KPMG

Regulatory Alert

Regulatory Insights

July 2023

Public Company Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure

KPMG Insight:

- *The SEC's final rule on cybersecurity disclosure for public companies introduces new requirements across cyber risk management, strategy, governance, and incident reporting.*
- *The final rule will increase the prominence of required disclosure of cybersecurity incidents in corporate filings and will likely spur boards and senior management to greater engagement on cybersecurity preparedness given the required disclosure of their roles in overseeing and implementing (as appropriate) policies, procedures, strategies, and programs to identify and manage cybersecurity risks.*
- *SEC significantly expanded the size of its cyber enforcement unit last year and in 2023 has named Cybersecurity (and its potential to impact operational resiliency) as an examination priority, with a key area of focus being the risk that cybersecurity failures pose to investor and consumer protection and national security.*
  - *Key issues for review will include appropriate controls and documentation around:*
  - *Incident response and resiliency*
  - *Governance and strategy*
  - *Access management*
  - *Third-party risk management*
  - *Training and awareness campaigns*
  - *Application of lessons learned*

The SEC issued final rules and amendments related to cybersecurity risk management, strategy, governance, and incident reporting for public companies subject to the Securities Exchange Act of 1934 (i.e., registrants).

These rules and amendments were adopted along the same thematic elements as proposed (see KPMG's Regulatory Alert, here), with some modifications to lessen incident reporting and disclosures around cybersecurity expertise (highlighted below); the rules and amendments are intended to enhance and standardize cybersecurity disclosures, as well as establish current and periodic reporting requirements.

Definitions. Definitions used throughout the new rules and amendments (outlined in new Item 106(a) of Regulation S-K) include:

- *Cybersecurity incident* means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.
- *Cybersecurity threat* means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.
- *Information systems* means electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

Cybersecurity Incidents Reporting on Form 8-K. Requires registrants to disclose information about a material cybersecurity incident "within four business days after the registrant determines that it has experienced a material cybersecurity incident." Modifications to the proposal are intended to "streamline" the required information, outlined in new Item 1.05 of Form 8-K, to include a description of the:

- Material aspects of the nature, scope, and timing of the incident, and
- Material impact or reasonably likely material impact on the registrant, including financial condition and results of operations.

SEC, citing the need to balance investors' needs and registrants' cybersecurity posture, did not adopt proposed disclosures regarding registrants' remediation status, whether the incident is ongoing, and whether data were compromised.

With regard to the timing of incident notification and materiality, SEC notes:

- The trigger for incident notification is the date on which a registrant "determines that it has experienced a material cybersecurity incident", rather than the date of incident discovery, although the two dates may coincide; registrants will be expected to make a materiality determination "without unreasonable delay" after discovery of the incident.
- Information will be deemed *material* if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."
- In an add-on to the proposal, SEC adopted a provision that disclosure may be delayed if the U.S. Attorney General determines that immediate disclosure would pose "substantial risk to national security or public safety" and notifies SEC in writing. SEC will consider additional requests for delay and may grant relief through exemptive orders.

SEC did not adopt the proposed Item 601(d)(1) that would have required for registrants to provide disclosure on their Form 10-Q or Form 10-K any "material changes, additions, or updates" to cybersecurity incidents that had been previously disclosed in Form 8-K. Instead, the final rules require registrants to file Form 8-K amendments within four business days after determining any information from Item 1.05 that was not previously determined or unavailable at the time of the required original filing.

Cybersecurity Risk Management, Strategy, and Governance Disclosures. Requires registrants to provide consistent and informative disclosures regarding their processes (in contrast to policies and procedures, as proposed), if any, for assessing, identifying, and managing material risks from cybersecurity threats (outlined in new Item 106(b)(1) of Regulation S-K), including whether the registrant:

- Has integrated cybersecurity processes into overall risk management system or processes, and how.
- Engages assessors, consultants, auditors, or other third parties in connection with such processes.
- Has processes to oversee and identify material risks from cybersecurity threats associated with use of any third-party service provider.

Additionally, registrants are required to provide a description of whether any risks from cybersecurity threats have materially affected the registrant. This information, outlined in new Item 106(b)(2) of Regulation S-K, would include whether previous cybersecurity incidents have materially affected a registrant's business strategy, results of operations, or financial condition, and if so, how.

The SEC did not adopt previously proposed disclosure elements regarding the registrant's prevention and detection activities, continuity and recovery plans, and previous incidents.

Board oversight. In the final rule, the SEC has "streamlined" required disclosure of the board's oversight of risks from cybersecurity threats (outlined in new Item 106(c)(1)), to include:

- Identification of any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats, and
- Description of the processes through which the board or responsible committee is informed about the risks.

SEC did not adopt the proposed disclosure on board cybersecurity expertise (proposed amendments to Item 407(j)) though the final rule does require disclosure of management expertise (described below). The SEC notes that it will continue to examine and consider board expertise, as applicable.

Role of management. Correspondingly, the final rule requires a description of management's role in assessing and managing material risks from cybersecurity threats (outlined in new Item 106(c)(2)), including whether:

- Certain management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise.
- The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents.
- Such persons or committees report information about risks from cybersecurity threats to the board or responsible board committee.

Foreign Private Issuers. The SEC also adopted rules and amendments to align incident reporting and periodic disclosures of foreign private issuers (FPIs) with those of public companies, as outlined below:

- Amended **Form 6-K**, like Form 8-K, to include "cybersecurity incidents" as a trigger for reporting for FPIs.
- Amended **Form 20-F** by adding new Item 16K which will require the same disclosures in FPI annual reports as new Item 106 of Regulation S-K.

Structured Data Requirements. The structured data requirements have been adopted as proposed. Registrants are required to report and disclose the above information in Inline XBRL format, in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual, beginning one year after initial compliance period with the related disclosure requirements (outlined below). Submission in the format is expected to make disclosures and reports more available and accessible to investors, market participants, and others.

Effective Date and Compliance Period. The final rules will become effective 30 days following publication in the Federal Register, and require:

- All registrants to provide disclosures in Regulation S-K Item 106 and comparable items in Form 20-F beginning with annual reports for fiscal years ending on or after December 15, 2023.
- All registrants other than smaller reporting companies to begin complying with the incident disclosure requirements in Form 8-K Item 1.05 and in Form 6-K on the later of 90 days after publication in the Federal Register, or December 18, 2023. Smaller reporting companies must begin complying with Form 8-K Item 1.05 on the later of 270 days from the effective date of the rules or June 15, 2024.

For more information, please contact Matt Miller, or Jonathan Fairtlough.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialmedia