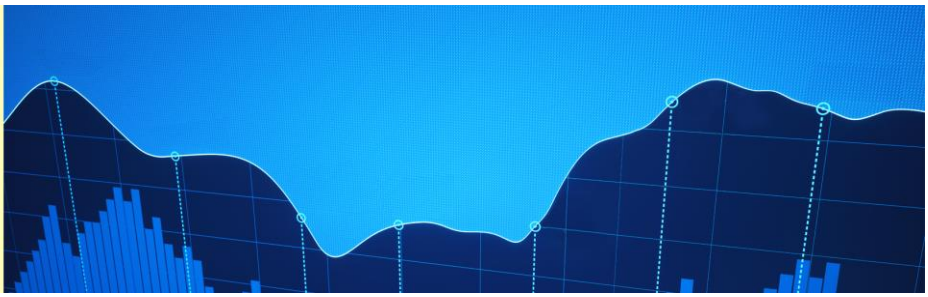
THOMPSON HINE



Securities Quarterly Update

July 2024 | Summer Edition

Welcome to the summer edition of Securities Quarterly Update*, a publication that provides updates and guidance on securities regulatory and compliance issues. In this edition, we look at the SEC's recent focus on cybersecurity, which highlights the importance of robust cyber risk management and disclosure practices for public companies.*

Recent Trends in Cybersecurity Following Adoption of New Rules

In July 2023, the SEC adopted final rules requiring certain cybersecurity-related disclosures intended to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies." These rules require that public companies provide cybersecurity-related disclosure in annual reports on Form 10-K and report material cybersecurity incidents on Form 8-K. For additional information, see our alert dated July 27, 2023 and our alert dated December 11, 2023. Following the adoption of these rules, the SEC has clarified the rules, instituted enforcement actions, and issued comment letters.

Disclosure Clarifications and Nuances

In June 2024, the SEC issued a statement seeking to clarify the interpretation of the rule requiring the reporting of material incidents under Item 1.05 on Form 8-K. The SEC clarified that Item 1.05 does not prohibit private discussions about incidents. Rather, companies can share information with vendors, customers, or others potentially impacted to aid in remediation and compliance. While concerns about violating Regulation FD exist, these rules do not fundamentally change for cybersecurity disclosures. Companies can navigate these rules by ensuring the shared information is either immaterial or shared with parties not covered by Regulation FD, or by using confidentiality agreements.

In May 2024, as detailed in our alert dated May 23, 2024, the Director of the SEC's Division of Corporate Finance made remarks focused on how organizations can disclose cybersecurity incidents that have not been identified as "material" and emphasized the relevant factors that should be considered when making materiality determinations.

In June 2024, the SEC's Division of Corporation of Finance updated its Form 8-K interpretations to add a series of questions and answers relating to cybersecurity disclosure. The SEC clarified that remediation of a cybersecurity attack prior to a finding of materiality under Item 1.05 did not preclude a company from finding that the cybersecurity attack was still material (see Question 104B.05), that remediation of a materiality cybersecurity incident prior to disclosure does not relieve a company from its obligation to report the incident under Item 1.05 (see Question 104B.06), that insurance reimbursement of a ransomware payment does not relieve a company of its obligation to report a material cybersecurity incident under Item 1.05 (see Question 104B.07), and that a ransomware payment made by a company that is small in size does not necessarily make the related cybersecurity incident immaterial (see Question 104B.08). The SEC also reiterated that a series of cybersecurity incidents involving ransomware attacks over time, either by a single threat actor or by multiple threat actors, could be considered material on a collective basis if the incidents were related (see Question 104B.09). In doing so, it noted that the definition of "cybersecurity incident" for Item 1.05 purposes includes "a series of related unauthorized occurrences." In numerous of these new Q&A, the SEC reiterated the "facts and circumstances" nature of a materiality determination for a cybersecurity incident. Additional interpretive guidance is likely to follow.

Enforcement Actions

In June 2024, the SEC announced an enforcement action against a public company for allegedly failing to properly manage cybersecurity and internal controls following a series of cyber incidents prior to the adoption of the SEC's new cybersecurity disclosure rules, resulting in payment of a fine of more than $2 million. According to the SEC, during these incidents, a hacker accessed information belonging to a number of customers. The SEC alleged that the company did not design effective disclosure controls to report cybersecurity issues to management, nor did it respond promptly to alerts of unusual activity. Additionally, the company arguably failed to maintain adequate cybersecurity-related internal accounting controls to ensure that access to its IT systems was properly authorized.

