WILMERHALE

SEC Issues New Guidance on Disclosing Cybersecurity Risks and Incidents

2011-10-27

On October 13, 2011, the Securities and Exchange Commission's (SEC) Division of Corporation Finance issued guidance on disclosure obligations relating to cybersecurity risks and cyber incidents.[1] The guidance, which is effective immediately, applies to domestic and non-US SEC registrants. It is intended to assist registrants in preparing disclosures under both the Securities Act of 1933 and the Securities Exchange Act of 1934.[2]

At the outset, the guidance explains that cyber incidents can occur when a company experiences an unintentional loss of data or a deliberate attack on its computer networks, and cautions that incidents can result in the loss of sensitive data, the corruption of important files, or even the disruption of company operations. The guidance notes several types of negative consequences public companies may confront in the wake of a cyber incident, including remediation costs, costs of increased cybersecurity protection measures, lost revenues, litigation costs, and reputational damage.

The guidance then explains that even though no rules explicitly address this topic, cyber incidents and the risk of such incidents may nevertheless give rise to disclosure obligations under current SEC rules. In light of the damage that a cyber incident can cause as well as existing obligations to disclose information that a "reasonable investor would consider important to an investment decision," registrants may be required to provide information that allows investors to understand the nature of a company's particular cybersecurity risks. Moreover, registrants may also need to disclose material information regarding specific cybersecurity risks and cyber incidents when such information is necessary to "make other required disclosures, in light of the circumstances under which they are made, not misleading."

Finally, the guidance outlines several particular areas where existing disclosure obligations may require companies to discuss cybersecurity risks and cyber incidents. Each area is described below:

Investment Risk Factors

The SEC guidance recommends that companies disclose cybersecurity risks and incidents as "risk factors" if such risks and incidents are "among the most significant factors" that make an investment in the company speculative or risky. Companies should take into account prior incidents, the severity and frequency of the incidents, the probability of future incidents, and potential costs or consequences. Costs of relevant preventative measures should be included in this analysis as well.

The SEC also notes that disclosures must be made in terms specific to the particular registrant, rather than in generic language. It provides the following examples of what an appropriate disclosure may include:

- "Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- "To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- "Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- "Risks related to cyber incidents that may remain undetected for an extended period; and
- "Description of relevant insurance coverage."

Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)

Regarding MD&A disclosures, the guidance recommends that registrants disclose cybersecurity risks and cyber incidents if costs or consequences associated with "one or more known incidents or the risk of potential incidents" would materially affect operational results, liquidity, financial condition, or would cause financial information not to be necessarily indicative of future operating results. For example, an attack that resulted in the theft of intellectual property might lead to reduced revenues, increased costs of litigation, or increased cybersecurity protection expenditures. The amount and duration of those costs should be included if material.

Description of Business

If a cyber incident affects a registrant's products, services, competitive conditions, or relationships with customers or suppliers, the guidance counsels registrants to disclose those incidents and any potentially material impact on the company.

Description of Legal Proceedings

If a material legal proceeding pertains to a cyber incident, such as material litigation arising from the loss of important customer information, the registrant is expected to explain the cyber incident and the associated claims allegedly arising from the incident as part of the "legal proceedings" section

in its disclosure.

Financial Statement Disclosures

The SEC recommends that registrants consider how cybersecurity risks and cyber incidents would affect financial statement disclosures under relevant accounting standards, both prior to an incident as well as during and after an incident. Prior to a cyber incident, registrants should consider accounting for the capitalization of costs incurred to prevent cyber incidents. During and after an incident, registrants should consider accounting for any incentives the company has offered to maintain business relationships with customers following the incident, and for contingent losses from asserted and unasserted claims against the company. The SEC notes that cyber incidents might result in diminished future cash flows, thereby requiring consideration of impairment of certain assets. The SEC notes that this may require the use of estimates. The SEC reminds its registrants that they must reassess the estimates periodically and advises companies to explain any risk or uncertainty of a reasonably possible change in estimates that would be material to the financial statements. Similarly, companies should also state whether potential changes in the estimates would be material to the financial statements. If a cyber incident occurs after the balance sheet date but before the issuance of financial statements, the SEC recommends that registrants evaluate whether to include disclosure of a recognized or unrecognized subsequent event in addition to any information related to such a disclosure.

Disclosure Controls and Procedures

Finally, the SEC guidance advises registrants to consider whether the cybersecurity risk or cyber incident might affect disclosures relating to disclosure controls and procedures themselves, such as if the incident affects the registrant's ability to record, process, summarize, and report any information required in any of its filings.

Conclusion

The SEC's guidance highlights the importance of cybersecurity not only as an issue for companies and their customers, but also for investors and the economy as a whole. Senator Rockefeller, pleased about the SEC's response to his earlier request, said the guidance "fundamentally changes the way companies will address cybersecurity in the 21st century."[3] Companies should evaluate their current cybersecurity-related disclosure practices to ensure these practices are consistent with the new guidance.

---

[1] Securities and Exchange Commission, CF Disclosure Guidance, Topic No. 2: Cybersecurity (Oct. 13, 2011), www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[2] In May 2011, Senator Jay Rockefeller (D-W.Va.), Chairman of the Senate Commerce Committee,

and four other Senators sent a letter to the SEC asking the Commission to clarify corporate disclosure requirements for cybersecurity-related incidents, quoting statistics from a 2009 survey concluding that 38 percent of Fortune 500 companies had made a significant oversight in their public filings by not discussing privacy and data security events. Letter from Sen. Jay Rockefeller and others to Securities and Exchange Commission Chairman Mary Schapiro (May 11, 2011), commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e.

[3] Rockefeller Says SEC Guidance Fundamentally Changes the Future of Cybersecurity (Oct. 13, 2011), commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=4acbf0d1-7695-4fd8-be64-b950da8f1372.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195