Details on SEC's New Cybersecurity Disclosures

Cybersecurity incidents are becoming more sophisticated and frequent. To address this issue, on July 26, 2023, the SEC issued a final rule to enhance and standardize required cybersecurity disclosures for registrants. The amendments mandate:

- A Form 8-K filing within four business days after a company determines a cybersecurity incident[1] is material.[2] A limited delay would be permitted only if a U.S. attorney general determines there is a substantial risk to national security or public safety
- New Regulation S-K Item 106 will require the following annual disclosures on Form 10-K:
  - A registrant's processes for the assessment, identification, and management of material risks from cybersecurity threats[3] and whether any risks from cybersecurity threats, including any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant
  - The board of directors' oversight of risks from cybersecurity threats
  - Management's role in assessing and managing material risks from cybersecurity threats

The only relief provided to smaller reporting companies (SRCs) is a delayed effective date.

Background

Currently, there are no explicit disclosure requirements in Regulation S-K or S-X that include cybersecurity risks or incidents. The SEC has issued interpretive guidance in 2011 and 2018 highlighting how existing securities laws apply to cybersecurity risks and incidents when material.

[1] Cybersecurity incident means 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.

[2] In securities law, materiality is generally understood to be when there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the total mix of information made available.

[3] Cybersecurity threat means any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

The majority of registrants reporting material cybersecurity incidents do so in a Form 8-K, press release, or periodic report. Cybersecurity disclosure in SEC filings varies widely in the level of detail on the cause, scope, impact, and materiality of incidents. This disclosure may be blended with other unrelated items, making it difficult for investors to locate and analyze the information provided. The SEC also has observed a disturbing trend of cybersecurity incidents reported in the media but not disclosed in a registrant's filings.

New Form 8-K Disclosures

Registrants would be 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.

In a change from the proposal that required details about the cyber incident, 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 [emphasis added]." Companies should consider both qualitative and quantitative factors in assessing the material impact of an incident. Examples of qualitative factors noted in the final rule include harm to a company's reputation, 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:

- 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, changing criteria for reporting to management or board committees, that would constitute unreasonable delay.

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

Limited Filing Delay

The final rule includes a delay provision in cases where 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 SEC exemptive order.

The SEC has reached out to the U.S. Department of Justice to establish an interagency communication process to allow for the attorney general's determinations to be communicated to the SEC in a timely manner.

Third-Party Systems

The final rule provides no exemption from providing disclosures about cybersecurity incidents on third-party systems used. The final rule makes clear that the disclosure requirements are not limited to where an information system[4] resides or who owns them. 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."

Risk Management & Strategy

The final rule amends Regulation S-K to require registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy. The SEC significantly scaled back from the proposal's list of prescriptive disclosures to a description of the registrant's processes for assessing, identifying, and managing material

[4] Information systems means information resources, owned, or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

risks from cybersecurity threats in sufficient detail for a reasonable investor to understand the process. This should include, but is not limited to:

- Whether and how such cybersecurity processes have been integrated into the registrant's overall risk management system or processes
- Whether the registrant engages assessors, consultants, auditors, or other third parties for cybersecurity (Names are not required.)
- Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider

The final rule also requires 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, and if so, how.

Governance

These amendments have been significantly scaled back from the proposal. The final rule requires only a description of the board's oversight of risks from cybersecurity threats and identification of any board committee or subcommittee responsible for oversight and the processes by which the committee is informed about such risks.

Registrants should consider disclosing the following as part of a description of management's role in assessing and managing the registrant's material risks from cybersecurity threats:

- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of the person or group in order to fully describe the nature of the expertise
- The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents
- Whether such persons or committees report information about such risks to the board of directors or a board committee or subcommittee

Conclusion

FORVIS works with hundreds of publicly traded companies in the delivery of assurance, tax, or advisory services within the United States and globally. For more information, visit forvis.com.

Contributors

Raymond Baxter
Director / IT Risk and Compliance
ray.baxter@forvis.com

Anne Coughlan
Director / National Office
anne.coughlan@forvis.com