JONES DAY

COMMENTARY

MARCH 2022

SEC Proposes Amendments Regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

IN SHORT

The Situation: On March 9, 2022, the U.S. Securities and Exchange Commission (the "SEC") proposed amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.

The Potential Result: If adopted as proposed, the amendments would, among other things, require current disclosure of material cybersecurity incidents within four business days of the determination that a cybersecurity incident is material, and periodic updates regarding previously reported cybersecurity incidents. The proposed amendments also would require periodic reporting about a registrant's policies and procedures to identify and manage cybersecurity risks; a registrant's board of directors' oversight of cybersecurity risk; management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures; and a registrant's board of directors' cybersecurity expertise, if any.

Looking Ahead: The proposed amendments are subject to a comment period of up to 60 days, and any final amendments to the current framework could reflect additional modifications made by the SEC in response to comments received on the proposed amendments.

As part of the SEC's broader rulemaking initiative, on March 9, 2022, the SEC proposed amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. The amendments are intended to provide consistent, comparable, and decision-useful disclosures that allow investors to evaluate registrants' exposure to cybersecurity risks and incidents as well as their ability to manage and mitigate those risks and incidents.

Existing Regulatory Framework Regarding Cybersecurity Disclosure

There are currently no disclosure requirements in Regulation S-K or Regulation S-X that explicitly refer to cybersecurity risks or incidents. Over the past decade, the SEC and its staff have issued interpretive guidance concerning the application of existing disclosure and other requirements under the federal securities laws relating to cybersecurity risks and incidents.

Disclosure of Material Cybersecurity Incidents

Under the proposals, Form 8-K would be amended to add Item 1.05, which would require registrants to disclose information about a material cybersecurity incident within four business days. The trigger for disclosure would be the date on which the registrant determines that a cybersecurity incident it has experienced is material, as opposed to the date on which the cybersecurity incident occurred. A registrant would be required to disclose a material cybersecurity incident on Form 8-K under the federal securities laws even if state law would otherwise allow the registrant to delay providing notice about such incident.

> The proposed SEC amendments are intended to provide consistent, comparable, and decision-useful disclosures that

> allow investors to evaluate registrants' exposure to cybersecurity risks and incidents as well as their ability to manage and mitigate those risks and incidents.

Periodic Cybersecurity Reporting

The proposed amendments include the addition of a new Item 106 to Regulation S-K and amendments of Forms 10-Q and 10-K, which would require a registrant to periodically report on the following items related to cybersecurity:

- Material changes, additions, or updates to cybersecurity incidents previously disclosed pursuant to Item 1.05 of Form 8-K;
- A series of previously undisclosed related, individually immaterial cybersecurity incidents that become material in the aggregate;
- The registrant's policies and procedures, if any, for identifying and managing 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 registrant's cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risks; and
- Management's role, and relevant expertise, in assessing and managing cybersecurity related risks and implementing related policies, procedures, and strategies.

The SEC acknowledged that registrants may not have complete information about a material cybersecurity incident at the time it determines a Form 8-K filing is required. Accordingly, Item 106 to Regulation S-K generally would permit registrants to disclose material changes, additions, and updates to prior disclosure in its Forms 10-Q and 10-K filings. However, the SEC also noted that certain situations may require and amended Form 8-K filing, including if the incident is determined to be significantly more severe than previously disclosed.

The proposed amendments also include an amendment to Item 407 of Regulation S-K that would require disclosure regarding whether any member of the registrant's board of directors has cybersecurity expertise.

Foreign Private Issuers

The proposed changes include amendments to Forms 20-F and 6-K that would require foreign private issuers to provide cybersecurity disclosure consistent with the disclosure proposed for domestic issuers.

FOUR KEY TAKEAWAYS

1. The proposed addition of Item 1.05 to Form 8-K would require disclosure of cybersecurity incidents within four days of determining they are material, regardless of state laws that could otherwise delay such disclosure and distinct from other state or federal reporting obligations (e.g., to customers, consumer credit reporting entities, state or federal regulators, and law enforcement agencies, etc.).
2. The addition of Item 106 of Regulation S-K and the amendment of Item 407 of Regulation S-K would significantly increase the required periodic disclosure of cybersecurity incidents and practices. Registrants


Bradley C. Brasser
Minneapolis/Chicago


Peter E. Devlin
New York


Rory T. Hood
New York


James T. Kitchen
Pittsburgh

should be prepared to increase the breadth of cybersecurity disclosure in their periodic reports.

3. Registrants should evaluate their internal cybersecurity policies and procedures, governance, and risk management practices with an eye toward increased public disclosure, and evaluate the risks associated with increased disclosure obligations.

4. Registrants should evaluate their current and potential directors for cybersecurity expertise.

Joel T. May
Atlanta

Mauricio F. Paez
New York

Lisa M. Ropple
Boston

Michael J. Solecki
Cleveland

Edward B. Winslow
Chicago

Jeremy W. Cleveland and Casey Duckworth, associates in the Silicon Valley Office, assisted in the preparation of this Commentary.