LexisNexis® Emerging Issues Analysis

Marc J. Lederer on

The SEC'S Division of Corporate Finance Provides Guidance on the Obligations of Public Companies to Disclose Cybersecurity Risks and Attacks

2012 Emerging Issues 6204

Click here for more Emerging Issues Analyses related to this Area of Law.

On October 13, 2011, the Division of Corporate Finance of the Securities and Exchange Commission ("SEC") published guidance (the "Guidance")[1] recommending that public companies[2] evaluate whether they may need to disclose cybersecurity risks and attacks[3] in their SEC filings. Specifically, the Guidance provides that public companies should consider if such disclosures, when applicable, should be included in the Risk Factors, Management's Discussion and Analysis of Financial Condition and Results of Operations ("MD&A"), Description of Business, Legal Proceedings, Financial Statement Disclosures and/or Disclosure Controls and Procedures Sections of their SEC filings.

Recommendations for Disclosures to Be Made by Public Companies Related to Cybersecurity

Although no existing securities disclosure requirement explicitly refers to cybersecurity risks and incidents, because a public company is required to provide material information that a reasonable investor would consider important to making an investment decision and refrain from making any disclosures that might be considered misleading,[4] operational and financial risk disclosures may need to include discussions related to cybersecurity.

---

1. http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm#_edn2

2. The Guidance states that it is intended to assist registrants in preparing disclosure required in registration statements under the Securities Act of 1933 and periodic reports under the Securities Exchange Act of 1934.

3. "Cybersecurity" is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access. http://whatis.techtarget.com/definition/cybersecurity.htm. Cyber attacks include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites.

4. Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9; see Securities Act Section 17(a), Exchange Act Section 10(b), and Exchange Act Rule 10b-5.

Marc J. Lederer on

The SEC'S Division of Corporate Finance Provides Guidance on the Obligations of Public Companies to Disclose Cybersecurity Risks and Attacks

Risk Factors Section

The Guidance recommends that a public company make a determination as to whether its risk factors disclosure should contain a discussion of cybersecurity risks and incidents. In determining whether such disclosure would be required, a public company should consider the following factors:

1) whether there have been prior cyber incidents and the severity and frequency of those incidents;

2) the probability that cyber incidents will occur, and the likely quantitative and qualitative magnitude of such potential incidents, including the costs and other consequences that would result from misappropriation of assets or sensitive information, corruption of data or operational disruption; and

3) the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which such company operates and risks to that security, including threatened attacks of which it is aware.

The Guidance states that if a public company concludes that it should discuss cybersecurity in its risk factors disclosure, then appropriate disclosures may include the following:[5]

1) a discussion of aspects of the public company's business or operations that give rise to material cybersecurity risks and potential costs and consequences;

2) to the extent the public company outsources functions that have material cybersecurity risks, a description of those functions and how the public company addresses those risks;

3) a description of cyber incidents experienced by the public company that are individually, or in the aggregate, material, including a description of the resulting costs and other consequences;

---

5. The Guidance advises public companies to avoid generic or "boilerplate" disclosures, and instead tailor their disclosures to the particular facts and circumstances.

4) risks related to cyber incidents that may remain undetected for an extended period; and

5) a description of relevant insurance coverage.

MD&A Section

The Guidance recommends that a public company address cybersecurity risks and incidents in its MD&A section if the "costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition." If it is reasonably likely that such attacks will lead to reduced revenues or increased costs, then the disclosures should include the amount and duration of the lower revenues and higher costs, if material.

Description of Business Section

The Guidance also advises public companies that if one or more cyber incidents materially affect such a company's products, services, relationships with customers or suppliers, or competitive conditions, the incident and the potential impact should be discussed in the "Description of Business" section.

Legal Proceedings

The Guidance advises that if a public company or any of its subsidiaries is a party to a pending material legal proceeding involving a cyber incident, the company should address the situation in its "Legal Proceedings" disclosure.

Financial Statement Disclosures

The Guidance notes that cybersecurity risks and incidents may have a broad impact on a public company's financial statements, depending on the nature and severity of the actual or potential incident, and that financial statements may need to take into account the costs incurred in preventing a cyber incident. In addition, financial statements may need to address costs incurred during and after a cyber incident, such

as costs incurred to mitigate damages from a cyber attack, losses from asserted and unasserted claims, as well as losses in the form of future diminished cash flows.[6]

Disclosure Controls and Procedures

As part of a public company's obligations to disclose its conclusions as to the effectiveness of its disclosure controls and procedures, the Guidance recommends that consideration be given to the risk that cyber incidents may pose to such company's ability to record, process, summarize, and report information that is required to be disclosed in SEC filings.

Practical Implications

Public companies should carefully consider whether cybersecurity risks and incidents should be disclosed in accordance with the Guidance. It would be advisable for public companies to have a written procedure for evaluating whether such disclosures are necessary based upon their previous cyber incidents and their impact, as well as the current state of their data security systems and procedures. Already there have a been a variety of ways that public companies have started to address cybersecurity risks in their filings with the SEC. However, this should come as little surprise since the Guidance is still fairly new and companies may have had very different experiences with cybersecurity threats and incidents. It should be noted that the SEC staff cautions public companies against revealing so much detail in their disclosures that it could inadvertently compromise their cybersecurity efforts, i.e. by inadvertently providing a road map to hackers for exploiting a company's data security weaknesses. In discussions with the SEC staff they have indicated they would encourage public companies seeking additional guidance to discuss cybersecurity disclosures with them in advance of their filings. Should the SEC question the adequacy of cybersecurity disclosures in a company's filings, the general practice of the SEC would be to address those concerns during the comment period, allowing companies the opportunity to respond to any such comments. Public companies should also note that

6. The Guidance provides that public companies should consider whether disclosure of a recognized or nonrecognized subsequent event is necessary if a cyber incident is discovered after the balance sheet date but before the issuance of financial statements. For a material nonrecognized subsequent event, the financial statements should disclose the nature of the incident and an estimate of its financial effect, or a statement that such an estimate cannot be made.

other regulations and rules, such as the SEC's Regulation S-P[7] and the numerous state and international privacy and data security laws and regulations[8], may also impose obligations related to cybersecurity.

Click here for more Emerging Issues Analyses related to this Area of Law.

About the Author. ***Marc J. Lederer*** *is a privacy law attorney at Willkie Farr and Gallagher LLP in New York, NY. He regularly counsels clients on privacy and data security issues. Mr. Lederer advises financial institutions as to compliance with the numerous federal, state, and international privacy and data security laws. Mr. Lederer can be reached by phone at 212-728-8624 or by email at mlederer@willkie.com.*

7. 17 CFR Part 248.

8. The European Commission Data Protection Directive 95/46 is an example of such an international law, and Massachusetts Rule 201 CMR 17.00 and Connecticut Public Act 08-167 are examples of such state laws and regulations.