No. 2023-08
27 July 2023

To the Point

SEC – final rule

SEC adopts disclosure requirements for cybersecurity incidents and risk management and governance

The rules are intended to enhance and standardize registrants' disclosures related to cybersecurity risk management, strategy and governance.

What you need to know

- The SEC adopted rules requiring registrants to disclose information about a material cybersecurity incident on Form 8-K within four business days of determining that the incident is material, with a delay only when the US Attorney General concludes that disclosure would pose a substantial risk to national security or public safety.
- The rules require registrants to describe the processes they use to assess, identify and manage cybersecurity risks, as well as the board's oversight of such risks and management's role in assessing and managing such risks.
- The rules apply to nearly all registrants that file periodic reports with the SEC, including smaller reporting companies and foreign private issuers.
- Calendar-year registrants must provide the risk management, strategy and governance disclosures in their 2023 annual reports. Most registrants must comply with the incident disclosure requirements on the later of 90 days after publication in the Federal Register or 18 December 2023.

Overview

The Securities and Exchange Commission (SEC or Commission) **adopted** rules to enhance and standardize disclosures by requiring registrants to timely report on cybersecurity incidents on Forms 8-K and 6-K and make disclosures about their cybersecurity risk management, strategy and governance in annual reports on Forms 10-K and 20-F.

The SEC said the rules are intended to make sure that registrants disclose material cybersecurity information and provide investors with more consistent, comparable and decision-useful information.

The rules codify many of the concepts in the interpretive guidance on cybersecurity that the SEC issued in 2018 (the 2018 Interpretive Release[1]) and in the Division of Corporation Finance's 2011 staff guidance[2] on cybersecurity disclosures. However, the rules require more prescriptive disclosures about cybersecurity incidents and risk governance.

The rules apply to nearly all registrants that are required to file periodic reports (e.g., Form 10-K, Form 20-F) with the SEC, including smaller reporting companies (SRCs) and foreign private issuers (FPIs).[3]

Key considerations

Incident disclosures

Form 8-K reporting requirements

The rules amend Form 8-K to add Item 1.05, which requires registrants to disclose a material cybersecurity incident within four business days of determining that the incident is material. Companies must make their materiality determinations without unreasonable delay, but the rules do not establish any bright lines or deadlines. FPIs are required to provide comparable disclosures on Form 6-K.

Item 1.05 requires registrants to disclose a material incident on Form 8-K and describe material aspects, including the nature, scope and timing of the incident, and the impact or reasonably likely impact on the registrant's financial condition and results of operations. In response to feedback on the proposal, the final rule requires the incident disclosures to primarily focus on the material impacts of the incident rather than details about the incident itself.

If any required information is not determined or is unavailable at the time the registrant prepares the initial Form 8-K, the registrant must file an amended Form 8-K containing such information within four business days after it determines such information or the information becomes available.

The SEC decided not to require registrants to report incidents that are individually immaterial but are material in the aggregate, as it had proposed, based on feedback that such a provision would have been challenging to implement. However, the rule expands the definition of "cybersecurity incident" to include "a series of related unauthorized occurrences," which reflects the fact that cyber attacks sometimes occur over time. The rule says that the Form 8-K requirement could be triggered even if the material impact to the registrant is caused by a series of individually immaterial related cyber attacks.

How we see it

Companies may find the requirement to report "a series of related unauthorized occurrences" challenging because the rule does not define "related." For example, registrants may need to develop a process to track individually immaterial related incidents over an undefined time period and identify controls over that process to make sure they are reporting all cybersecurity incidents subject to the rule.

The rule states that what constitutes materiality for purposes of determining whether an incident must be reported in a Form 8-K is consistent with the Supreme Court's definition of materiality, and registrants need to thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances of the cybersecurity incident, including quantitative and qualitative factors.

The rule also affirms that a registrant is not expected to publicly disclose detailed technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities that would impede its response or remediation of the incident.

A registrant may delay reporting a cyber incident on Form 8-K if the US Attorney General determines that the disclosure poses a substantial risk to national security or public safety and notifies the Commission of such determination in writing prior to the Form 8-K deadline.[4]

How we see it

In its 2018 Interpretive Release, the SEC said registrants had an obligation to use Form 8-K to disclose information about material incidents. Although the final rules formalize the timing and specify the content and location of cybersecurity incident disclosure, the use of materiality as the threshold for providing disclosure about cyber incidents is not changing.

Materiality assessments in the context of cybersecurity incidents are often complex, and registrants of all sizes may struggle to perform them. Many companies have followed the SEC's recommendation to establish disclosure committees that consider the materiality of information, and they could be involved in these assessments.

A registrant is not expected to publicly disclose detailed technical information about its planned response to the incident or its cybersecurity systems that would impede its response or remediation of the incident.

Risk management, strategy and governance disclosures

The rules also add Item 106 to Regulation S-K, and Item 16K to Form 20-F, to require registrants to disclose their cybersecurity risk management, strategy and governance.

Risk management and strategy

The rules require registrants to disclose their processes, if any, to assess, identify and manage risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. For example, a registrant is required to disclose whether and how any such processes have been integrated into its overall risk management system or processes.

A registrant is also required to disclose whether it uses assessors, consultants, auditors or other third parties in connection with such processes, and whether it has processes in place to oversee and identify risks related to its use of third-party service providers.

A registrant must also disclose 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 its business strategy, results of operations or financial condition and if so, how.

Governance

The rules require registrants to disclose the board's role in overseeing risks from cybersecurity threats. Registrants are required to identify any board committee or subcommittee that oversees cybersecurity risks, if applicable, and describe the processes by which the committee is informed about such risks.

The rule requires disclosures about management's role in assessing and managing material risks from cybersecurity threats, including whether certain management positions or committees are responsible for assessing and managing cybersecurity risk and their relevant expertise. Registrants must also disclose the processes by which management is informed about and monitors the prevention, detection, mitigation and remediation of cybersecurity incidents, including whether management reports information about such risks to the board.

The SEC did not adopt the proposed requirement to disclose board members' cybersecurity expertise. The adopting release states that effective cybersecurity processes are designed and administered at the management level, and the board can effectively oversee management's efforts without specific subject-matter expertise.

How we see it

Registrants may need to identify and disclose in their annual reports management's relevant expertise to assess and manage material risk from cybersecurity threats.

Transition period

All domestic registrants must provide Regulation S-K Item 106 disclosures, and FPIs must comply with the comparable requirements in Form 20-F beginning with annual reports for fiscal years ending on or after 15 December 2023.

All registrants other than SRCs are required to disclose a material cybersecurity incident on Form 8-K within four business days of determining that a cybersecurity incident is material on the later of 90 days after publication in the Federal Register or 18 December 2023. SRCs must begin complying with Form 8-K disclosure requirements on 15 June 2024.

Endnotes:

1 ***Commission Statement and Guidance on Public Company Cybersecurity Disclosures***, 26 February 2018.

2 ***CF Disclosure Guidance: Topic No. 2: Cybersecurity***, 13 October 2011.

3 The rule did not amend Form 40-F, and therefore, it doesn't apply to Canadian FPIs under the multijurisdictional disclosure system.

4 The delay provision for substantial risk to national security or public safety is separate from Exchange Act Rule 0-6, which provides for the omission of information that has been classified by an appropriate department or agency of the federal government for the protection of the interest of national defense or foreign policy. If the information a registrant would otherwise disclose on an Item 1.05 of Form 8-K or pursuant to Item 106 of Regulation S-K or Item 16K of Form 20-F is classified, the registrant should comply with Exchange Act Rule 0-6.