COLLECTIVE INTELLIGENCE

What to Know About the SEC's New Rules on Cybersecurity Disclosures

July 2023

On July 26, 2023, the US Securities and Exchange Commission (SEC) adopted sweeping changes to cybersecurity disclosure requirements for publicly traded companies. Companies must begin complying as soon as December 2023.

These rules set a new standard for communicating about cybersecurity to investors and the public, and all companies should be not only aware of the changes but actively preparing to meet the requirements.

There are three key elements in the new rules that corporate leaders should know:

1) **Disclosure of material cybersecurity incidents.** Publicly listed companies experiencing a cybersecurity incident will be required to disclose it within four business days of determining that the incident is material.
2) **Annual reporting on cybersecurity risk management, strategy and governance.** Companies will be required to report new cybersecurity disclosures annually, including:
    - Processes in place for assessing, identifying and managing material risks from cybersecurity threats.
    - Any material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents.
3) **Comparable disclosures by foreign private issuers.** Foreign private issuers will be required to make comparable disclosures to the SEC.

Actions to take now

Companies across all sectors and regions face increasing odds of experiencing a cybersecurity incident. How a company prepares and responds during an incident, however, is within its control. In light of these new rules, corporate executives should:

- **Bring together leaders from different business functions to discuss the implications of these rules for the company's crisis management plans.** Core functions such as IT, legal, finance, HR, government relations and communications should have a seat at the table to ensure a coordinated approach. Discuss how these rules affect existing plans and protocols and whether updates are needed. Publicly listed companies must begin complying with the SEC's incident disclosure requirements as early as December 18, 2023.

- **Refresh cybersecurity incident response plans and conduct simulations to build muscle memory.** Update existing plans and protocols and socialize them internally so leaders understand their respective roles. Conduct tabletop exercises to pressure test these plans and help employees practice responding to a live cybersecurity incident before a real crisis occurs. Use crisis preparedness activities as an opportunity to modernize business continuity planning and ensure plans account for the real risk of significant and sustained operational impairment resulting from ransomware and other pervasive cybersecurity threats.
- **Prepare for the addition of cybersecurity risk management information to the company's annual report.** Review existing information, identify potential gaps, and begin mapping out the story you will tell when it comes to cybersecurity risk management, strategy, and governance as part of the company's overall annual reporting process. Publicly listed companies must provide these disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023.

Industry reactions and implications

Reactions to the SEC rules have been mixed. While government and corporate leaders broadly agree that updated cybersecurity disclosure frameworks are needed, many have expressed concerns about the final rules, including the limitations of a four-day incident reporting window and the potential negative ramifications for investors and companies if an incident is reported before a company has had sufficient time to investigate.

As these rules go into effect, there will be wide-ranging implications, including:

- **Changing dynamics for cybersecurity incident response.** The rules will change public companies' processes and decision-making calculations for determining when and how to disclose a cybersecurity incident. The rules both shorten the potential timeframe and lower the bar for what previously constituted a material incident, which will likely increase the frequency of reporting and overall public awareness of cybersecurity incidents. Delays will be only permitted if the US attorney general assesses serious national security or public safety risks associated with disclosure.
- **Increasing transparency and focus on cybersecurity governance and risk management.** The rules require public companies to disclose sufficient detail about their cybersecurity practices to allow investors to ascertain a company's risk profile. The rules also require companies to explain the role of their board in cybersecurity governance and risk management, which is notable and could be followed by additional board-level requirements in the future.
- **Heightened stakes for public companies and executives.** SEC enforcement of the rules concerning cybersecurity incident disclosures will ultimately raise the stakes for publicly listed companies and their executives and directors, with the potential for financial and reputational fallout.

Brunswick's global Cybersecurity, Data, and Privacy practice group advises companies in every region and every sector on effective strategies to prepare for, respond to, and lead through cybersecurity and data protection challenges and opportunities.

To continue the conversation

Please reach out to Brunswick's Cybersecurity, Data, and Privacy Team at cyber@brunswickgroup.com.

BRUNSWICK