Cyber Disclosure Is A Mainstay In 2025 SEC Exam Priorities

By **Anjali Das** (January 15, 2025)

Anjali Das

On Oct. 21, the U.S. Securities and Exchange Commission highlighted its examination priorities for 2025.[1]

Not surprisingly, one of the SEC's priorities will be cybersecurity risk due to the proliferation of cyberattacks. In particular, the SEC has indicated that it will examine public companies' cybersecurity practices to assess whether they are "reasonably managing information security and operational risks," as well as making appropriate disclosures of material cybersecurity incidents in public SEC filings.

Despite a new administration and a new SEC chair incoming, cybersecurity disclosures and risk management practices will remain important due to the growing threat of cyberattacks.

SEC's 2025 Examination Priorities

The SEC has statutory authority under the federal securities laws to conduct examinations of registered entities at any time. The SEC staff of the Division of Examinations may call the entity and follow up with a letter notifying it of the examination, requesting information and documents. The staff will typically request meetings with the entity's personnel to discuss the information provided, and may ask for supplemental information or documents.

Once the staff has completed its interviews and analyses, it typically conducts a conference with the entity to discuss any issues identified during the examination process. Section 4E(b)(1) of the Exchange Act requires the staff to provide the entity with written notification that the investigation has concluded, and whether it was concluded without making any findings or if the entity must undertake corrective actions. In addition, the SEC may choose to bring an enforcement action against an entity for noncompliance and violation of federal securities laws.[2]

The SEC emphasizes its risk-based approach to conducting examinations of registered entities. The SEC published its fiscal year 2025 examination priorities to highlight critical issues that the SEC's Division of Examinations "believes present the highest risk areas to investors and the markets."[3]

In the past two years, the division has increased its capabilities in cybersecurity, which it identifies as a perennial risk to registrants "due to the proliferation of cybersecurity attacks."[4] Accordingly, the SEC has identified cybersecurity as an examination priority.

In particular, the division intends to focus on registrants' "policies and procedures, governance practices, data loss prevention, access controls, account management, and responses to cyber-related incidents, including those related to ransomware attacks."[5]

SEC's Cybersecurity Disclosure Rules

In March 2022, the SEC proposed rules mandating that public companies disclose cybersecurity risk management, governance, and material cybersecurity incidents. The final rules went into effect Sept. 5, 2023, and apply to all public companies that are subject to

the reporting requirements under federal securities laws.

As of Dec. 18, 2023, companies must disclose material cybersecurity incidents in Form 8-K Item 1.05 within four business days, per the cybersecurity incident disclosure rule. In addition, the cybersecurity risk management disclosure rule mandates that companies provide cybersecurity risk management disclosures in Regulation S-K, Item 106, beginning with annual reports for fiscal years ending on or after Dec. 15, 2023.

Cybersecurity Incident Disclosure Rule

The SEC rules require prompt disclosure of a material cybersecurity incident. The SEC defined a "cybersecurity incident" as "an unauthorized occurrence, or a series of related unauthorized occurrences, 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."[6]

Notably, the SEC rules do not expressly define the term "materiality." However, in the securities law context, the U.S. Supreme Court interpreted this in its 2011 decision in Matrixx Initiatives v. Siracusano to mean information that a reasonable shareholder would consider important in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available" to the public.[7]

Form 8-K, Item 1.05, focuses on the impact a cybersecurity incident may have on the company's financial condition and results of operations. However, as noted by the SEC, this is not an exclusive test for materiality. Instead, companies may consider other factors such as reputational harm, competitiveness and potential litigation attributable to the incident.

Importantly, the SEC rules do not exempt companies from disclosing known third-party cybersecurity incidents that may have a material impact on the company. This is a growing concern in light of increasing supply chain, vendor and systemic cyber risk.

Generally, the four-business-day reporting deadline is triggered when a company first determines that an incident may have a material impact on the organization — not within four business days of the initial discovery of an incident.[8] In fact, the SEC has acknowledged that it is unlikely a company will be able to determine materiality at the outset.

Nonetheless, the SEC encourages companies to diligently gather information to conduct a thorough, documented materiality analysis without unreasonable delay. This analysis may change based on new developments and as more information becomes available. In that event, the company should update its prior disclosures as needed.

