SEC Proposes New Rules on Cybersecurity Disclosures: Four Things to Know

Carol W. Sherman, Lauren Kouser

March 30, 2022

On March 9, the U.S. Securities and Exchange Commission (SEC) announced proposed amendments to its rules regarding cybersecurity disclosures to satisfy a growing investor need to know more about how registrants are managing emerging cybersecurity risks.

The proposed rules enhance and standardize registrants' cybersecurity disclosures regarding risk management, strategy, governance and incident reporting. The proposed rules would adopt mandatory disclosures in periodic reports, require current reporting of material cybersecurity incidents on Form 8-K and require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL).[1]

The proposed rules would require registrants to include in periodic disclosures, among other things, policies and procedures to identify and manage cybersecurity risks; management's role in implementing cybersecurity policies and procedures; board of directors' oversight of cybersecurity risk; and updates about previously reported material cybersecurity incidents. The proposal further would require annual reporting or certain proxy disclosure about the board of directors' cybersecurity expertise, if any.

The proposed rules would require disclosures on Form 10-K about a company's governance, risk management, and strategy with respect to cybersecurity risks. SEC chair Gary Gensler expressed support for the proposed rules as a means to strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting by requiring information to be disclosed in a "consistent, comparable and decision-useful manner."

Highlights of the proposed rules include the following.

INCIDENT DISCLOSURE

Current reporting of material cybersecurity incidents would be required. A material cybersecurity incident may result from accidental exposure of data or intentional attacks. This may include, for example, an unauthorized incident which compromised the confidentiality, integrity, or availability of an information asset, or a violation of the registrant's security policies or procedures; an unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems; an unauthorized party accessing, or a party exceeding authorized access, and altering or stealing data; a malicious actor offering to sell or threatening to publicly disclose sensitive company data; or a malicious actor demanding payment to restore company data that was altered or stolen.[2]

The proposed rules would amend Form 8-K to require that registrants disclose information about a material cybersecurity incident within four business days after determining it has experienced a material cybersecurity incident. In addition to a brief description of the nature and scope of the incident, such disclosure would include, to the extent known, when the incident was discovered, whether it is ongoing, whether any data was compromised, any effect of the incident on the registrant's operations and any remediation efforts. Form 6-K would also be amended under the proposed rules to add "cybersecurity incidents" as a reporting topic for foreign issuers.

The proposed rules would amend Form 10-K and Form 10-Q to require that registrants provide updated disclosures regarding previously disclosed cybersecurity incidents and, to the extent known to management, disclose when a series of previously undisclosed immaterial cybersecurity incidents become material in the aggregate.

RISK MANAGEMENT, STRATEGY AND GOVERNANCE DISCLOSURE

Companies would also have to periodically disclose their risk management, strategy and governance processes for managing cybersecurity risks. The proposed rules would amend Form 10-K to require a registrant to describe its policies and procedures for identifying and managing cybersecurity threats, which includes whether cybersecurity is part of the registrant's business strategy, financial planning and capital allocation. The proposed rule would also require disclosure regarding the board's oversight of cybersecurity risks and management's role and expertise in assessing and managing cybersecurity risks and implementing the related policies, procedures and strategies.

Under the proposed amendment to Item 407 of Regulation S-K, a registrant must also disclose in annual reports and certain proxy filings whether any board member has any expertise in cybersecurity, including the name of any such director and details describing the nature of the expertise.

The proposed rule changes would also apply to foreign issuers and would require foreign issuers to include cybersecurity disclosures in their annual reports filed on Form 20-K that are consistent with the required disclosures proposed on the domestic forms.

CONCLUSION

The proposed amendments are intended to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification to investors of material cybersecurity incidents.

The proposed rules are subject to public comment, which comment period will remain open through May 9, 2022.

---

[1] *See* SEC Fact Sheet, Public Company Cybersecurity Proposed Rules *available at* https://www.sec.gov/files/33-11038-fact-sheet.pdf.
[2] *See* SEC Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure *available at* https://www.sec.gov/rules/proposed/2022/33-11038.pdf.