NOW & NEXT

Securities Alert

AUGUST 10, 2023

SEC adopts Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rules

By Lloyd Spencer and Andrew Pearce

New SEC final rules expand reporting obligations for cybersecurity.

What's the Impact

- The new rules require a public company to file a Form 8-K within four business days after it determines that is has experienced a material "cybersecurity incident."
- The new rules require annual disclosure regarding a company's risk management and strategy relating to cybersecurity threats and the oversight of such risk management and strategy.
- Companies should begin evaluating the role that their information security professionals, compliance professionals, and management will have with respect to the new rules.
- All companies, except smaller reporting companies, must begin complying by September 5, 2023.

On July 26, 2023, the US Securities and Exchange Commission (the SEC) adopted final rules requiring US public companies to disclose material cybersecurity incidents on Form 8-K and, on an annual basis, disclose material information regarding their cybersecurity risk management,

strategy, and governance on Form 10-K. The final rules also require foreign private issuers to make comparable disclosures on Forms 6-K and 20-F.

The SEC indicated that the final rules are intended to result in enhanced, consistent, comparable, and decision-useful disclosures that would allow investors to evaluate public companies' exposure to material cybersecurity risks and incidents and their ability to manage and mitigate those risks.

The rules represent an expansion in the reporting obligations regarding cybersecurity incidents and transparency around public companies' cybersecurity risk management policies and procedures and the oversight role of management and boards of directors in managing companies' cybersecurity risk.

Requirements of Cybersecurity Incident Disclosure Rules

Form 8-K Requirements

The rules add a new Item 1.05 to Form 8-K, which requires a public company to file a Form 8-K within four business days after it determines that is has experienced a material "cybersecurity incident." The trigger for Item 1.05 of Form 8-K is the date on which the company determines that the incident it has experienced is material, and not the date of discovery itself. An instruction to Form 8-K provides that materiality determinations must be made "without unreasonable delay" after discovery of a cybersecurity incident, and the SEC states in the adopting release that "adhering to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance." In addition, the SEC stated that companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident. A company's materiality determination may depend on quantitative factors, qualitative factors such as reputational harm, the possibility of litigation or regulatory investigations or actions, and whether initiated by state, federal, or non-US regulatory or governmental authorities.

The report must describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the company, including its financial condition and results of operations, which may include harm to a company's reputation, customer or vendor relationships, or competitiveness. The instructions to Item 1.05 clarify that a company 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 company's response or remediation of the incident.

Notably, an untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility and is covered by a limited safe harbor for Section 10(b) and Rule 10b-5 liability.

Definition of Cybersecurity Incident

The rules define, which should be construed broadly, 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 rules define the term "information systems" to mean information resources owned or used by the company, resulting in a Form 8-K being triggered not only by an incident involving the company's own systems, but also an incident involving the systems of a third-party service provider (e.g., a cloud service provider). The adopting release emphasizes that the term "cybersecurity incident" extends to a series of related unauthorized occurrences, which means that Item 1.05 may be triggered even if individually, each related incident would not be considered material itself. Also, the SEC noted that an accidental occurrence may be an "unauthorized occurrence" and thereby a cybersecurity incident under the definition even if there is no confirmed malicious activity.

Permitted Delays in Filing Form 8-K

Item 1.05(c) provides that the Form 8-K filing may be delayed if the US 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. In such case, the filing may be delayed for a time specified by the Attorney General, up to 30 days following the date when the disclosure was otherwise required to be provided. This delay may be extended for an additional period of up to 30 days if the Attorney General determines that a disclosure continues to present a substantial risk to national security or public safety and notifies the SEC in writing. In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the SEC of such determination in writing. Beyond this final 60-day delay, if the Attorney General indicates that further delay is necessary, the SEC will consider additional requests for delay and may grant such relief through exemptive orders.

Item 105(d) provides that if a company is subject to the Federal Communications Commission's notification rule for breaches of customer proprietary network information, the company may delay providing the disclosure required by Item 1.05 for such period that is applicable under the notification rule and in no event for more than seven business days after notification required under that provision has been made, so long as the company notifies the SEC in correspondence submitted via the EDGAR system no later than the date when the disclosure required by Item 1.05 was otherwise required to be provided.

Updating Disclosure

If the information regarding such material aspects or material impact (or reasonably likely material impact) was not determined or was unavailable at the time of the initial Item 1.05 Form 8-K filing, a company will be required to amend it to disclose such information within four business days after the company, without unreasonable delay, determines such information, or within four business days after such information becomes available. Companies are reminded, however, that they have a duty to correct prior disclosures they later determine are (i) untrue or

(ii) missing a material fact necessary to make the disclosure not misleading at the time the disclosure was made.

