Cybersecurity Disclosures - SEC's New Promulgation

By: Josef Rashty, CPA

Internet is now an integral part of our business activities; however, it also poses a host of challenges, including cybersecurity risks. The SEC issued its new rules on cybersecurity that went into effect in September 2023, with enforcement that began in December 2023. The SEC aims its cybersecurity rules at publicly listed companies; however, most public companies are reliant on many smaller third-party software and supply chain companies, and a cyberattack at any point along that chain may have a material impact on their operations. Therefore, such third-party companies – whether public or not – should also familiarize themselves with the new regulations.

In July 2023, the SEC Release No. 33-11216, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (rule or promulgation), applies to all public business entities (PBEs) subject to the Securities Exchange Act of 1934, including foreign filers (except Canadian foreign private issuers that file Form 30-F and asset-backed securities issuers). Private companies who plan an initial public offering (IPO) may also adopt the SEC promulgation voluntarily. This article expounds on the implications of the new rules.

SEC's New Guidance

The final SEC rule establishes new requirements for the following:

- Material cybersecurity incidents, which companies need to disclose on Form 8-K within four business days. A registrant may delay filing the Form 8-K if the U.S. Attorney General "determines immediate disclosure would pose a substantial risk to national security or public safety."
- Annual disclosures in Form 10-K about (1) cybersecurity risk management and strategy, (2) "management's role in assessing and managing material risks from cybersecurity threats" and (3) "the board of directors' oversight of cybersecurity risks."
- The presentation of disclosures in Inline eXtensible Business Reporting Language (Inline XBRL).

Form 8-K

The SEC's guidance requires that PBEs report material cybersecurity incidents on Form 8-K within four days after reckoning that the cybersecurity incident was material. Companies can defer from filing a material cybersecurity incident (for up to 90 days in two consecutive deferrals) if the U.S. Attorney General determines that disclosure may pose a substantial risk to national security or public safety.

This guidance implies that the PBEs cannot delay their Form 8-K filing due to internal or external law enforcement investigations.

Form 10-K

The SEC's guidance created Item 106(b) of Regulation S-K to require disclosure about a registrant's risk management and strategy.

The promulgation requires that registrants disclose their cyber risk management system in their Form 10-Ks in sufficient detail and simple language. The disclosures should identify, assess and manage any material risks from cybersecurity threats. Registrants should also describe whether any risk from cybersecurity threats has materially affected or is reasonably likely to affect their operations.

The rule also created Item 106(c)(1) of Regulation S-K, which requires the registrants to disclose the board of directors' oversight of cybersecurity risks. The disclosure should include the processes of the communication with the board committee or subcommittee responsible for overseeing the process.

Registrants should describe the board of directors' oversight of risks from cybersecurity threats. If applicable, companies must identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks. In addition, companies must describe management's role in assessing and managing the company's material risks from cybersecurity threats, with such disclosure addressing, as applicable.

As noted by the SEC, many companies currently address cybersecurity risks and incidents in the risk factor sections of their filings, and risk oversight and governance are often addressed in companies' proxy statements. However, the new rule requires

disclosures to appear in a newly designated Item 1C in Part I of the Form 10-K and does not allow the disclosures to be incorporated from the proxy statement.

Companies should review their risk factor and proxy statement disclosures when drafting the new discussions of cybersecurity risk management, strategy and governance to maintain consistency with the company's past public statements regarding its cybersecurity risks governance and processes and to assess how those disclosures may be conformed or enhanced going forward.

Most likely, companies will continue to include disclosure of cybersecurity governance in their proxy statements and, therefore, should be mindful that they are using terminology consistently across the documents. Furthermore, they should consider whether they need to repeat their Form 10-K disclosures in their proxy statement disclosure.

Companies should note that beginning this year, Form 10-K should be tagged in iXBRL (block text tagging for narrative disclosures and detail tagging for quantitative amounts).

