Updates
August 08, 2023
It’s Official: Cybersecurity Disclosure Is Coming This Year

The U.S. Securities and Exchange Commission (SEC) adopted final rules on July 26, 2023, requiring public companies to provide current disclosure, within what may be a short time window, about material cybersecurity incidents and to include disclosure relating to cybersecurity risk management, strategy, and governance in annual reports.

According to the SEC, these rules are designed to enhance and standardize disclosures regarding cybersecurity risk management, strategy, and incidents, which in the SEC's view have been inconsistent (and in some cases deficient) since the SEC first published guidance in this area back in 2011. The final rules are based on a rule proposal published by the SEC more than one year ago in March 2022 and do scale back some of the previously proposed disclosure requirements.

The final rules affect both domestic and foreign issuers and create disclosure requirements on Forms 8-K and 10-K and Forms 6-K and 20-F, respectively.

New Form 8-K Disclosure Requirements

The final rules require registrants to disclose, via a current report on Form 8-K under new Item 1.05, any cybersecurity incident that is determined by the registrant to be material. The SEC defines a "cybersecurity incident" as "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." The SEC clarifies that this includes cybersecurity incidents affecting a registrant's data that is housed on a third-party service provider's system, such as data stored on a third-party cloud service. This disclosure will be "filed" with the SEC, not "furnished." Any required Form 8-K must be filed within four business days after the company determines that the incident was material.

Materiality Determinations Must Be Made Without Unreasonable Delay

The nature and timing of materiality determinations are important areas of focus. The materiality threshold for cybersecurity incidents will be consistent with the standard analysis in securities law: information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" to investment decision-making. In the cybersecurity context, a materiality assessment may take into account factors such as impact on operations and financial condition; reputational harm; effect on competitiveness or relationships with customers and vendors; potential litigation or regulatory action; and loss of data, assets, or intellectual property.

Critically, the new rule requires registrants to make materiality determinations "without unreasonable delay" after discovery of the incident. The SEC acknowledges that "in the majority of cases, the registrant will likely be unable to determine materiality the same day the incident is discovered" and requires registrants to develop information relevant to materiality without unreasonable delay. The final rules provide a few examples of what would or would not be considered unreasonable delay. For example, the SEC states in the final rules that "a company being unable to determine the full extent of an incident because of the nature of the incident or the company's systems, or otherwise the need for continued investigation regarding the incident, should not delay the company from determining materiality." Additionally, the SEC states that if the materiality determination is to be made by a board committee, the committee may not intentionally delay meeting to make a materiality determination past the normal time it takes to convene a meeting of its members. A company also may not revise existing incident response policies or procedures "in order to support a delayed materiality determination for or delayed disclosure of an ongoing cybersecurity event."

Disclosure Requirements

The required Form 8-K disclosure must include material aspects of the nature, scope, and timing of the incident, as well as the impact or reasonably likely impact of the incident on the registrant, including on its financial condition and results of operations. Companies should take into consideration both quantitative and qualitative factors when disclosing. Harm to a company's reputation, consequences to customer and vendor relationships, or effects on the company's competitiveness are examples of factors companies must consider when drafting disclosure. The final rules explicitly state the disclosure should focus on the impacts of the incident as opposed to providing details regarding the incident itself. A registrant will not have to disclose, for example, the vulnerability that an attack exploited or the steps that the registrant is taking to respond to or remediate the cybersecurity incident.

Any required information about a previously disclosed cybersecurity incident that was not determined or was unavailable at the time of the original Form 8-K filing that later comes to light must be provided via an amendment to the prior-filed Form 8-K. The Form 8-K/A must be filed within four business days after the registrant determines such information or such information becomes available. For example, if the company develops reportable information after its initial filing, such as if its investigation reveals that additional systems were compromised or that the cost of remediation will be substantially greater than initially expected, it must file an amended Form 8-K within four business days after such determination. This requirement to file an amendment to a Form 8-K replaces the proposed requirement to report any "material changes, additions, or updates" to previously filed Form 8-K disclosure in a Form 10-Q or Form 10-K for the period in which the update occurred.

