STINSON

News & Insights

SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

Alert
07.27.2023

On July 26, 2023, the Securities and Exchange Commission (SEC) adopted final rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose, on an annual basis, material information regarding their cybersecurity risk management, strategy, and governance.

Form 8-K Item 1.05 - Material Cybersecurity Incidents

Required Disclosure

The rules create a new Item 1.05 of Form 8-K, which provides that if a registrant experiences a cybersecurity incident that is determined by the registrant to be material, the registrant must describe the material aspects of the nature, scope and timing of the incident. The registrant must also describe the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.

A "cybersecurity incident" is defined to mean 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. "Information systems" is defined to mean 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.

The required information must be provided in an Interactive Data File in accordance with Rule 405 of Regulation S-T and the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) Filer Manual.

A report pursuant to Item 1.05 must be filed within four business days after the registrant determines that it has experienced a material cybersecurity incident. A registrant's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident. The disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing.

To the extent that the information called for in Item 1.05 is not determined or is unavailable at the time of the required filing, the registrant must include a statement to that effect in the filing. The registrant then must file an amendment to its Form 8-K filing under Item 1.05 containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available.

A registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as to avoid impeding the registrant's response or remediation of the incident.

Materiality Assessment

The SEC declined to provide additional guidance regarding the application of a materiality determination to cybersecurity and declined to replace materiality with a significance standard. The SEC expects that registrants will apply materiality considerations as would be applied regarding any other risk or event that a registrant faces. According to the SEC, carving out a cybersecurity-specific materiality definition would mark a significant departure from current practice, and would not be consistent with the intent of the final rules. Accordingly, the SEC reiterated, consistent with the standard set out in the cases addressing materiality in the securities laws, that information is 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." Because materiality's focus on the total mix of information is from the perspective of a reasonable investor, companies assessing the materiality of cybersecurity incidents, risks and related issues should do so through the lens of the reasonable investor. The evaluation should take into consideration all relevant facts and circumstances, which may involve consideration of both quantitative and qualitative factors. Thus, for example, when a registrant experiences a data breach, it should consider both the immediate fallout and any longer term effects on its operations, finances, brand perception, customer relationships, and so on, as part of its materiality analysis. The SEC also noted that, given the fact-specific nature of the materiality determination, the same

incident that affects multiple registrants may not become reportable at the same time, and it may be reportable for some registrants but not others.

Form 10-K, Item 1C

The rules also created a new Item 106 in Regulation S-K. It will be mandatory for registrants to disclose the information required by Item 106 in Form 10-K under a new Item 1C Cybersecurity. The information required by this Item must be disclosed in an Interactive Data File in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual. The required information includes:

Risk Management and Strategy

A description of the registrant's processes, if any, for assessing, identifying and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

- Whether and how any such processes have been integrated into the registrant's overall risk management system or processes.
- Whether the registrant engages assessors, consultants, auditors or other third parties in connection with any such processes.
- Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

Registrants must also describe whether 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 and if so, how.

A "cybersecurity threat" is defined to mean 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.

Governance

Registrants are also required to describe the board of directors' oversight of risks from cybersecurity threats. If applicable, the registrant must identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.

SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

Management's role in assessing and managing the registrant's material risks from cybersecurity threats must also be disclosed. In providing such disclosure, a registrant should address, as applicable, the following nonexclusive list of disclosure items:

- Whether and which 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, detection, mitigation, and remediation of cybersecurity incidents.
- Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Board of Directors' Cybersecurity Expertise

The SEC declined to adopt disclosures regarding cybersecurity expertise of directors in the final rules.

S-3 Eligibility

General Instruction I.A.3.(b) of Form S-3 was amended so that the untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility.

Implementation Deadlines

The final rules will become effective 30 days following publication of the adopting release in the *Federal Register*. With respect to Regulation S-K Item 106, all registrants must provide such disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. With respect to compliance with the incident disclosure requirements in Form 8-K Item 1.05, all registrants other than smaller reporting companies must begin complying on the later of 90 days after the date of publication in the *Federal Register* or December 18, 2023. Smaller reporting companies will have an additional 180 days and 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. With respect to compliance with the structured data requirements, all registrants must tag disclosures required under the final rules in Inline eXtensible Business Reporting Language (XBRL) beginning one year after initial compliance with the related disclosure requirement.

See a copy of the final rules.

RELATED CAPABILITIES

Corporate Finance

Cybersecurity & Data Privacy