Insights: Alert

SEC Issues Final Rule on Cybersecurity Incident Reporting and Cybersecurity Risk Management Disclosure

August 8, 2023

Written by **Eric S. Kracov** and **David M. Eaton**

The Securities and Exchange Commission (the "SEC") issued a final rule on July 26, 2023 that will require public companies to disclose material cybersecurity incidents on Form 8-K within four business days of discovery. In addition, the SEC will now require public companies to disclose on an annual basis in Form 10-K their process for assessing, identifying and managing material risks from cybersecurity threats, as well as information on how companies' boards and officers govern cyber risk management.

The incident reporting requirements become effective for companies, other than smaller reporting companies, on December 18, 2023. Smaller reporting companies will not be subject to the rule until June 15, 2024. All reporting companies will be subject to the disclosure rules covering their cybersecurity risk management process in annual reports for fiscal years ending on or after December 15, 2023.

We provide the historical context for the new rules below, followed by our summary of them.

Background

The final rules follow over a decade of development of the agency's position on disclosure of data breaches or similar incidents. The SEC first proposed formal rules relating to disclosure of cybersecurity incidents and related risk management processes in March 2022 after providing interpretive guidance in prior years. The agency has also engaged in significant enforcement activity involving companies that failed to disclose, delayed disclosure of, or provided inadequate disclosure concerning, a cybersecurity incident.

The new disclosure rules reflect the SEC's belief that cybersecurity incidents are continuing to grow in both number and severity and that prior guidance was insufficient to ensure that investors were made aware of such incidents on a timely basis and with sufficient detail to understand the company's incident response. Moreover, the agency concluded that, in light of the growing dependence of the economy on the security of electronic systems and the increasing cost of maintaining an adequate defense against cybersecurity incidents, investors needed robust disclosure of the risk management framework for cybersecurity, board oversight of risk from cybersecurity threats, and management's role in assessing and managing such risks.

Definitions

For purposes of both the new Form 8-K requirements and the required annual risk management disclosure, a "cybersecurity incident" is defined as "an unauthorized occurrence, or a series of unauthorized occurrences, on

or conducted through the registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein." The rules also define a "cybersecurity threat" as any potential occurrence that could result in a cybersecurity incident. The rules cover all "information systems" which is defined to include electronic information resources owned or used by the registrant that are used to collect, process, maintain, use, share, disseminate, or dispose of information used to maintain or support the registrant's operations.

Cybersecurity Incident Reporting on Form 8-K

The new rule adds item 1.05 to Form 8-K covering "material cybersecurity incidents." When the rules become effective, public companies will have to disclose information relating to a material cybersecurity incident four business days after they determine they have experienced one. The disclosure must include the following information: (i) a description of the material aspects of the nature, scope, and timing of the incident and (ii) an assessment of the material impact or reasonably likely material impact of the incident on the company, including the financial impact and the impact on operations. However, companies 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 would impede the registrant's response or remediation of the incident." The adopting SEC release notes that, in assessing the impact of the incident, companies should consider qualitative factors (impact on reputation, actual or potential litigation or regulatory investigations, or competitiveness) as well as quantitative factors.

The determination of materiality relies on the standard securities law formulation that considers whether there is a substantial likelihood that a shareholder would consider the information important in making an investment or whether the information would significantly alter the "total mix" of information available about the company. The determination must be made "without unreasonable delay" following discovery of the incident and the filing must indicate if any required disclosure has not been determined or is not available at the time of the filing. That said, the SEC advises that while the determination "need not be rushed prematurely, it also cannot be unreasonably delayed in an effort to avoid timely disclosure." Significantly, the release notes that the fact that the full extent of the incident is not yet known or that further investigation will be necessary "should not delay the company from determining materiality." Examples of unreasonable delay include delay in scheduling a board committee meeting to determine materiality or revision of internal policy to extend assessment deadlines or to change the criteria used to determine incident reporting to management or the board.

The rules include a reminder that companies have a continuing obligation to provide updated and/or corrected disclosure on a cybersecurity incident by means of an amended Form 8-K filing. The amended filing would provide any required information that was not determined or was unavailable at the time of the initial filing. The new rules do not, however, require an update on the remediation status of an event.

A failure to report a material cybersecurity incident on a timely basis does not result in a loss of Form S-3 eligibility. In addition, untimely filing of a Form 8-K reporting a cybersecurity incident will not itself be deemed a Rule 10b-5 violation (however, this limited safe harbor does not shield the company or insiders from liability if they are under a "disclose or abstain from trading" obligation under insider trading laws). Separately, the SEC declined to treat the new Form 8-K filing as furnished rather than filed. They also rejected a safe harbor for a company's attempt to make materiality determinations "without unreasonable delay" after discovery, opining that adherence "to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance."