Cybersecurity Risk Management Disclosure Rule

Pursuant to SEC Regulation S-K, Item 106, companies are required to make annual disclosures in their Form 10-K about their cybersecurity risk management and processes for assessing, identifying, and managing material risk from cyber threats. These disclosures should address the following risk management factors:

- Processes for assessing, identifying and managing material risks from cyber threats;
- Whether these processes have been integrated into the company's overall risk management;
- Processes to identify cyber threats associated with third-party service providers; and

- Whether any cyber threats have materially affected the company.[9]

In addition, companies must disclose board and management oversight of cybersecurity risk, including the following:

- The board committee responsible for oversight of cyber threats;

- The process by which the board is informed about cyber risks;

- Management's role in assessing material risks from cyber threats;

- Management positions or committees responsible for assessing and managing cyber risks, and their relevant expertise;

- The process by which management is informed of and monitors cybersecurity incidents; and

- Whether management reports cybersecurity incidents to the board.[10]

SEC Enforcement Actions for Misleading Cybersecurity Disclosures

The SEC has started bringing charges for violations of the federal securities laws against companies that fail to make appropriate cybersecurity disclosures, resulting in substantial civil fines.[11] As noted by the SEC's acting director of the Enforcement Division, "while public companies may become targets of cyberattacks, it is incumbent upon them to not further victimize their shareholders … by providing misleading disclosures about the cybersecurity incidents."[12]

Specifically, in October, the SEC announced that it had charged four companies — Unisys Corp., Avaya Holdings Corp., Check Point Software Technologies Ltd. and Mimecast Ltd. — with misleading cyber disclosures. The SEC's charges against each of these companies involved the sophisticated SolarWinds Orion software supply chain hack.

In the December 2020 SolarWinds incident, foreign adversary nation-state threat actors allegedly leveraged the SolarWinds Orion platform to install malicious code that infiltrated and stole sensitive information from a number of SolarWinds' downstream customers.[13] In each of these instances, the companies allegedly downplayed and misrepresented the extent of their cybersecurity risk in their SEC filings, despite knowledge to the contrary.

Unisys

The SEC alleged that Unisys was aware that it used a version of the compromised SolarWinds Orion software, and experienced prolonged and persistent compromises of its environment linked to the same threat actor, in addition to the unauthorized access and transfer of 33 gigabytes of data from its systems.

The SEC claimed that the company's cybersecurity risk disclosures were materially false and misleading because they inaccurately described, in hypothetical terms, the intrusions and risk of unauthorized access to data.

In addition, the SEC alleged that the company's misleading disclosures were attributed to inadequate controls and procedures that failed to ensure that potentially material cybersecurity incidents were timely communicated to management or timely reported. Moreover, the company's incident response policies did not require cybersecurity personnel to report incidents to management or the legal team.

The SEC issued a cease-and-desist order and imposed a $4 million civil penalty against the company for violations of the federal securities laws.[14]

Avaya

In the case of Avaya, the SEC alleged that the company was aware that two of its servers had installations of the infected SolarWinds Orion software; the same threat actor also compromised the company's email environment, including the account of one of its incident response personnel; and it accessed 145 files containing sensitive information.

Notwithstanding, the SEC claimed that the company failed to disclose material facts regarding the scope of the incident and misrepresented that there was unauthorized access to a limited number of emails.

The SEC issued a cease-and-desist order and imposed a $1 million civil penalty against the company for violations of the federal securities laws.[15]

Check Point

The SEC alleged that Check Point's internal investigation revealed that the SolarWinds Orion incident affected two of its servers. The investigation also uncovered the threat actor's network reconnaissance, attempted lateral movement within the network, use of tools to compress and steal data, and compromise of two corporate accounts.

According to the SEC, the company's risk profile changed materially due to the SolarWinds Orion compromise, which was likely launched by a nation-state threat actor.

The SEC concluded that the company failed to accurately reflect these cyber risks in its SEC filings. Instead, the company purportedly issued generic risk disclosures that did not specifically address the actual known events.

