FORsights™

Urgent Reminders on Required SEC Cyber Disclosures for Registrants

This summer's cyberattacks on healthcare and car dealerships are a timely reminder on the need for constant vigilance. Here is a helpful refresher on the SEC's cybersecurity disclosure requirements (timing, level of detail, and breaches at third-party systems), including two recently issued clarifications and SEC interpretations on ransomware payments. The SEC cybersecurity rule is now also effective for smaller reporting companies.

Form 8-K Disclosures

Registrants are required to disclose information about a cybersecurity incident within four business days after a registrant determines—**without unreasonable delay**—that it has experienced a **material** cybersecurity incident. The filing time frames start when the registrant determines an incident is material, not necessarily the incident's discovery date.

The SEC notes that an accidental occurrence is an unauthorized occurrence, even if there is no confirmed malicious activity. For example, if a company's customer data is accidentally exposed, allowing unauthorized access, the data breach would constitute a cybersecurity incident that would require a materiality analysis to determine if disclosure is required.

The final rule requires information on the incident's impacts, "the material aspects of the nature, scope, and timing of the incident, and ***the material impact or reasonably likely material impact*** on the registrant, including its financial condition and results of operations." Companies should consider both qualitative and quantitative factors in assessing the material impact of an incident. Examples of qualitative factors include harm to a company's reputation, its customer or vendor relationship, or the possibility of litigation or regulatory actions. The SEC intentionally did not include a quantifiable trigger for the impact assessment.

"A lack of quantifiable harm does not necessarily mean an incident is not material."

Registrants should provide the above items to the extent known at the time of the Form 8-K filing. Companies can file an amended Form 8-K with respect to any information that was not determined or was unavailable at the time of the initial Form 8-K filing.

Required disclosures do not include specific, technical information about a registrant's planned incident response or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident.

Without Unreasonable Delay

The final rule provides several examples of this concept, including:

- If the materiality determination is to be made by a board committee, intentionally deferring the committee's meeting on the materiality determination past the normal time it takes to convene its members would constitute unreasonable delay.
- If a company were to revise existing incident response policies and procedures to support a delayed materiality determination or delayed disclosure of an ongoing cybersecurity event, *e.g.*, extending the incident severity assessment deadlines, or changing criteria for reporting to management or board committees, that would constitute an unreasonable delay.

Adhering to normal internal practices and disclosure controls and procedures is sufficient to demonstrate good faith compliance.

Limited Filing Delay

There is a limited delay provision if disclosure poses a substantial risk to national security or public safety. A U.S. attorney general must determine that the disclosure poses a substantial risk to national security or public safety and notify the SEC in writing. Initially, disclosure may be delayed for a period determined by the attorney general, up to 30 days from when the disclosure would have been provided. The delay may be extended for an additional period of up to 30 days if the attorney general determines that disclosure continues to pose a substantial risk to national security or public safety, and again notifies the SEC in writing. In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the attorney general determines that disclosure continues to pose a substantial risk to national security and notifies the SEC in writing. After this, relief can only be granted by an SEC exemptive order.

Third-Party Systems

There is no exemption from providing disclosures about cybersecurity incidents on third-party systems used. The disclosure requirements are not limited to where an information system resides or who owns it. Depending on the facts, disclosure may be required by both the service provider and the customer, or by one but not the other. Registrants are only required to disclose based on the information available to them; registrants are not required to conduct additional inquiries outside of the regular channels of communication and complying with the registrant's controls and procedures. No safe harbor is provided for information disclosed about third-party systems.

"We do not believe a reasonable investor would view a significant breach of a registrant's data as immaterial merely because the data were housed on a third-party system, especially as companies increasingly rely on third-party cloud services that may place their data out of their immediate control."

For more details, see "Details on SEC's New Cybersecurity Disclosures."

Subsequent Clarifications

Form 8-K Item 1.05 vs. Item 8.01

On May 21, 2024, the Division of Corporation Finance issued a statement clarifying what should be disclosed in the newly created Item 1.05 in Form 8-K. Item 1.05 requires the disclosure of a cybersecurity incident "that is determined by the registrant to be material." It could be confusing for investors if companies disclose either immaterial cybersecurity incidents or incidents for which a materiality determination has not yet been made in Item 1.05.

A voluntary disclosure for a cybersecurity incident for which a materiality determination has not been made or an incident that was determined to be immaterial should be filed in Item 8.01.