Scope of Disclosure

The SEC's final rule focuses on the material aspects of the incident and material impacts on the company. The guidance provides registrants with some flexibility: For example, Item 1.05 states that companies "need not disclose specific or technical information" about the incident "in such detail as would impede" response or remediation of the cybersecurity incident.

Cybersecurity Risk Management, Strategy and Governance

The SEC's final rule introduces new Item 106 of Regulation S-K, which requires a description in the Form 10-K of a company's processes, if any, for assessing, identifying and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. Item 106 states that in providing such disclosure, a company should address, as applicable, the following non-exclusive list of disclosure items:

- Whether and how the registrant has integrated its cybersecurity processes into its overall risk management system
- Whether the registrant engages assessors, consultants, auditors or other third parties in connection with its cybersecurity processes
- Whether the registrant has processes to oversee and identify risks from cybersecurity threats associated with the engagement of any third-party service provider

Companies must also describe 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 company, including its business strategy, results of operations, or financial condition, and if so, how.

Materiality

The definition of materiality in the SEC guidance is consistent with the federal securities laws and numerous court cases. The Supreme Court deems information to be material if there is a "substantial likelihood that a reasonable investor would consider it important" or if it would have "significantly altered the 'total mix' of information made available." There is often a high degree of judgment in making a materiality determination. Companies should analyze quantitative and qualitative factors and evaluate the cybersecurity incident and its reasonably likely impacts – for example, qualitative factors include harm or potential harm to a registrant's reputation, competitiveness, or customer and vendor relationships.

Ransomware

Cyberattack criminals often use a malware that they implement in companies' hardware that prohibits their access to their files. Cybercrime encrypts companies' files and demands a ransom payment for the decryption key. The criminals often place organizations in a position where paying the ransomware is the easiest and cheapest way to regain access to their files, even though the Federal Bureau of Investigation (FBI) guidance does not support paying ransom to hackers.

The spirit of the SEC guidance requires that victims of cyberattacks disclose the amount of paid ransomware to cybercriminals. However, companies often refrain from disclosing this information, fearing that such an admission could bring them legal and reputational risks. For example, the casino operators Caesar Entertainment did not disclose payment to hackers after a cyberattack late last summer. (On Sept. 22, 2023, The Wall Street Journal reported that the company had paid the $30 million ransom that hackers demanded.)

Effective Dates

The SEC's final rules become effective 30 days following publication of the adopting release in the Federal Register. The SEC's rule-effective dates of compliance are as follows:

Smaller Reporting Companies

Form 8-K reporting	June 15, 2024
Form 10-K reporting for fiscal years ending on or after:	Dec. 15, 2023

All Other Registrants

Form 8-K reporting	Dec. 18, 2023
Form 10-K reporting for fiscal years ending on or after:	Dec. 15, 2023

Therefore, smaller reporting companies have an additional 180 days before they begin providing the Form 8-K disclosures.

Regulation S-K, Item 10(f)(1), defines a *smaller reporting company* as a registrant that has a public float of less than $250 million, as well as companies with less than $100 million in annual revenues in the previous year and no public float or a public float of less than $700 million. (A public float is the multiplication of the number of the registrant's shares held by non-affiliates by the market price.)

Final Remarks

Corporate lawyers, chief financial officers and security chiefs are wrestling with how much information to report about cyberattacks under the new SEC guidance. Their concerns are potential lawsuits and the possibility of more cybersecurity hacks.

Some registrants have complained about the 8-K four-day reporting window and the difficulty of determining what constitutes materiality, but most security chiefs believe that larger companies are already complying with what the SEC rule mandates, at least for annual reporting purposes. It appears that the consensus is that the SEC rule will bring much-needed transparency to cybersecurity matters.

About the Author

Josef Rashty, CPA, Ph.D. (Candidate), has received his master's in accounting from Oklahoma State University and provides consulting services in Silicon Valley. He can be reached at *j_rashty@yahoo.com*.