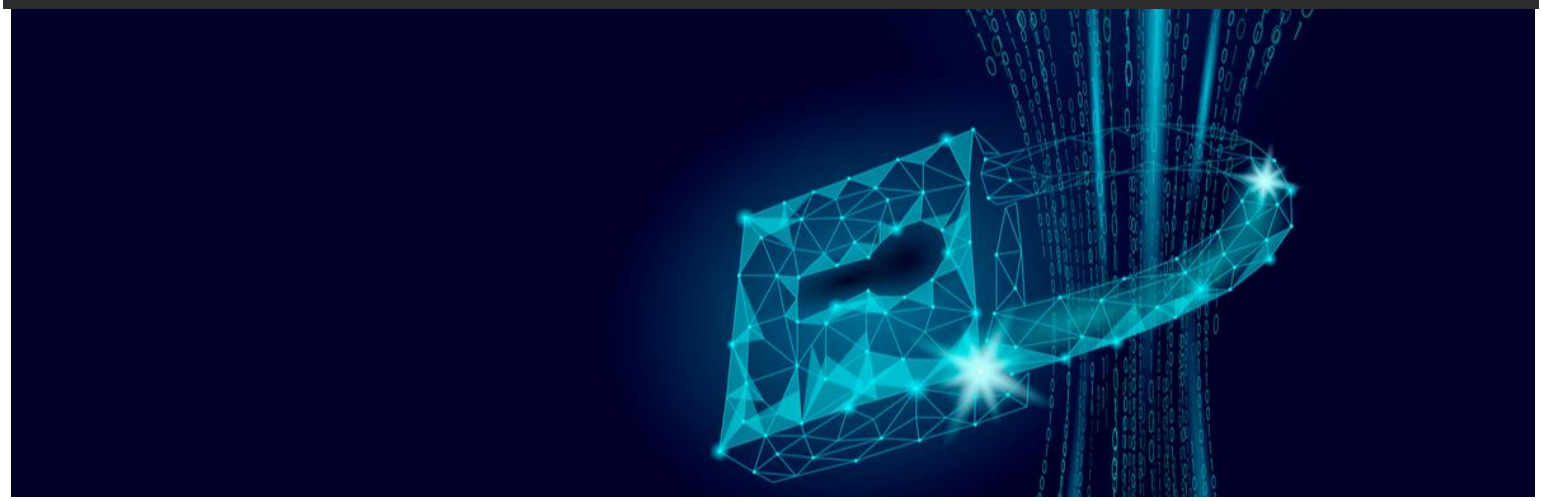
GT GreenbergTraurig

Alert | Data Privacy & Cybersecurity/ Financial Regulatory & Compliance



July 2023

SEC Finalizes Cyber Rules for Public Companies: What You Need to Know

Go-To Guide:

- The SEC has continued its focus on cybersecurity risks, adopting a final rule governing such risks for public companies.
- Once the rule is in force, public companies will have four business days to file an 8-K disclosing a material cybersecurity event.
- Companies will also be required to disclose their process for assessing, identifying, and managing material cyber risks in their annual reporting.
- Disclosure of the Board of Directors' oversight of cybersecurity risks will now be required in annual 10-K reporting.

On July 26, 2023, the Securities and Exchange Commission (SEC) adopted the long-awaited final rule requiring that public companies disclose information about cybersecurity incidents within four business days of determining the incident is material. GT wrote about the proposed rule shortly after it was released in March 2022. For context, Commissioner Caroline Crenshaw noted, in connection with the adoption of the rule, that, "cybersecurity breaches reported by public companies increased by nearly 600% in the last decade and the costs, borne by issuers and their investors, are estimated to be in the trillions of dollars per year in the U.S. alone."

The final rules contain new Item 1.05 on Form 8-K requiring disclosure of any material cybersecurity incidents and a description of the material aspects of the nature, scope and timing of the incident within four business days of the determination that the incident is material.

Materiality is defined as having a "substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or would have "significantly altered the 'total mix' of information made available."

The four-day timing requirement is consistent with the SEC's requirement to disclose any material adverse event; arguably, a significant cyber incident could give rise to an 8-K filing even before this rule takes effect. SEC Chair Gary Gensler recognizes that fact in his press release announcing the final rules, noting "[m]any public companies already do this, but it's not done consistently."

