akerman

Practice Update

SEC Enhancing Disclosure Requirements for Cybersecurity

April 6, 2022
By Douglas B. Paul

Over the last few years, the Securities and Exchange Commission (the "SEC" or "Commission") has issued guidance and proposed rules to enhance existing cybersecurity disclosure requirements, and that trend continues in 2022. The SEC first issued cybersecurity-related guidance in 2011, when the SEC's Division of Corporation Finance described how to disclose cybersecurity risks and incidents, and again in 2018, when the SEC provided interpretive guidance to reinforce and expand the 2011 staff guidance. This year, the Commission has already waded into the cybersecurity rulemaking arena twice in substantial ways.

First, on February 9 the SEC proposed a cybersecurity-related rule, Rule 206(4)-9 to the Investment Advisers Act of 1940, that would impose additional requirements on registered investment advisers related to preventative cyber risk management, reporting and disclosure requirements, and record keeping. For Akerman's insight into this proposed rule, see Akerman's Practice Update "SEC's New Proposed Rules Contain Changes for Investment Advisers of Private Funds" (February 22, 2022).

And second, on March 9 the SEC issued a 129-page cybersecurity-related proposed rule that would require companies to disclose cybersecurity

Related People

Elizabeth F. Hodge
Thomas J. Kearney
Esther L. Moreno
Douglas B. Paul
Christina C. Russo

Related Work

Data Privacy and Security
Litigation
White Collar Crime and Government Investigations

Related Offices

Washington, D.C.

incidents more quickly; update prior disclosures of cybersecurity incidents as needed; periodically describe their risk governance and management strategies; report whether their management or directors have cybersecurity expertise; and provide the proposed disclosures in Inline eXtensible Business Reporting Language ("Inline XBRL"), among other things ("Proposed Rule"). Specifically, in a 3-1 vote along party lines, the Commission proposed that public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 be required to:

- Report "material cybersecurity incidents" on Form 8-K within four business days of determining that an incident is material;
- Update and provide more detail about previously reported cybersecurity incidents on Forms 10-K and 10-Q;
- Disclose the company's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board's oversight of cybersecurity risks on Form 10-K; and
- Disclose whether any board member has cybersecurity expertise in proxy statements and annual reports.

The Proposed Rule is intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. In announcing the Proposed Rule, SEC Chair Gary Gensler said that "companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner." Key elements of the Proposed Rule, and their potential benefits and concerns, are discussed in detail below.

Prompt and Standardized Disclosure of Material Cybersecurity Incidents

Under the Proposed Rule, upon determining that an incident is "material," a public company would have four business days to disclose it in an amended Form 8-K. The Commission said that determining "materiality" for purposes of cybersecurity incident disclosure would be consistent with its previous standards for materiality, and cited to *TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976), *Basic, Inc. v. Levinson*, 485 U.S. 224, 232 (1988), and *Matrixx Initiatives, Inc. v. Siracusano* 563 U.S. 27 (2011). The Proposed Rule provides a non-exclusive list of examples of cybersecurity incidents that may trigger the proposed disclosure requirement if determined to be material by a public company.

A company that makes a determination that an incident is material would have four business days to report the following information to the Commission under new proposed Item 1.05 of Form 8-K:

- when the incident was discovered, and if it is continuing; the scope and nature of the incident;
- if any data was stolen, altered, accessed, or used for an unauthorized purpose;
- the impact on operations; and
- if the company has remediated or is currently remediating the incident.

Current reports on Form 6-K that are required of foreign private issuers instead of Form 8-K would also be amended to add "cybersecurity incidents" as an item that may trigger a Form 6-K. The Proposed Rule would not require companies to disclose specific technical details about any breaches or remediation efforts (which may risk providing hackers with information to use in future cyberattacks), but aims to inform investors about incidents that could negatively impact a business through interruptions, extortion, reputational harm, stock declines, or lost revenue. Additionally, internal or external ongoing investigations (including law

enforcement investigations) into the cybersecurity incident would not be grounds for a company to delay reporting the incident, even if it was otherwise permitted to delay providing public notice under applicable state law. Lastly, it is important to note that failure to timely file a Form 8-K for a cybersecurity incident would not result in a loss of Form S-3 eligibility.

Updated Disclosures of Previous Incidents

Under the Proposed Rule, public companies would also be required under proposed Item 106(d) of Regulation S-K to provide updated disclosures about any previously disclosed cybersecurity incidents in their periodic reports to meet these new requirements, for as long as there are material changes during a given reporting period. The Proposed Rule provides the following examples of the type of updated disclosures that should be provided:

- any material impact of the incident on the company's operations and financial condition;
- any potential material future impacts on the company's operations and financial condition;
- whether the company has remediated or is currently remediating the incident; and
- any changes in the company's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes.

Further, to the extent known to management, the company must also provide disclosure when any series of previously undisclosed incidents has become material in the aggregate. The Commission noted that this requirement to update previous disclosures is a recognition that a company's understanding of a cybersecurity incident will likely evolve over time (e.g., they may gain a better understanding of the scope of the incident, whether customer data was compromised, the impact on

operations, and whether remediation efforts were effective). This proposed requirement for companies to disclose updated information allows investors to stay informed as the company's knowledge of the event evolves.

