are considered as part of the company's business strategy, financial planning and capital allocation and, if so, how.

Governance. Proposed Item 106(c) of Regulation S-K would require companies to disclose information related to cybersecurity governance, including the board's oversight of cybersecurity risks 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 company's cybersecurity policies, procedures and strategies.

Proposed Item 106(c)(1) would require the following disclosures about the board's oversight of cybersecurity risks:

- 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 of cybersecurity risks and the frequency of its discussions on this topic; and
- Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

Although SEC rules have long required companies to disclose information about material cybersecurity incidents, the proposal would impose a four-day deadline.

Proposed Item 106(c)(2) would require the following disclosures about management's role in assessing and managing cybersecurity-related risks and in implementing the company's cybersecurity policies, procedures and strategies:

- Whether certain management positions or committees are responsible for measuring and managing cybersecurity risks — specifically the prevention, mitigation, detection and remediation of cybersecurity incidents, and the relevant expertise of such persons or committee members;
- Whether the company has a 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, and 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 of directors or a board committee on cybersecurity risks.

Board of directors cybersecurity expertise. Proposed Item 407(j) of Regulation S-K, applicable to proxy statements and annual reports on Form 10-K, would require disclosure about the cybersecurity expertise of any members of the board of directors, including the name(s) of any such director(s) and a description of the nature of the expertise.

Proposed Item 407(j)(1)(ii) includes the following nonexclusive list of criteria that companies would need to consider in reaching a determination on whether a director has expertise in cybersecurity:

- Whether the director has prior work experience in cybersecurity;
- Whether the director has obtained a certification or degree in cybersecurity; and

- Whether the director has knowledge, skills or other background in cybersecurity.

Inline XBRL tagging. The proposed rules would require Item 1.05 of Form 8-K and Items 106 and 407(j) of Regulation S-K to be tagged using Inline XBRL.

Takeaways

Although SEC rules have long required companies to disclose information about material cybersecurity incidents, the proposal would impose a four-day deadline, which companies may find challenging to meet without protocols in place for prompt escalation and assessment of cybersecurity incidents. The proposal also includes more detailed and prescriptive disclosure requirements about the company's management of cybersecurity risks, board governance of such risks and the directors' cybersecurity expertise. Companies may want to consider how their disclosures under the proposed rules would look. Companies may also want to consider whether their current cybersecurity incident response plans include adequate escalation and assessment protocols to meet applicable regulatory disclosure deadlines and test such plans to provide management and board members with experience in how the company will meet such deadlines when responding to cybersecurity incidents.

Next steps

Comments on the proposal are due in 60 days (by May 9, 2022) or 30 days after publication in the Federal Register, whichever is later. The proposal includes specific requests for comment on a number of aspects of the proposed rules, in addition to soliciting comments generally.

Notes

[1] https://bit.ly/3MXkuX4

[2] https://bit.ly/3JfJ17r

[3] https://bit.ly/3icXg0E

[4] https://bit.ly/3qafG6F

About the authors




(L-R) **Brian V. Breheny** is a Washington, D.C.-based corporate partner and heads **Skadden, Arps, Slate, Meagher & Flom LLP**'s Securities and Exchange Commission reporting and compliance practice. **Raquel Fox** is also a corporate partner in the firm's Washington, D.C., office, concentrating on capital markets, mergers and acquisitions, corporate governance, and general corporate and securities matters. She advises clients on the full range of SEC reporting and compliance requirements. **Marc S. Gerber** is an M&A partner in the firm's Washington, D.C., office. He concentrates in the areas of mergers and acquisitions, corporate governance, general corporate and securities regulation, and environmental, social and governance matters. Gerber has represented purchasers and sellers in a wide variety of transactions, including private acquisitions and divestitures, negotiated and contested public acquisitions, and proxy fights. **William Ridgway** is a litigation partner based in the firm's Chicago office. He focuses on white collar crime, cybersecurity, data privacy and national security matters, and complex civil litigation. He also co-leads the firm's cybersecurity practice and advises clients on incident preparation and response issues. This article was originally published March 11, 2022, on the firm's website. Republished with permission.

This article was published on Westlaw Today on March 16, 2022.