In brief

No. US2022-04
March 17, 2022

SEC proposes new cybersecurity disclosure requirements

At a glance

The SEC proposed new disclosures related to cybersecurity for all public companies and foreign private issuers. Comments are due on the proposal in May.

What happened?

On March 9, the SEC proposed amendments to enhance and standardize disclosures related to cybersecurity. Key provisions of the proposal, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, include the following.

Timely disclosure of material incidents

A registrant would be required to report a cybersecurity incident on Form 8-K within 4 business days of when it is determined to be material. The determination of whether an incident is material would be based on the definition of materiality used in the securities laws.

Disclosures 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 registrant's operations, and
- whether the registrant has remediated or is currently remediating the incident.

Registrants would also need to disclose in their Form 10-Ks and 10-Qs any material changes, additions, or updates to information that was previously disclosed in the Form 8-K in which the initial incident was reported. In addition, a series of previously unreported individually immaterial incidents would need to be disclosed in Forms 10-K and 10-Q when they become material in the aggregate.

Annual disclosures of risk management and strategy

Proposed Item 106 in Regulation S-K would require registrants to provide more consistent and informative disclosure on their cybersecurity risk management and strategy. Disclosures would include management's role and relevant expertise in assessing and managing cybersecurity risks and implementing related policies, procedures, and strategies. The proposal also calls for expanded disclosures of policies and procedures, if any, for identifying and managing cybersecurity risks and information about a registrant's cybersecurity governance.

Management's role and expertise

Disclosures of management's role and expertise would include:

- whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, and a description of their relevant expertise,

- whether there is a designated chief information security officer, or comparable, and to whom that individual reports within the organization, and a description of their relevant expertise,
- the processes by which information security officers or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents, and
- whether and how frequently information security officers or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.

Policies and procedures for identifying and managing cybersecurity risk

Disclosures of policies and procedures would include a description of the registrant's cybersecurity risk assessment program, if any, contingency or recovery plans, and use of third parties. In addition, a registrant would be required to disclose whether and how it considers cybersecurity risks as part of its business strategy, financial planning, and capital allocation, as well as to explain how previous cybersecurity incidents have informed changes in its governance structure.

Lastly, a registrant should indicate whether cybersecurity risk and incidents have affected or are reasonably likely to affect its results of operations or financial condition and if so, how.

Board governance

Registrants would be required to disclose details of the board of directors' oversight of cybersecurity risk and cybersecurity expertise, if any. Disclosures related to board oversight would include:

- whether the full board, specific members, or a committee is responsible for oversight of cybersecurity risks,
- the processes by which the board is informed about 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.

Registrants would also be required to disclose whether any director has cybersecurity expertise, and if so, the director's name and the nature of that expertise. While the proposal does not define "cybersecurity expertise," it includes criteria that should be considered in this determination, including whether a director has prior work experience in or knowledge of cybersecurity or a certification or degree in cybersecurity.

Other new cyber rules and proposals

Legislative action

On March 15, the Strengthening American Cybersecurity Act (the Act) was signed into law. Provisions of this Act will require critical infrastructure owners and operators to report "substantial" cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours and ransomware payments within 24 hours. The Act also grants the CISA director broad authority to develop rules within 24 months. See our Cyber breach reporting to be required by law for better cyber defense for more details.

SEC proposal for registered investment advisors and funds

The SEC proposed a rule in February that would require registered investment advisers, registered investment companies, and business development companies to adopt and implement written cybersecurity policies and procedures to address cybersecurity risks. The proposal also would require advisers to confidentially report significant cybersecurity incidents affecting the adviser or its fund or private fund clients to the SEC.

Existing SEC cyber guidance

Current SEC interpretive guidance on cybersecurity disclosure is included in 2011 and 2018 disclosure guidance. Current guidance may require disclosure of cybersecurity risks, policies and procedures, and material incidents in Risk Factors, Business Description, MD&A, Legal Proceedings, Disclosure Controls & Procedures, or the financial statements, but there are no prescriptive requirements as to the level of detail.

Why is this important?

The March 9 proposal applies to all public companies, including foreign private issuers (FPIs). Although disclosure requirements currently vary for domestic and foreign registrants, the proposal would amend the requirements for FPIs to provide consistent cybersecurity disclosures for all registrants.

According to the SEC's release, the amendments are designed to provide investors with better information about a registrant's cybersecurity risk management, strategy, governance, and exposure to cybersecurity incidents.

If the rules are finalized as currently proposed, several of the provisions will be subject to interpretation and judgment, including how to apply the definition of a cyber incident and how to determine which incidents are material.

What's next?

Comments are due the later of 30 days after it is published in the Federal Register or May 9. The SEC will consider the feedback received and issue a final rule, likely before the end of the year. In the interim, companies should consider whether their processes, controls, governance structure, or disclosures would need to be enhanced to comply with the proposal if it were finalized as currently drafted.

We will release a podcast later in March that summarizes the proposal. Look for it at viewpoint.pwc.com or wherever you get your podcasts.

To have a deeper discussion, contact:

Mary Grace Davenport
Partner
Email: mary.grace.davenport@pwc.com

Kyle Moffatt
Partner
Email: kyle.moffatt@pwc.com

Valerie Wieman
Partner
Email: valerie.wieman@pwc.com

Maria Constantinou
Managing Director
Email: maria.constantinou@pwc.com

For more PwC accounting and reporting content, visit us at viewpoint.pwc.com. On the go? Take our podcast series with you at the Viewpoint podcasts page.