KPMG

Regulatory Alert

Regulatory Insights

March 2022

Cybersecurity: SEC Proposals for Public Company Reporting, Disclosures

The SEC cybersecurity disclosure proposed rules reiterate the importance of cyber hygiene and incident reporting. The proposed rules would increase the prominence of required disclosure of cyber security incidents in a number of corporate filings, including annual filings and on Forms 8-K and 6-K. For registered companies, the proposed disclosure requirements would demand (1) a better understanding of risks and potentially new technology and processes to meet the potential reporting requirements and (2) greater engagement on cyber security preparedness. Organizations should look to enhance their current cybersecurity risk management and reporting processes accordingly.

The SEC has proposed 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 proposals are intended to enhance and standardize disclosures around cybersecurity. As proposed, the rules would establish both current and periodic reporting - requirements.

Definitions. Proposed Item 106(a) of Regulation S-K outlines definitions used throughout the proposal, including:

- *Cybersecurity incident* would mean an unauthorized occurrence 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* would mean any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein
- *Information systems* would mean 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. A new proposed Item 1.05 would be added to Form 8-K and require 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. This information 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 unauthorized purpose

- The effect of the incident on the registrant's operations
- Whether the registrant has remediated, or is currently remediating, the incident

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

- The trigger for incident notification would be the date on which a registrant determines that a cybersecurity incident is material, rather than the date of incident discovery, although the two dates may coincide; registrants would be expected to make a materiality determination as soon as reasonably practicable after discovery of the incident
- Information would 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."

Cybersecurity Incidents Disclosure in Periodic Reports. Proposed Item 106(d)(1) of Regulation S-K would amend **Forms 10-Q and 10-K** to require disclosure of material changes, additions, or updates of the incidents disclosed in Form 8-K. The proposal includes "non-exclusive" examples of the types of disclosures that would be provided, including:

- Any material impact of the incident on the registrant's operations and financial condition
- Any potential material future impacts on the registrant's operations and financial condition
- Whether the registrant has remediated, or is currently remediating, the incident
- Any changes in the registrant's policies and procedures because of the cybersecurity incident, and how the incident may have informed such changes

Additionally, proposed Item 106(d)(2) would require disclosure, or updates to previous disclosures, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate.

Cybersecurity Risk Management, Strategy, and Governance Disclosures. Proposed Item 106(b) of Regulation S-K would require registrants to provide consistent and informative disclosures regarding their ***policies and procedures*** around cybersecurity risk management and strategy, including whether:

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

Board oversight. In addition, proposed Item 106(c)(1) would require disclosure of the board's oversight of cybersecurity risk, including:

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

Role of management. Correspondingly, proposed Item 106(c)(2) would require a description of management's role in assessing and managing cybersecurity-related risks and in implementing the registrant's cybersecurity policies, procedures, and strategies, including:

- Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members

- Whether the registrant has a designated a chief information security officer, or someone in a comparable position, and to whom that individual reports within the registrant'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
- Whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk

Board expertise. Finally, the proposal would amend Item 407 of Regulation S-K to add paragraph (j) which would require disclosure regarding board member cybersecurity expertise. Specifically, it would require disclosure in annual reports and certain proxy filings if any member of the registrant's board of directors has expertise in cybersecurity, including the name(s) of such director(s) and details necessary to describe the nature of their expertise

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

- Amends **Form 6-K**, like Form 8-K, to include "cybersecurity incidents" as a trigger for reporting for FPIs
- Amends **Form 20-F** by adding proposed Item 16J which would require the same disclosures in FPI annual reports as proposed in Items 106 and 407(j) of Regulation S-K.

Structured Data Requirements. The SEC also proposed requiring registrants 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. Submission in the format is expected to make disclosures and reports more available and accessible to investors, market participants, and others.

Public comment period. The SEC is seeking public comments on the proposed rules. The SEC states the public comment period will remain open for 30 days following the publication of the proposal in the Federal Register, or May 9, 2022 (60 days after publication on the SEC's website), whichever period is longer.

Please refer to:

- SEC Proposed Rules: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
- KPMG Regulatory Alert | Cybersecurity: SEC Proposal for Adviser/Fund Risk Management
- KPMG Regulatory Alert | Cybersecurity: SEC Reg SCI Proposal, Future Considerations
- KPMG Regulatory Alert | Cyber incident notifications

For additional information, please contact Matt Miller, Fred Rica, or Timothy Brown.

Contact the author:

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

kpmg.com/socialmedia