Limited Delay for National Security or Public Safety Reasons

The final rules provide for a delay in the within-four-business-days disclosure requirement if the U.S. attorney general makes a determination that such disclosure would pose a threat to national security or public safety and notifies the SEC of such determination in writing. The attorney general's determination must specify the length

of time for which delay in disclosure should be permitted, up to 30 days. The disclosure delay may be extended for an additional 30 days if the attorney general determines disclosure continues to pose a threat to national security or public safety and again notifies the SEC of such determination in writing. After that, the disclosure delay may be extended by the attorney general for up to an additional 60 days in "extraordinary circumstances" for national security (but not public safety) concerns. These determinations by the attorney general will likely be rare.

Key Differences From Proposed Rule

The final rules differ from the proposed rules in some ways, including the following:

- The SEC is not requiring disclosure about the remediation status of the incident.
- There is no absolute requirement to state whether remediation is ongoing and whether any data was compromised; these only need to be disclosed if required under the registrant's materiality analysis.
- An instruction has been added to Item 1.05 to clarify that 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 would impede the registrant's response or remediation of the incident."
- The requirement that companies disclose cybersecurity incidents "without unreasonable delay" is a change from the proposed rules, which would have required disclosure "as soon as reasonably practicable."

Timing of Implementation

The new Form 8-K disclosure requirements take effect on December 18, 2023. Companies can take some comfort in the fact that this Form 8-K Item 1.05 has been added to the safe harbor list of Form 8-K items for which a late filing will not affect Form S-3 eligibility. Additionally, Item 1.05 will be included in the list of Form 8-K items eligible for a limited safe harbor under the anti-fraud provisions of the Securities Exchange Act of 1934, as amended (Exchange Act), meaning that no failure to file a report on Form 8-K required by Item 1.05 will be deemed to be a violation of Section 10(b) of the Exchange Act or Rule 10b-5 thereunder.

New Form 10-K Disclosure Requirements

Annual Reports on Form 10-K will also be required to include new cybersecurity disclosure under Item 106 of Regulation S-K. New Item 106 will require the following disclosures:

- **Cybersecurity risk management.** A description of the registrant's processes, if any, to assess, identify, and manage material risks arising from the threat of cybersecurity incidents, addressing "whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand [the registrant's] cybersecurity processes," including the following nonexclusive list of matters: (1) "[w]hether and how the described cybersecurity processes have been integrated into the registrant's overall risk management system or processes"; (2) "[w]hether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes"; and (3) "[w]hether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider."
- **Impact of cybersecurity threats and incidents.** A description of "[w]hether 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."
- **Board's role in oversight of cybersecurity risk.** A description of the board's oversight of risks from cybersecurity threats, identifying the board committee(s) or subcommittee(s) responsible for such

oversight, if any, and disclosing the processes by which the board, committee, or subcommittee is informed about any such risks.
- **Management's role in cybersecurity risk management.** A description of management's role in assessing and managing the registrant's material risks from cybersecurity threats, addressing the following nonexclusive list of matters: (1) "[w]hether 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;" (2) "[t]he processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents"; and (3) "[w]hether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors."

In a welcome departure from the proposed rules, the final rules do not require proxy statement disclosure of whether a member of the registrant's board of directors has cybersecurity expertise.

The disclosure requirements under Regulation S-K Item 106 must be included in any annual report on Form 10-K covering a fiscal year ending on or after December 15, 2023. This means calendar-year companies will have to include this information in their Form 10-K filings covering fiscal year 2023.

Foreign Private Issuers

The final rules require similar disclosures by foreign private issuers (FPIs). Like domestic issuers, FPIs must now furnish on Form 6-K any information about a material cybersecurity incident that the FPI disclosed or otherwise publicized in any foreign jurisdiction, to any stock exchange, or to securityholders. Also, similar to domestic issuers, FPIs are required to disclose in their Form 20-F their boards of directors' role in oversight of risks related to cybersecurity threats as well as management's role in assessing and managing any material risks arising from cybersecurity threats.