The SEC issued a cease-and-desist order and imposed a $995,000 civil penalty against the company for violations of the federal securities laws.[16]

Mimecast

Finally, in the case of Mimecast, the SEC alleged that the company identified computers in its network that had installations of the compromised SolarWinds Orion software. The company discovered that the same threat actor exfiltrated a Mimecast-issued authentication certificate used by 10% of its customers, comprising five of Mimecast's own customers' cloud platforms using the exploited certificate.

In addition, the company was purportedly aware that the threat actor gained access to its email, source code and a database containing encrypted credentials for 31,000 customers in addition to server/network configuration information for 17,000 customers. The SEC claimed that the company failed to disclose the number of customers whose information was compromised, or the nature or quantity of source code that was stolen.

The SEC issued a cease-and-desist order and imposed a $990,000 civil penalty against the company for violations of the federal securities laws.

Key Takeaways

Given the SEC's heightened scrutiny of cybersecurity disclosures, which is a stated examination priority for 2025, it is imperative that companies and their directors and officers take steps now to ensure they have appropriate governance and processes in place to address and assess cyber threats and risks.

As a threshold matter, companies should review their existing incident response plan to select personnel responsible for identifying and responding to threats, establish criteria for determining the level of severity of an incident, and decide when and how incidents should be reported to management.

Management, in turn, should designate a committee to conduct a timely, well-documented materiality analysis to evaluate whether an incident should be disclosed in Form 8-K, Item 1.05. This analysis should consider various factors such as the type of incident, the impact on business operations, the ability to restore systems, the loss or theft of sensitive data, negative publicity, reputational harm, customer attrition, remediation costs, business interruption loss, available cyber insurance, the overall impact on the company's finances, the threat of litigation, and third-party claims. The materiality analysis is a living document that should be updated to reflect new information as the investigation unfolds.

As reflected by the SolarWinds Orion software hack, third-party vendor and supply chain risk is a growing concern. When a cybersecurity incident originates outside the company, the company is not absolved from conducting due diligence and a materiality analysis. While the company may have to rely on the third party for some information, it should be in a position to address and evaluate the known impact on the company.

Once management and/or the board determines that an incident is material, it must be reported in Form 8-K, Item 1.05, within four business days. Boilerplate or generic cybersecurity disclosures will not suffice.

Instead, companies should include sufficient detail for investors to understand the nature and scope of an incident, including the impact on the company's operations and finances. These cybersecurity disclosures should be updated as needed to reflect any substantive new information and developments.

While 2025 will bring a new administration and a new SEC chair, cyber threats will likely increase in terms of the level of sophistication of cybercriminals, in addition to the sheer volume and severity of cyberattacks on victim organizations. To that end, companies should make a New Year's resolution to review and update their cybersecurity disclosure and risk management practices and processes.

Anjali C. Das is a partner, and co-chair of the national cybersecurity and data privacy practice, at Wilson Elser Moskowitz Edelman & Dicker LLP.

[1] SEC Fiscal Year 2025 Examination Priorities, p. 12.

[2] SEC 2389 (03-23): Information for Entities Subject to Examination or Inspection by the SEC.

[3] SEC Fiscal Year 2025 Examination Priorities.

[4] Id.

[5] Id.

[6] 17 CFR § 229.106(a).

[7] See Matrixx Initiatives v. Siracusano, 563 U.S. 27, 38-40 (2011).

[8] A limited exception for delay in reporting an otherwise material cybersecurity incident occurs if there is a determination by the Attorney General that such disclosure would pose a substantial risk to national security or public safety.

[9] 17 CFR § 222.106(b).

[10] 17 CFR 229.106(c).

[11] SEC press release 2024-174: "SEC Charges Four Companies with Misleading Cyber Disclosures" (October 22, 2024).

[12] Id. at p. 2.

[13] New York Department of Financial Services (NY DFS) Report on the SolarWinds Cyber Espionage Attack and Institutions' Response (April 2021).

[14] In the Matter of Unisys Corporation, SEC Administrative Proceeding File No. 3-22272, Cease and Desist Order.

[15] In the Matter of Avaya Holdings Corp., SEC Administrative Proceeding File No. 3-22269, Cease and Desist Order.

[16] In the Matter of Check Pont Software Technologies Ltd., SEC Administrative Proceeding No. 3-22270, Cease and Desist Order.