The final rule differs in key ways from the proposed rule. Mr. Gensler said, "the final rules will require issuers to disclose only an incident's material impacts, nature, scope, and timing, whereas the proposal would have required additional details, not explicitly limited by materiality." Additionally, "doubts as to the critical nature" of the relevant information should be "resolved in favor of those the statute is designed to protect," namely investors.

Mr. Gensler was quick to point out that the requirement triggers not from the date an incident occurred, but from the date the company determined its material impact. While this clarification may ease some anxiety as to whether companies will be expected to make a public filing while in the early days of investigating an incident, from a practical perspective, any significant delay in reporting could risk regulatory and public scrutiny concerning the timing of a company's investigation.

Although the deadline to disclose may be extended if the U.S. Attorney General determines that disclosure would pose a substantial risk to national security or public safety, such an extension likely will be rare for companies. This exemption somewhat aligns with the exemption in state data breach notification laws that permits a company to delay notification if law enforcement believes doing so would interfere with an ongoing investigation. In practice, law enforcement rarely directs companies to delay notification.

The new Item 106 of Regulation S-K requires disclosure of processes for assessing, identifying, and managing material risks from cybersecurity threats. It also requires a determination of whether any cybersecurity threats or previous incidents have materially affected or are reasonably likely to materially affect the company. While many companies already were including cyber risks in their disclosures, there previously were no explicit requirements to do so.

Item 106 will also require companies to describe in their annual 10-K report the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

Form 6-K will require foreign private issuers to disclose information about material cybersecurity incidents that they disclose in a foreign jurisdiction to any stock exchange or to security holders. Form 20-F will require foreign private issuers to make disclosures similar to those required by new Item 106 of Regulation S-K.

The rule passed by a slim 3-2 majority, with Commissioners Hester M. Peirce and Mark T. Uyeda opposing. Peirce, while acknowledging that the final rule is better than the proposed rule, argues that the final rule provides a road map for cyber criminals on which companies to attack and how to attack them, micromanages and "reads like a test run for future overly prescriptive, overly costly disclosure rules

covering a never-ending list of hot topics." Uyeda echoes by claiming that the new rule inappropriately elevates cybersecurity risks over that of other risks such as "customer acquisition and retention, product development, innovation, [and] globalization" which sends mixed signals to investors. However, Gensler argues that the new rule merely takes the existing various disclosures companies made and makes them more "consistent, comparable, and decision-useful…"

Public companies have a little breathing room to prepare for the rule changes, but not much. The final rules take effect 30 days following publication of the adopting release in the Federal Register. The Form 10-K and Form 20-F disclosures will be due beginning with annual reports for fiscal years ending on or after Dec. 15, 2023. The Form 8-K and Form 6-K disclosures will be due beginning the latter of 90 days after the date of publication in the Federal Register or Dec. 18, 2023. Smaller reporting companies will have an additional 180 days before they must begin providing the Form 8-K disclosure.

Takeaways

- **Update Your Incident Response Plans**: With the rules finalized, now is the time to consider updating your 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 and how the company will determine whether the materiality threshold has been met (and thus the four-day deadline to report started to run). Consider building into the plan the need to include updates in quarterly 10-Q reports.
- **Assign a Board Committee Oversight of Cybersecurity Risk**: Notwithstanding that the final rule does not include the proposal's requirement that companies have a board member who is a cybersecurity expert, Boards should consider assigning an existing committee the task of focusing specifically on cybersecurity risks. Committee members ideally should either have a cybersecurity background or receive regular training on cyber risks, given the highly technical nature of cyber. 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**: Regulators, including the SEC, have ramped up their focus on the risks third-party service providers pose to a company. This is particularly true in light of the widespread impact of recent highly publicized vendor data security incidents, including SolarWinds and MOVEit, affecting thousands of companies worldwide. Companies should address these risks in their annual reporting and be prepared to 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 years and the threat of wiper attacks by foreign governments have placed emphasis on the need to include cyber risks in continuity planning.
- **Create a Checklist for 10-K Cyber Risk Disclosures**: The final 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 there should be less reliance on general statements about cyber risks and more specificity, with a goal toward providing investors enough information to make an informed decision.

GT GreenbergTraurig

Authors

This GT Alert was prepared by:

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

* Special thanks to Chicago Summer Associate Spencer Harris ˇ for his valuable contributions to this GT Alert.

ˇ *Not a licensed attorney*.