The SEC explicitly did not adopt cybersecurity disclosure requirements for Form 40-F filers, reasoning that "such filers are already subject to the Canadian Securities Administrators' 2017 guidance on the disclosure of cybersecurity risks and incidents."

Smaller Reporting Companies

The SEC declined to exempt smaller reporting companies (SRCs) from the final rules and instead gave SRCs a 180-day break in the effective date for compliance with the Form 8-K disclosure required under new Item 1.05, with the SRC compliance requirement effective June 15, 2024. However, SRCs are required to comply with the Form 10-K disclosure requirements for any filing covering a fiscal year ending on or after December 15, 2023, just like all other registrants.

iXBRL Tagging Requirements

All companies will be required to meet iXBRL tagging requirements for all disclosure under the new rules, albeit with a compliance deadline of one year after the applicable disclosure requirement compliance deadline, so likely at some point in December 2024.

Enforcement and Other Considerations

Two commissioners voted against adopting the final rules. The dissenting commissioners raised concerns regarding their application and the SEC's authority to promulgate such rules in the first instance. Commissioner

Hester M. Peirce, for example, disagreed that the safeguards outlined above are appropriate to protect victims of cybersecurity incidents; in particular, she opined that the national security or public safety exception is impractical and will be a difficult barrier for registrants to overcome as they navigate incident response. She explained further that the disclosure requirements prescribed in the final rules (e.g., the nature, scope, and timing of the incident) reject financial materiality as the touchstone for disclosure, going beyond the SEC's authority, and may even inform hackers' ransom demands. Commissioner Mark T. Uyeda expressed similar sentiments. While the final rules shed light on registrants' cybersecurity disclosure and reporting requirements, there appears to be uncertainty around the feasibility of the final rules and their enforceability. This uncertainty, especially as it relates to the SEC's authority, may form the basis for litigation as the final rules are implemented and enforced.

It is clear, however, based on prior enforcement actions that the SEC will continue to prioritize cybersecurity disclosures as part of its enforcement agenda. Enforcement actions like *First American* and, most recently, *Blackbaud*, demonstrate the importance of registrants' materiality assessment, as the SEC emphasized the need for an internal reporting structure that allows cybersecurity-related information to make its way to management responsible for disclosures. The SEC continues to emphasize that investors receive transparent material information regarding who knew what, when they knew, what they found out, and what they understood the scope of the incident to be. The final rules formalize concerns raised in those enforcement actions, indicating that the SEC will likely continue to focus on how registrants determine what to disclose when a cybersecurity incident occurs.

Practical Tips: What Should Companies Do Now To Prepare

Although implementation of the final rules is a few months off yet, companies should begin considering the impending new disclosure requirements. Here are some ways to prepare:

1. Review and update company disclosure controls and procedures to ensure information regarding possible material cyber incidents are timely reported to those in charge of making disclosure decisions.
2. Evaluate the board's oversight structure and consider whether oversight of cybersecurity risks should be assigned to a committee if it is not already. Also, keep in mind that any such changes should be disclosed in upcoming proxy statement disclosure.
3. Review and update as necessary the company's cybersecurity risk management processes, including at both the board and management levels.
4. Consider developing a materiality matrix to assist in determining whether a cybersecurity incident is material.
5. Prepare a draft of the new Form 10-K disclosure well in advance of the Form 10-K filing deadline.

Additional guidance on implementing the new SEC rule will be posted on Perkins Coie's *Perkins on Privacy* and *Public Chatter* blogs.

Authors

Explore more in

Corporate Governance Privacy & Security White Collar & Investigations Data Security Counseling and Breach Response

Related insights

Update

2022 Breach Notification Law Update: State and Federal Requirements Continue To Evolve

Update

SEC Proposes New Cybersecurity Disclosure Rules on Incident Reporting, Risk Management, Strategy, and Governance