Published on *The National Law Review* https://natlawreview.com

SEC Adopts Cybersecurity Incident and Risk Management Disclosure Rules

Article By:

Eric S. Wu

Bruce A. Radke

Michael J. Waters

Brandon P. Krueger

On July 26, 2023, the Securities and Exchange Commission (the "***SEC***") adopted new rules requiring public companies to disclose within four business days material cybersecurity incidents they experience and to disclose annually their cybersecurity risk management, strategy, and governance. In response to opposition expressed during the comment period, these final rules omitted several of the more burdensome aspects of the rules that were originally proposed in March 2022.

Form 8-K Disclosure of Material Cybersecurity Incidents

- The SEC added a new Item 1.05 to Form 8-K that requires companies to disclose a cybersecurity incident within four business days of the date such cybersecurity incident is determined to be *material*.
    - Instruction 1 to Item 1.05 requires registrants to make a materiality determination without unreasonable delay after the discovery of the incident.
    - The materiality standard is the same as with respect to other required disclosures – information is material "if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision" or if it would have "significantly altered the 'total mix' of information made available."
    - Item 1.05 permits the registrant to delay disclosure of the incident if the U.S. Attorney General concludes and notifies the SEC in writing, that immediate disclosure poses a substantial risk to national security or public safety.
    - The U.S. Attorney General may take into consideration other Federal or non-Federal law enforcement agencies' findings.

- Item 1.05(a) requires the registrant to describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact (or reasonably likely material impact) on the registrant and its financial condition and results of operations.
    - No disclosure is required regarding the incident's remediation status, whether it is ongoing, or whether data were compromised. However, discussion of data theft, asset loss, intellectual property loss, reputational damage, or business value loss may still be relevant to the materiality determination.
    - Further, registrants are not required to disclose specific or technical information about the planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities to the extent such details would hinder the registrant's response to or remediation of the incident.
    - Instruction 2 to Item 1.05 requires registrants to file an amendment on Form 8-K/A to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing within four business days after the registrant, without unreasonable delay, determines such information.
- Notably, the SEC amended the instructions to Form S-3 by adding Item 1.05 to the list of Form 8-K items for which an untimely filing would not result in the loss of eligibility to use shelf registration statements filed on Form S-3.
- Due to the fact that registrants must evaluate materiality immediately after discovery of the relevant incident, the SEC also adopted amendments to Rules 13a-11(c) and 15d-11(c) under the Securities Exchange Act of 1934, as amended (the "***Exchange Act***"), to include Item 1.05 in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act.

Annual Disclosure of Cybersecurity Risk Management, Strategy and Governance

- The SEC added Item 106 to Regulation S-K that requires disclosure in a registrant's annual report on Form 10-K of (1) the registrant's processes – if any – for assessing, identifying, and managing material risks from cybersecurity threats, and whether any risks from cybersecurity threats, including risks from previous cybersecurity incidents, have materially affected (or are reasonably likely to materially affect) the registrant, and (2) the Board's oversight of such risks and management's role in assessing and managing such risks.
    - Under this requirement, registrants should provide investors with enough information for them to understand the registrant's cybersecurity practices, but the disclosure need not include a level of detail that could increase the registrant's vulnerability to future cyberattacks.
- Item 106(a) contains the following definitions (which also apply to new Item 1.05 of Form 8-K discussed above):
    - *"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.

- Item 106(b)(1) specifically requires registrants to disclose the following in sufficient detail for a reasonable investor to understand:

  - whether they have processes to oversee and identify material risks from cybersecurity threats associated with their use of third-party service providers;

  - whether they engage assessors, consultants, auditors or other third parties in connection with any such processes; and

  - whether and how their cybersecurity threat assessment, identification and management processes have been integrated into their overall risk management system or processes.

- Item 106(b)(2) requires registrants to disclose whether and how any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected (or are reasonably likely to materially affect) the registrant, including its business strategy, results of operations, or financial condition.

- Item 106(c)(1) requires a description on Form 10-K of the board of directors' oversight of risks from cybersecurity threats.

- Item 106(c)(2) requires a description on Form 10-K of management's role and expertise in assessing and managing the registrant's material risks from cybersecurity threats. Specifically, registrants should consider disclosing:

  - whether and which management positions or committees are responsible for assessing and managing such risks, including the relevant expertise of such persons;

  - the process by which such persons or committees are informed about an monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and

  - whether such persons or committees report information about such risks to the Board or a committee or subcommittee of the Board.

The SEC also added new requirements to Forms 20-F and 6-K that require foreign private issuers to provide disclosure that substantially mirrors the new disclosure requirements discussed above.

Consistent with the SEC's push to modernize registrants' disclosure, all disclosure required under the new rules must be tagged using Inline XBRL beginning one year after initial compliance with the related disclosure requirement.

The new rules will become effective 30 days after publication in the Federal Register.

- The annual disclosure requirements will be due beginning with annual reports for fiscal years ending on or after December 15, 2023.
- Compliance with the incident disclosure requirements on Form 8-K and Form 6-K commences beginning on the later of 90 days after publication in the Federal Register or December 18, 2023.
- Smaller Reporting Companies must comply with the incident disclosure requirements beginning on the later of 270 days after publication in the Federal Register or June 15, 2024.

Action Items for Registrants

- Establish an incident response plan to (1) identify potential cybersecurity incidents, (2) contain, remediate and respond to incidents, (3) quickly assess the materiality of such incidents (both individually and in the aggregate) and (4) disclose material incidents on Form 8-K in a timely manner.
    - Update incident response plans and conduct mock tabletop breach exercises.
- Develop and implement a comprehensive cybersecurity program and draft required disclosures for inclusion in the next annual report on Form 10-K.
    - Review current disclosure controls and procedures related to cybersecurity.
- Ensure that the Board's risk management program encompasses cybersecurity issues.

National Law Review, Volume XIII, Number 213