GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity

March 2022

SEC Continues Rolling Out Cybersecurity Rules, this Time Targeting Public Companies

This GT Alert covers the following:

- The SEC issued long-awaited proposed cybersecurity rules and amendments applicable to public reporting companies.
- The rules require public companies to report material cybersecurity incidents on Form 8-K within four business days.
- The rules **do not** contain specific requirements around cybersecurity measures that must be adopted, like risks assessments, vulnerability scans, or adoption of multifactor authentication, opting to keep requirements focused on disclosures.
- The rules also require periodic disclosures regarding, among other things:
    - A detailed summary of the company's policies and procedures to identify and manage cybersecurity risks;
    - Management's role in implementing cybersecurity policies and procedures;
    - Board of directors' cybersecurity expertise and its oversight of cybersecurity risks; and
    - Detailed updates about previously reported material cybersecurity incidents.

Continuing its focus on cybersecurity, on March 9, 2022, in a party-line vote, the SEC proposed rules and amendments governing cybersecurity reporting requirements for public companies subject to the Securities Exchange Act of 1934. In announcing the proposal, SEC Chair Gary Gensler stated, "Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks … [I]f adopted [these] proposals would strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting." The proposed rules come on the heels of the SEC's recent cybersecurity enforcement actions (see GT Alert from Sept. 8, 2021) and proposed cybersecurity rule applicable to registered investment advisers and investment companies (see GT Alert from Feb. 11, 2022).

Background and Current Requirement

The SEC's Division of Corporation Finance issued guidance concerning public company disclosure obligations relating to cybersecurity risks and incidents in 2011 and expanded upon that guidance in 2018. In its earlier guidance, the SEC addressed the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the context of cybersecurity. In its most recent release, the SEC noted that although company disclosures of both material cybersecurity incidents and cybersecurity risk management and governance have improved since 2018, disclosure practices are inconsistent. Cybersecurity incidents have dramatically increased since 2018, and the impact of the SolarWinds Orion breach by Russia in 2020 put cybersecurity risk management on the forefront of the SEC's agenda. SEC enforcement activity concerning cybersecurity risk management, corporate governance and related disclosures has followed.

Noting recent research suggesting that cybersecurity is among the most critical governance-related issues for investors, the SEC believes investors would benefit from timely and consistent disclosure about material cybersecurity incidents. The proposed rules are designed to better inform investors about public company cyber risk management, strategy, and governance and to provide timely notice of material cybersecurity incidents. The proposal would define "cybersecurity incident" as "an unauthorized occurrence 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." With enhanced disclosures that are consistent, comparable, and decision-useful, the SEC maintains investors will be better positioned to evaluate company exposure to cybersecurity incidents as well as their ability to manage and mitigate the risks.

Incident Disclosure Proposed Amendments

The SEC, in an attempt to address growing concern that material cybersecurity incidents are under-reported and that existing reporting may not be sufficiently timely, has proposed that:

(1) Companies disclose information about material cybersecurity incidents in a current report on Form 8-K within four business days after the company has determined that it experienced a material cybersecurity incident. The proposed rule would amend Form 8-K by adding new Item 1.05, mandating disclosures concerning: (a) when the incident was discovered and whether it is ongoing, (b) a description of the nature and scope of the incident, (c) whether data was stolen, altered, accessed, or used for an unauthorized purpose, (d) the effect of the incident on the company's operations and (e) whether the company has remediated or is currently remediating the incident. Companies would not be required to disclose specific, technical information about their planned responses or their cybersecurity systems, related networks or potential vulnerabilities in such detail as would impede their responses or remediation of the incidents.

The trigger for the filing is the date on which the company determines that the incident is material, rather than the date of discovery of the incident. What constitutes "materiality" for purposes of cybersecurity incident disclosure would be consistent with case precedent in the securities law context, where courts have deemed information material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or if it would have "significantly altered the 'total mix' of information made available." The SEC indicated that it expects companies will be diligent in making materiality determinations. Proposed Item 1.05 would not provide for a reporting delay when there is an ongoing internal or external investigation relating to the incident.

(2) Add a new Item 106(d) of Regulation S-K and Item 16J(d) of Form 20-F to require registrants to provide updated disclosure relating to previously disclosed cybersecurity incidents and to require disclosure, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate; and

(3) For foreign private issuers who are not required to file current reports on Form 8-K, amend Form 6-K to add "cybersecurity incidents" as a potential trigger for Form 6-K filing.

