Davis Polk

SEC adopts cybersecurity disclosure mandates for public companies

July 31, 2023 | Client Update | 9-minute read

The final rules require current reporting of cybersecurity incidents and annual risk management disclosure for public companies that are likely to compound compliance costs and enforcement risks.

On July 26, 2023, the Securities and Exchange Commission adopted final rules in a 3-2 vote that mandate cybersecurity incident and risk management disclosures for public companies. While the final rules drop the requirement to identify board-level cybersecurity expertise and pare back the disclosure requirement to aggregate incidents in quarterly reporting, they hew closely in many respects to the agency's rule proposal from a year ago. Domestic public companies will be required to report material cybersecurity incidents within four business days (with limited exceptions), effective as early as December this year, and all public companies will be required to include cybersecurity risk management disclosures in their annual reports beginning with the 2023 Form 10-K or Form 20-F for companies on the calendar year.

The final rules, which come on the heels of recent rule proposals for regulated market participants, are likely to spur additional compliance costs and enforcement risks as the SEC continues to step up its policing of cybersecurity risk management and reporting.

Current reporting of cybersecurity incidents

Since 2011, the SEC has encouraged public companies to file a Form 8-K upon the occurrence of a material cybersecurity incident. The final rules turn the guidance into a mandate for Form 8-K under new Item 1.05.

– **Timing.** A company must report a cybersecurity incident on Form 8-K within four business days after it determines that the incident is material. The materiality determination must be made "without unreasonable delay," a change from the requirement in the proposal to make the determination "as soon as reasonably practicable." The SEC made this change to address concerns that companies would feel the need to disclose before making a materiality determination and to allow companies to take time to properly evaluate the event.

  The release includes examples of what would constitute "unreasonable delay," such as when a company intentionally delays a committee meeting on the materiality determination past the normal time it takes to convene its members, or if a company revises policies and procedures to delay a determination by extending its incident severity assessment deadlines. But the SEC notes that if companies adhere to normal internal practices and disclosure controls and procedures, that will suffice to demonstrate good faith compliance.

  Importantly, the SEC provided that the failure to make a Form 8-K disclosure on time will not impact Form S-3 eligibility.

– **Content.** The final rules require companies to "describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."

  The SEC did not adopt, as proposed, a requirement for disclosure regarding the incident's remediation status, whether

it is ongoing, and whether data was compromised, reflecting comments that this information would cause more harm than benefit.

- **Updates.** If any information a company is required to disclose is not determined or is unavailable at the time of the required filing, the company must identify that information in its original Form 8-K filing and later amend its Form 8-K with that additional information within four business days after it has been determined or becomes available. This new requirement replaces the mandate in the rule proposal for disclosure to be updated in subsequent Forms 10-Q or 10-K.
- **Broader definition of "cybersecurity incident."** While the final rules dropped the proposal to disclose when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate, the SEC instead expanded the already broad definition of "cybersecurity incident" to capture a series of related occurrences that collectively may have a material impact on a company. This would include when a company finds that it has been materially affected by what may appear as a series of related cyber intrusions, each of which may be immaterial.
- **Limited reporting delay for national security and conflict with FCC rule.** The final rules include a limited exception to the four-day reporting requirement if the U.S. Attorney General determines that disclosure poses a "substantial risk to national security or public safety" and notifies the SEC in writing. The exception seems exceedingly impractical, considering the need to obtain a determination from the Attorney General within the tight timeframe. It also only allows for a reprieve of up to 30 days following the date when the disclosure was otherwise required to be provided (though the delay could potentially be extended). In addition, there is no exception where other law enforcement agencies, or foreign agencies, would prefer non-disclosure, although the SEC suggested that other agencies could coordinate with the Attorney General. The final rules also provide that companies subject to a Federal Communications Commission notification rule for breaches of customer proprietary network information may delay making a Form 8-K disclosure for up to seven business days following notification to the relevant agencies under the rule to address potentially conflicting disclosure timelines.

Foreign private issuers already have an obligation to disclose material information on Form 6-K that they disclose offshore, on a stock exchange or to their security holders, and the new rules simply add material cybersecurity incidents to the list of material information included in the form. In practice, this does not change foreign private issuers' disclosure obligation on Form 6-K.

Annual cybersecurity risk management disclosure

Companies will be required to include additional cybersecurity risk management disclosures in Forms 10-K and 20-F, including the following:

- **Processes.** Companies must describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. The discussion should address whether and how they are integrated into overall risk management processes, whether the company engages consultants or other third parties in connection with its 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. For companies that have not done so, the assessment of material risks from third-party service providers should be considered early on in order to evaluate the appropriate disclosure for Form 10-K or 20-F.

