Guidepost

THE SEC HAS NEW CYBERSECURITY RULES. ARE YOU PREPARED AND READY?

On July 26, 2023, the Securities and Exchange Commission (SEC) implemented new cybersecurity rules to require disclosure of material cybersecurity incidents within four business days, with limited exceptions. Additionally, public companies will be required to provide annual disclosures regarding cybersecurity governance and risk management in order to be more transparent about their cybersecurity posture. These rules become effective in December 2023 and will influence both compliance costs and the potential for enforcement actions.

Companies and entities subject to these rules should not delay in evaluating their internal cybersecurity plans and taking action. It is worth noting that the SEC has already taken enforcement actions related to cybersecurity incidents, even prior to the finalization of the new rules.

Cybersecurity incidents can take shape in a number of different forms, be carried out by organized cybercrime rings or third-party vendor attacks and have varying scales of impact. However, their central theme remains disruption, leading to financial losses and reputational damage.

The most common types of breaches experienced by organizations include IT failure (24%); human error (21%); supply chain attack (19%); destructive attack (17%); ransomware attack (11%); and other malicious attack (8%). Reaching an all-time high, the cost of a data breach averaged $4.35 million in 2022, climbing 12.7% from $3.86 million in 2020. Additionally, the cost of noncompliance fines could be staggering.

The new SEC rule addresses two main areas:

1. **Incident Disclosure:**

Timing: A company must report a cybersecurity incident on Form 8-K within four business days after it decides that the incident is material. When assessing materiality, companies should consider a range of information, encompassing quantitative and qualitative factors. Even incidents with low odds of negative outcomes but potential for substantial loss or liability could be considered material. The materiality determination remains consistent, relying on the principle that a reasonable investor would deem it significant. Nonetheless, companies aren't obligated to

disclose technical details of their responses or cybersecurity systems publicly. Such disclosure could impede their ability to effectively address the incident. A company must make the materiality determination without unreasonable delay. The SEC provides examples of what constitutes "unreasonable delay", such as when a company intentionally delays a committee meeting on the materiality determination beyond 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 deadlines. The SEC notes that if a company adheres to a normal internal practice and disclosure controls and procedures, that will suffice to demonstrate good faith compliance.

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 company, including its financial condition and results of operations.

Broader definition of "cybersecurity incident": The SEC 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. The new item 106 (a) of Regulation S-K defines a cybersecurity incident as an unauthorized event or related events that compromise a company's information systems, risking confidentiality, integrity, or availability.

2. **Annual cybersecurity risk management disclosure:**

The rule calls for disclosure of management's role in implementing cybersecurity policies and procedures, including risk management and strategy. It also requires disclosure of board oversight, how cybersecurity risks factor into company strategy, financial planning, and capital allocation, as well as information about the presence of a chief information security officer (CISO) and policies for identifying and managing cyber risks.

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 providers. 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.

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. Companies are not required to disclose any board expertise in relation to cybersecurity or whether the board considers cybersecurity as part of its business strategy, risk management and financial oversight.

Role of management. 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.

Disclosure of risks from cybersecurity threats. The 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." The SEC asks companies to "consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident."

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.

Take Immediate Steps to Improve Cybersecurity Posture

Companies will need to take immediate steps to improve their cybersecurity posture given the SEC's history of enforcement actions against regulated entities for identity theft violations and public companies for cyberattack-related disclosure and control violations. Below are some recommendations to mitigate some of the risk of the constantly evolving nature of cybersecurity. Companies should not delay implementing these recommendations, as they can save companies from security breaches that can lead to reputational damage, business interruption and hefty fines.

- Consider the services of an independent CISO.
- Conduct periodic risk of network security.
- Conduct briefings to executive teams and boards on these exercises as well as to test written protocols to ensure alignment and effective oversight.
- Create or update the Incident Response Plan for compliance with the new SEC requirements.
- Ensure cybersecurity risk management processes have been integrated into the overall risk management system or processes.
- Ensure processes are in place to oversee and identify risks from cybersecurity threats associated with third-party service providers.

- Ensure processes are in place to monitor and inform persons, boards or committees about the prevention, detection, mitigation, and remediation of cybersecurity incidents.
- Conduct annual table-top exercises to test incident response procedures to ensure alignment with the SEC requirements.
- Provide ongoing cybersecurity training to all employees.

The new SEC rules aim to enhance cybersecurity awareness, potentially impacting compliance costs and enforcement actions. Companies are advised to promptly assess their cybersecurity strategies to avoid breaches that could lead to financial losses and reputational harm. Companies should also strongly consider engaging assessors, consultants, auditors, or other third parties to evaluate the entire cybersecurity risk management processes.

C. TODD DOSS

Senior Managing Director

Christopher "Todd" Doss has a diverse background in managing and coordinating responses to complex security incidents, including but not limited to cyber-attacks, data breaches, and insider threats. Having led more than 4,000 cyber incident responses and investigations, he has gained an in-depth knowledge of designing and executing response plans and leading cybersecurity risk management projects.

MATTHEW CORWIN CISA, CISSP, CDPSE

Managing Director

Matthew A. Corwin has more than 20 years of experience specializing in privacy, regulatory compliance, and cybersecurity with specialized hands-on experience directing the implementation and integration of secure design principles and service engineering initiatives leveraging the latest technologies. He has a successful track record of facilitating technology-business alignment while balancing risk exposure and corporate growth. Mr. Corwin also has extensive expertise in analyzing technical architecture to attain and demonstrate best-in-class industry and regulatory standards compliance in global environments.