In May 2024, the SEC fined the owner of several major financial exchanges $10 million for allegedly mishandling a cyber intrusion. According to the SEC, a hacker inserted malicious code into a VPN device used to remotely access the company's corporate network. Although the intrusion did not impact market operations, the SEC alleged that the company delayed notifying its subsidiaries and the SEC about the incident, taking four days to assess its impact and conclude it was minimal. This delay arguably violated federal regulations and the company's internal procedures.

Comment Letters

The SEC's Division of Corporation Finance has begun issuing comment letters addressing cybersecurity disclosures.

Form 8-K

As an example, a company filed a Form 8-K under Item 1.05 reporting that it had detected unauthorized activities on its IT systems, leading to business disruptions. In response, the company stated it immediately launched an investigation with external cybersecurity experts, activated its incident response plan, and shut down certain systems. The attack also involved data theft, including personal information, and encryption of IT systems, impacting business operations.

In response to the Form 8-K, the SEC issued a comment letter, requesting further details in an amended Form 8-K, as required by Instruction 2 to Item 1.05. The SEC highlighted that while the full scope and impact of the cyber incident were not initially known, and its material impact on business operations was expected to continue, the company had not yet determined its potential effects on financial condition or results of operations. The SEC asked for an expanded discussion to cover the scope of business operations affected and to describe all known and likely material impacts such as potential effects on vendor relationships, reputational harm due to stolen data and unfulfilled orders, and any impacts on financial condition or operational results.

Form 10-Q

As another example, a company announced that it had identified a cybersecurity incident impacting certain internal operations and IT systems. In its subsequent Form 10-Q, the company disclosed that operational delays due to the cybersecurity incident and related investigation and remediation costs adversely impacted the company's quarterly results.

Following the Form 10-Q disclosure, the SEC issued a comment letter regarding, among other things, the cybersecurity disclosure. The SEC highlighted that the incident limited the company's ability to take orders, invoice third parties, and ship its products and requested that future filings quantify the impact on net sales and product volume sold in accordance with Item 303(c) of Regulation S-X.

Takeaways

The SEC's recent focus on cybersecurity highlights the importance of robust cyber risk management and disclosure practices for public companies. Following the SEC's adoption of new rules in July 2023, companies should ensure compliance with these enhanced standards, including by incorporating them into their disclosure committee practices and implementing structures and controls to support these disclosures (through updated incident response plans or otherwise).

Recent enforcement actions underscore the need for effective internal controls and timely response protocols. Companies failing to meet these expectations have faced significant penalties, as seen with the $2 million fine for allegedly inadequate cybersecurity management and the $10 million fine for allegedly delayed incident reporting. Additionally, SEC comment letters have emphasized the

need for tailored disclosure, urging companies to detail the scope of affected operations and quantify impacts on financial performance.

Now that initial annual cybersecurity disclosures have been completed, public companies should continue refining their cybersecurity disclosure practices in light of the SEC's recent comment letters, additional interpretative guidance, and industry practices, including by reviewing peer disclosures. An effective process for assessing the materiality of cybersecurity incidents remains crucial, and companies should be prepared to justify their evaluations with both quantitative metrics and qualitative insights into potential impacts on operations, finances, and reputation. Vendor and other third-party management should also be periodically revisited as cybersecurity programs and disclosure practices evolve over time.

FOR MORE INFORMATION

For more information, please contact:

Jurgita Ashley
216.566.8928
Jurgita.Ashley@ThompsonHine.com

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Benjamin M. Russell
404.407.3609
Benjamin.Russell@ThompsonHine.com

Michael Blane
212.908.3953
Michael.Blane@ThompsonHine.com

or another member of our Securities, Capital Markets & Corporate Governance or Privacy & Cybersecurity teams.

Previous Editions of Securities Quarterly Update

- Q2 | Spring 2024
- Q1 | Winter 2024
- Q4 | Fall 2023
- Q3 | Summer 2023