  The SEC explains that it substituted the term "processes" in place of the originally proposed "policies and procedures" to avoid requiring the disclosure of operational details "that could be weaponized by threat actors" or suggesting that companies need to formally codify their processes.
- **Board oversight.** Companies must describe the board of directors' oversight of risks from cybersecurity threats, identify any board committee or subcommittee responsible for such oversight, as well as describe the processes by which the board or any such committee is informed about these risks. This disclosure must be in the Form 10-K, not the proxy statement, even if it is otherwise already in the proxy statement. Companies are not required to disclose any particular board expertise in relation to cybersecurity, a change from the rule proposal, or whether the board considers cybersecurity as part of its business strategy, risk management and financial oversight.
- **Role of management.** Instead of board expertise, companies must describe management's cybersecurity expertise and its role in assessing and managing material risks from cybersecurity threats. As part of that disclosure, companies must disclose, to the extent applicable, whether and which management positions or committees are charged with managing cybersecurity risks, the processes by which the relevant 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 these risks to the board or board committees.

The final rules do not include the requirement in the rule proposal to disclose the frequency of management and board discussions on cybersecurity risks.

- **Disclosure of risks from cybersecurity threats.** The final rules also require disclosure of 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." In the adopting release, the SEC asks companies to "consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident."

Potential compliance and enforcement implications

- **Incident response may be more costly and complicated.** Companies will need to quickly determine cybersecurity incident materiality and make disclosures within four business days of the determination—an aggressive timeline, as compared to most other federal and state breach notification laws. Companies will also need to track incident-related required disclosures to include any required updates in amended Form 8-K filings.
- **De facto minimum standards for cybersecurity risk management processes.** Under the guise of disclosure, the SEC is effectively signaling minimum standards for cybersecurity risk management processes by requiring them to be addressed in Forms 10-K and 20-F.
- **Disclosure in ESG reports.** Many companies already disclose cybersecurity risks and board and management oversight in their ESG reports. The SEC is increasingly focused on matters related, directly or indirectly, to ESG disclosures wherever they appear, not just in SEC filings. This means companies should review carefully their cybersecurity disclosures in ESG reports with the same level of care with which they review their SEC filings and ensure those disclosures are accurate, appropriately balanced and consistent with disclosure in their SEC filings.
- **Increased enforcement risk.** The new disclosure requirements come at a time of heightened SEC focus on cybersecurity disclosure enforcement, including actions involving the disclosure of hypothetical cybersecurity risks when actual events had occurred, and disclosure controls and procedures around cybersecurity event reporting. Materiality already was an important part of companies' responses to cybersecurity incidents, but the rule creates a framework for SEC Enforcement to second-guess when a materiality determination was made, whether initial filings were updated sufficiently during the fast-moving context of a cybersecurity incident and whether companies fairly describe their management and governance of cybersecurity risks.

Combined, the final rules and enforcement actions significantly increase the SEC's oversight of public companies' cybersecurity risk management practices and the risk of liability when they suffer breaches, even though they usually will be in the posture of a victim of a sophisticated attack.

Compliance dates

Compliance dates for the final rules are much earlier than is typical for new SEC rules, and will require disclosure in the near-term for all public companies (other than filers under the multijurisdictional disclosure system, or MJDS, to which the new rules do not apply):

- For incident disclosure in Form 8-K or Form 6-K, companies (other than smaller reporting companies) must begin complying on the later of the date that is 90 days after publication of the adopting release in the Federal Register and December 18, 2023. Smaller reporting companies have an additional 180 days to comply with the incident disclosure requirements (though they will be required to comply with the annual disclosure requirements on the same timeline as other companies).
- For annual disclosures on Form 10-K or Form 20-F, companies must provide required disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023 (for calendar-year companies, this means required disclosure begins with the 2023 10-K or 20-F, filed in 2024).
- Companies must tag required disclosures under the final rules in Inline XBRL beginning one year after the initial compliance date for the related disclosure requirement.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Ning Chiu
+1 212 450 4908
ning.chiu@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

Joseph A. Hall
+1 212 450 4565
joseph.hall@davispolk.com

Michael Kaplan
+1 212 450 4111
michael.kaplan@davispolk.com

Alain Kuyumjian
+1 212 450 3628
alain.kuyumjian@davispolk.com

John B. Meade
+1 212 450 4077
john.meade@davispolk.com

Emily Roberts
+1 650 752 2085
emily.roberts@davispolk.com