Risk Management, Strategy, and Governance Disclosure

In addition to incident reporting, the SEC proposal requires enhanced and standardized disclosure on registrants' cybersecurity risk management, strategy, and governance. While these requirements are arguably all part of what a company should already be disclosing about cybersecurity risks, what's notable in the proposed rules is the level of detailed required to be included in the reports. Specifically, the proposal would:

(1) Add Item 106 to Regulation S-K and Item 16J of Form 20-F to require a registrant to:

a. Describe its policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity as part of its business strategy, financial planning, and capital allocation. Among other things, proposed Item 106(b) would require a company to disclose a number of details about its cybersecurity program, including risks posed by third parties, how it detects and prevents cybersecurity incidents, business continuity planning, and impact of previous incidents on a company's practices.

b. Require disclosure about the board's oversight of cybersecurity risk and management's role and expertise in assessing and managing cybersecurity risk and implementing the registrant's cybersecurity policies, procedures, and strategies. Proposed Item 106(c)(1) would include a discussion regarding how the board manages cybersecurity oversight, how and how often the board is informed about cybersecurity risks, and the board's consideration of these risks as part of its business strategy, risk management and financial oversight. Proposed Item 106(2) would require similar descriptions regarding the management positions or committees responsible for managing cybersecurity risk, including whether the company has designated a chief information officer and the processes by which management is informed about and monitors the prevention, detection, mitigation, and remediation of cybersecurity incidents.

(2) Amend Item 407 of Regulation S-K and Form 20-F to require disclosure regarding board member cybersecurity expertise. Proposed Item 407(j) would require disclosure in annual reports and certain proxy filings if any member of the company's board of directors has expertise in

> cybersecurity, including the name(s) of any such director(s) and any detail necessary to fully describe the nature of the expertise. The proposal does not define what constitutes "cybersecurity expertise" but does contain a nonexclusive list of criteria to consider, such as prior work experience in cybersecurity, certifications, or degrees in cybersecurity or relevant knowledge, skills, or other background in cybersecurity. Proposed Item 407(j)(2) would create a safe harbor intended to clarify that a board member designated as having cybersecurity expertise would not be deemed an expert for any purpose (including for purposes of Section 11 of the Securities Act of 1933) and would not impose on such person any additional duties or liabilities.

While these new disclosure requirements are significant, what is also notable is what is not included. The SEC's proposed rules governing registered investment advisors and broker dealers mandate specific security measures that must be adopted. The proposed public company rules do not go that far. However, based on the proposed reporting requirements, it appears that the SEC is pushing companies towards more robust cybersecurity disclosures. Even if the final rules vary from the proposals, companies may want to consider the following actions.

Takeaways:

- **Update Your Incident Response Plans**: Public companies may want to consider updating their incident response plans to include the four business-day requirement for filing an 8-K after identifying a material cybersecurity incident. The plan should outline the specific pieces of information the SEC says should be contained in the report. Consider building into the plan the need to potentially include updates in quarterly 10-Q reports.
- **Assign a Board Committee Oversight of Cybersecurity Risk**: Given the focus on board oversight, boards may want to consider assigning an existing committee the task of focusing specifically on cybersecurity risks. Committee members ideally should have either a cybersecurity background or receive regular training on cyber risks. The committee may consider requesting frequent updates from management about cybersecurity threats to ensure appropriate resources are allocated to addressing such risks.
- **Design a Vendor Management Program**: One common thread throughout the recent proposed rules by the SEC is the emphasis on the risks posed to a company by third party service providers. It is increasingly important that companies show careful vetting in the selection of service providers and consistent monitoring of vendors' network access and security practices.
- **Develop a Business Continuity Plan that Incorporates Cyber**: While business continuity plans historically have focused on more traditional disasters and outages, the increase in ransomware attacks in recent months and the threat of wiper attacks by foreign governments has placed emphasis on the need to include cyber risks in continuity planning.
- **Create a Checklist for 10-K Cyber Risk Disclosures**: The proposed rules mandate disclosure of multiple items that lend themselves nicely to a checklist of points that must be included in a company's 10-K disclosure. The SEC has indicated that there should be less reliance on general statements about cyber risks and more specificity, with a goal toward providing investors with enough information to make an informed decision.

GT GreenbergTraurig

Authors

This GT Alert was prepared by:

- Steven M. Malina | +1 312.476.5133 | malinas@gtlaw.com
- Jena M. Valdetero | +1 312.456.1025 | valdeteroj@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Long Island. Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.