The rule identifies two circumstances in which a disclosure delay is permissible. First, the Form 8-K filing may be delayed if disclosure would pose a substantial risk to national security or public safety. The delay is permissible if the U.S. Attorney General has notified the SEC that a substantial risk exists, in which case a delay of up to 30 days is permissible with additional extensions possible if the substantial risk continues to exist. Second, for a company subject to the breach disclosure rules of the Federal Communications Commission relating to customer proprietary network information, disclosure may be delayed if the company notifies the SEC no later than the day disclosure would otherwise be required under the SEC rules.

Disclosure of Cybersecurity Risk Management, Strategy, and Governance in Form 10-K

The SEC also adopted new Item 106 to Regulation S-K that will require a reporting company to provide disclosure in their annual report that identifies "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." This formulation represents a revision of the rule included in the March 9, 2022 proposed regulations which would have required a more granular discussion of a company's cybersecurity risk management structure. The agency agreed with commenters who argued that a more detailed level of disclosure went beyond the level that is material to investors and could increase vulnerability to an attack by revealing important operational details of the risk management process.

The final rule also focuses on a non-exclusive list of three areas of disclosure that will help investors to place the disclosed cybersecurity processes in context:

- Whether and how the cybersecurity processes have been integrated into the registrant's overall risk management system or process;
- Whether the registrant engages consultants, auditors or other third parties in connection with their cybersecurity processes; and
- Whether the registrant has a process to identify material risks from cybersecurity threats associated with the use of third-party service providers.

Separately, the new rules will require disclosure about the board's oversight of the company's cybersecurity risk. Specifically, the disclosure must include information on how the board manages the oversight process, i.e., through a board committee or subcommittee, and the process whereby the board or board committee is informed about such risks. The agency dropped language in the proposed regulations that would have required disclosure of board level cybersecurity expertise.

The disclosure must also identify management's role in assessing and managing material risks from cybersecurity threats with a focus on three areas:

- Identification of the management positions and committee that are responsible for assessing and managing cybersecurity risks and the relevant expertise of such persons or committee members;
- The process by which such persons are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- How such persons report information about cybersecurity risk to the board and/or the appropriate board committee.

Foreign Private Issuers; XBRL

Foreign private issuers will be subject to similar, although more streamlined, rules for annual reports on Form 20-F and current reports on Form 6-K.

In addition, beginning a year after the initial applicable compliance date, cybersecurity disclosures in both annual and current reports must also appear in interactive data files.

Next Steps

While we expect virtually all companies have engaged in advanced planning around cybersecurity incidents, that planning may not adequately integrate the SEC's new external disclosure requirements. Consequently, you should consider the following next steps:

- Begin the process of reviewing and, as necessary, updating board and management processes to ensure that required disclosures reflect a robust approach to cybersecurity threats and incident risk management. The review should consider whether the company's chief cyber risk and security managers—including the chief information officer or chief information security officer, as applicable—regularly report on cyber risk to the board or an appropriate board committee. Companies should also give due consideration to peer and industry practice.
- The company's disclosure controls and procedures should be revisited to make sure the company cyber risk and security processes and personnel are an integrated part of them. The disclosure controls and procedures must be designed to provide reasonable assurance that information on a cybersecurity threat or incident flows to senior management and the board in a timely fashion.
- In particular, the company's disclosure controls and procedures should be designed to meet the four-business day disclosure deadline once a material cybersecurity incident has occurred and that all relevant parties—including specifically the company's cyber risk and security managers—have an understanding of what “materiality” means in the context of a cybersecurity incident. This system should be an integral part of the company's incident response plan or other playbooks or checklists for cybersecurity incidents.
- Remember that the new rules also apply to incidents involving third-party vendors that hold or otherwise maintain the company's information in their system. Vendor risk management processes should be reviewed to ensure their adequacy vis-a-vis cybersecurity.
- Take a practice run at how the company will disclose cybersecurity risk management, strategy, and governance. The disclosure will need to provide investors with a reasonable understanding of these areas without revealing information that could be useful to bad actors, and the new disclosure should be consistent with the company's prior disclosures in this area. Remember that you will need to collect biographical information from your key cyber risk managers regarding their expertise in this area.

If you have any questions regarding this alert, please reach out to your Kilpatrick Townsend contact.

Related People

Eric S. Kracov

t 212.775.8732

ekracov@ktslaw.com

David M. Eaton

t 415.273.4324

deaton@ktslaw.com