If a company discloses an immaterial incident (or one for which it has not yet made a materiality determination) in Item 8.01, and then subsequently determines that the incident is material, it should file an Item 1.05 within four business days of the materiality determination. That Form 8-K may refer to the earlier Item 8.01 Form 8-K, but the company would need to ensure that the disclosure in the subsequent filing satisfies the requirements of Item 1.05.

If a cybersecurity incident is so significant that a company determines it to be material even though the company has not yet determined its impact, the company should disclose the incident in Item 1.05, including a statement that the company has not yet determined the incident's impact (or reasonably likely impact), and amend the Form 8-K to disclose the impact once that information is available. The initial Form 8-K filing should provide investors with information necessary to understand the material aspects of the nature, scope, and timing of the incident, notwithstanding the company's inability to determine the incident's impact (or reasonably likely impact) at that time.

Interaction with Regulation FD

On June 20, 2024, Erik Gerding, director of the Division of Corporation Finance, issued a statement about interactions with Regulation FD, which requires public disclosure of any material nonpublic information that has been selectively disclosed to securities market professionals or shareholders. Item 1.05 does not prohibit a company from privately discussing a material cybersecurity incident with other parties or from providing additional incident information beyond Item 1.05's requirements. These other parties could include vendors, customers, law enforcement, or national security agencies to assist with remediation, mitigation, risk avoidance efforts, or to facilitate those parties' compliance with their own incident disclosure and reporting obligations.

Nothing in Item 1.05 alters Regulation FD or makes it apply any differently to communications regarding cybersecurity incidents.

> *"There are several ways that a public company can privately share information regarding a material cybersecurity incident beyond what was disclosed in its Item 1.05 Form 8-K without implicating Regulation FD. For example, the information that is being privately shared about the incident may be immaterial, or the parties with whom the information is being shared may not be one of the types of persons covered by Regulation FD. Further, even if the information being shared is material, nonpublic information and the parties with whom the information is being shared are the types of persons covered by Regulation FD, an exclusion from the application of Regulation FD may apply. For example, if the information is being shared with a person who owes a duty of trust or confidence to the issuer (such as an attorney, investment banker, or accountant) or if the person with whom the information being shared expressly agrees to maintain the disclosed information in confidence (e.g., if they enter into a*

confidentiality agreement with the issuer), then public disclosure of that privately-shared information will not be required under Regulation FD."

SEC Compliance & Disclosure Interpretations (C&DIs)

On June 24, 2024, the SEC's Division of Corporation Finance issued five new C&DIs to address certain interpretative issues regarding cybersecurity incident reporting under Item 1.05 of Form 8-K where a company has made a ransomware payment. The new C&DIs address materiality determinations in instances where payments have been made to threat actors and remind companies that these decisions should take multiple factors into account. In brief, the C&DIs explain that:

- If a company experiencing a ransomware attack makes a payment that causes the cyberattack to end before a materiality determination is made, the company must still assess the materiality of the incident. In making the required materiality determination, a registrant cannot necessarily conclude that the incident is not material simply because of the prior cessation or apparent cessation of the incident. (Question 104B.05)
- If a company determines a ransomware attack is material and makes a payment that causes the attack to end before the company has reported the incident on Form 8-K, the company is not relieved of its requirement to report the incident. (Question 104B.06)
- If a company's cyber insurance policy covers the cost of a ransomware payment, this fact alone would not support a conclusion that the incident was immaterial. (Question 104B.07)
- The amount demanded or paid in a ransomware payment should not be the sole factor in assessing the materiality of an incident. (Question 104B.08)
- If a company experiences a series of ransomware attacks over time that are individually immaterial, it should consider whether any of those incidents were related, and if so, determine whether those related incidents, collectively, were material. (Question 104B.09)

Registrants should take all relevant facts and circumstances into consideration, which may involve consideration of both quantitative and qualitative factors, including both the immediate fallout and any longer-term effects on its organizational operations, finances, brand perception, or customer relationships, as part of its materiality analysis.

Conclusion

The assurance team at Forvis Mazars delivers extensive experience and skilled professionals to align with your objectives. Forvis Mazars works with hundreds of publicly traded companies in the delivery of assurance, tax, or consulting services, within the U.S. and globally. Our cybersecurity professionals bring a wide breadth of knowledge and strategies tailored to your industry to help you and your clients avoid interruptions and stay out of harm's way. For more information, visit forvismazars.us.

Contributor

Anne Coughlan

Director/Professional Services Group

anne.coughlan@us.forvismazars.com