Cybersecurity Risk Management, Strategy and Governance

In addition to requiring prompt and standardized disclosures about cybersecurity incidents, the Proposed Rule also aims to enhance and standardize public companies' disclosures about cybersecurity risk management, strategy, and governance. In its Proposed Rule, the Commission noted that Division of Corporation Finance staff observed that most companies that disclosed a cybersecurity incident in 2021 did not also describe their risk oversight or any related policies and procedures and may have only provided general disclosures. The Proposed Rule would require companies to provide more detail. Specifically, companies would be required to describe their policies and procedures to identify and manage cybersecurity threats, including whether cybersecurity is a part of its business strategy, financial planning, and capital allocation; and to disclose information in their annual reports and certain proxy filings about the board's oversight of cybersecurity risk. The Proposed Rule provides specific requirements regarding applicable disclosure.

Another important aspect of the Proposed Rule relates to the board's oversight of cybersecurity risk. Proposed Item 106(c) of Regulation S-K would require a discussion, as applicable, of the following:

- whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks;
- the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and

- whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

Proposed Item 106(c) would require companies to disclose management's role and specific expertise in managing that risk, and in implementing the appropriate policies and procedures, including the processes by which the board is informed about cybersecurity risks.

The Commission believes that providing more detail about company's policies, procedures, and strategies for mitigating cyber risks will be useful for investors to make more informed decisions. In addition, companies would be required to provide a description of their board's cybersecurity expertise (e.g., work experience in cybersecurity, including as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations, incident response manager or business continuity planner; or certification or degree in cybersecurity). Of note, the Proposed Rule would require disclosure of the name of any director having cybersecurity expertise and a description of the nature of the expertise.

The Proposed Rule would also amend the annual report on Form 20-F applicable to foreign private issuers to require the same types of disclosure relating to risk management, strategy and governance discussed above.

Potential Benefits of Proposed Rule

As Chairman Gensler stated, the Proposed Rule could have benefits for both companies and investors. For example:

- With this Proposed Rule, companies dealing with the aftermath of a cybersecurity breach would have improved, uniform guidance about what to disclose and how to disclose it.

- By requiring quicker and more uniform responses, companies would understand how to best address cybersecurity incidents, and as a result, investors can trust that material cybersecurity incidents will be disclosed promptly and with important details about how the breach may impact the company.
- The additional focus on disclosing the cybersecurity experience of directors and management's cybersecurity governance may encourage companies to seek out directors and executives with those skills, which could lead to enhanced cybersecurity knowledge and experience at companies. This could offer companies more protection from cybersecurity incidents.
- By requiring the disclosure of a company's board cybersecurity expertise, the SEC may be signaling that it wants companies to have at least one board member who is a cybersecurity expert. This may be similar to the way the Commission encourages an issuer to have at least one "audit committee financial expert" on its audit committee (and if there is not such an expert, the issuer must explain why in its disclosures).

Potential Negatives of Proposed Rule

Despite the good intentions of the new disclosure requirements, companies may find them burdensome and challenging to implement. The Proposed Rule raises many potential issues, including:

- Is it realistic to require companies to comply with a four business day deadline from the determination that a cybersecurity incident is material to then determining how to properly disclose it?
- Is this deadline an arbitrary timeframe that puts the desires of investors to know about cyber incidents ahead of companies' ability to accurately understand and disclose them?

Similarly, could the four business day deadline force companies to rush to make improper materiality determinations?

- Could a company seeking to comply with the rules err on the side of disclosure and unnecessarily disclose a cyber incident that is later determined to be non-material?
- Would the rush to meet the four business day disclosure requirement and the potential for generic and possibly misleading disclosure in the Form 8-K ultimately undermine investors' ability to rely on these disclosures?
- Despite the SEC's comment that it does not expect companies to disclose system vulnerabilities and specific technical responses to cybersecurity incidents, could the four business day disclosure requirement inadvertently encourage other bad actors to attack a company's cybersecurity systems?
- How will companies reconcile the SEC's four business day turnaround with overlapping and possibly conflicting notification requirements to the multiple agencies that can govern cybersecurity breaches, as well as state or local laws that may mandate that customers or other affected persons be notified in the event of a breach?

Conclusion

While the SEC's most recent Proposed Rule continues its efforts to enhance investors' ability to understand the impact of cybersecurity incidents on public companies, it remains to be seen whether companies will be able to comply with this Proposed Rule.

The SEC is likely to receive significant commentary from both companies and the investing public during the rulemaking process. The public comment period is open through May 9, 2022. In the meantime, public companies should take this opportunity to assess how their cybersecurity

policies and procedures align with the reporting requirements of the Proposed Rule and how they can begin to close the gap.

This information is intended to inform firm clients and friends about legal developments, including recent decisions of various courts and administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.