Third-Party Service Providers

The rules do not exempt disclosure of cybersecurity incidents on third-party systems used by the company and do not provide a safe harbor for information disclosed relating to third parties. Companies will need to be able to assess whether a cybersecurity incident at a third-party service provider will have a material impact on the company and thereby trigger a Form 8-K filing. This may require companies to enhance their policies and procedures or to consider adding additional provisions to agreements with third-party providers to ensure appropriate oversight of their third-party risk management programs, including reporting mechanisms for cybersecurity incidents. However, in the adopting release, the SEC indicated that the final rules "generally do not require that registrants conduct additional inquiries outside of their regular channels of communication with third-party service providers pursuant to those contracts and in accordance with registrants' disclosure controls and procedures."

XBRL Tagging

The information required by new Item 105 of Form 8-K must be tagged using Inline XBRL.

Cybersecurity Risk Management, Strategy, and Governance Disclosure

Risk Management and Strategy

New Item 106(b) of Regulation S-K requires a company to describe the processes it has, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. Companies are directed to address the following non-exclusive list of items in their disclosure, but are not required to file their cybersecurity policies and procedures:

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

Companies also must describe whether any risks from cybersecurity threats, including because of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition, and if so, how. The disclosures required by new Item 106 will be required in a company's annual report on Form 10-K. In the final rules, the SEC did not allow Item 106(b) disclosure to be provided in the proxy statement and did not require Item 106 disclosures in registration statements but the SEC stated in the adopting release that companies should

consider the materiality of cybersecurity risks and incidents when preparing required disclosures in the registration statement.

Governance

The rules add a new Item 106(c) to Regulation S-K requiring a description of the board and management's oversight of cybersecurity risk.

Under Item 106(c)(1), as adopted, companies should describe the board of directors' oversight of risks from cybersecurity threats, and if applicable, 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.

Item 106(c)(2) requires a description of management's role in assessing and managing the company's material risks from cybersecurity threats. In making this disclosure, the company should consider disclosing the following non-exclusive 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; and
- 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.

These disclosures regarding cybersecurity risk management, strategy, and governance will be required in a company's annual report on Form 10-K.

In the final rules, the SEC did not allow Item 106(c) disclosure to be provided in the proxy statement.

Definition of Cybersecurity Threat

The rules define "cybersecurity threat" 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.

XBRL Tagging

The information required by new Items 106(b) and (c) of Regulation S-K must be tagged using Inline XBRL.

Disclosure by Foreign Private Issuers

Amendments to Forms 20-F establish disclosure requirements for foreign private issuers parallel to those adopted for domestic issuers in Regulation S-K Item 106. Amendments to Form 6-K also parallel those adopted for domestic issuers in Form 8-K Item 1.05, and require foreign private issuers to furnish on Form 6-K information about material cybersecurity incidents that the issuers disclose or otherwise publicize in a foreign jurisdiction to any stock exchange or to security holders.

Compliance Timeline

The final rules will be effective for all companies on September 5, 2023. All companies, except smaller reporting companies, must begin complying with the new incident disclosure requirements of Item 1.05 of Form 8-K on December 18, 2023. Smaller reporting companies have an additional 180 days and must begin complying with Item 1.05 of Form 8-K on June 15, 2024. All companies must provide disclosure under new Item 106 of Regulation S-K beginning with annual reports for fiscal years ending on or after December 15, 2023.

In addition, all companies must tag both real-time and periodic disclosures required under the final rules in Inline XBRL beginning one year after initial compliance with the related disclosure requirement.

What's Next

Companies should begin evaluating the role that their information security professionals, compliance professionals, and management will have with respect to the new rules, specifically regarding the company's risk management, strategy, and governance of its cybersecurity program and ensuring that information regarding cybersecurity incidents is promptly communicated to the persons who can evaluate whether Form 8-K disclosure is required. Additionally, companies should begin focusing on implementing disclosure controls and procedures to comply with those requirements, particularly with respect to making materiality determinations and preparing disclosures regarding cybersecurity incidents. Issuers will also need to consider how their risk management and governance processes will be disclosed and if any revision to those processes is needed.

For additional information on the new rules, see the press release announcing adoption of the final rules and the fact sheet published by the SEC.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Lloyd H. Spencer
202.585.8303
lspencer@nixonpeabody.com

Andrew Pearce
617.345.6019
apearce@nixonpeabody.com