INSIGHTS

A Cyber Incident Moves Pretty Fast, If You Aren't Ready To Respond, You Might Blow It

February 26, 2018

The Securities and Exchange Commission (SEC) expanded its warnings to public companies that generic disclosures identifying cybersecurity risk factors may be insufficient. Rather, the SEC seems to expect companies to conduct careful inward assessments that identify unique strengths and weaknesses, and that disclosures should be tailored to that assessment. Additionally, senior leadership should be included in developing response plans that go well beyond addressing technology risks. An effective response plan should include internal directions for managing incident disclosure and trigger internal controls to prevent the violation of other securities laws like those against insider trading. This advice comes in a new "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," ("Guidance") issued on February 21, 2018, that expands on staff-level guidance from 2011. While not itself a rule or regulation, the Guidance represents the Commission's interpretation of federal securities laws and regulations as applied to cybersecurity risks and incidents.[1]

One of the most basic points in the Guidance is that cyber-related risks and incidents should be promptly disclosed. The Commission says it is "critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack."[2] It also stresses the importance of establishing effective disclosure controls and procedures to ensure an accurate and timely response after a company learns of an incident. In particular, the Commission believes that the development of controls and procedures is "best achieved" when a company's leadership "are informed about the cybersecurity risks and incidents that the company has faced or is likely to face."[3]

To determine what cybersecurity risks and incidents must be disclosed, companies should consider the potential materiality of any identified risk and, in the case of incidents, the importance of compromised information and the impact of the incident on company operations. The materiality of cybersecurity risks or incidents generally depends upon their nature, extent, potential magnitude, and range of harm that such incidents could cause. And while the SEC recognizes that ongoing investigation of an incident may affect the scope of disclosure, an ongoing internal or external investigation does "not on its own provide a basis for avoiding disclosures of a material cybersecurity incident."[4] Further, when cybersecurity-related disclosure is warranted, the SEC expects companies to avoid generic disclosure and instead provide specific information tailored to their particular risks and incidents.

The Commission also underscored the applicability of insider trading prohibitions to cybersecurity incidents and encouraged companies to consider preventative measures. Directors, officers, and other corporate insiders "must not trade a public company's securities while in possession of material nonpublic information," including knowledge of a significant cybersecurity incident experienced by the company.[5] Companies and their leaders are encouraged to consider, before an incident occurs, how internal policies and procedures might prevent trading—or even the appearance of trading—on the basis of material nonpublic information related to cybersecurity risks and incidents.

Some commissioners suggested that the Guidance should be more detailed and include additional expectations, including potential disclosure requirements about (1) a company's protocols relating to cybersecurity risks and its capacity, and any measures taken, to respond to cybersecurity incidents; (2) whether a particular cybersecurity incident is likely to occur or recur; or (3) how a company is prioritizing cybersecurity risks, incidents, and defense.[6] Voluntary disclosures along those lines may be prudent, and subsequent guidance is likely forthcoming, but for now the Commission's message is clear: companies and their leaders should not wait until a cyber-related incident occurs to plan their response. A bungled response can turn even a minor cyber incident into a major liability. To reduce regulatory and market risks, public companies should assesse their unique cybersecurity risks, involve leaders in developing post-incident policies and procedures to comply with securities laws; and promptly make tailored disclosures when warranted.

---

[1] *SEC Interpretive Releases*, Sec. & Exch. Comm'n, ***https://www.sec.gov/rules/interp.shtml*** ("The Commission occasionally provides guidance on topics of general interest to the business and investment communities by issuing 'interpretive' releases, in which we publish our views and interpret the federal securities laws and SEC regulations.").

[2] Guidance at 4.

[3] Guidance at 4.

[4] Guidance at 12.

[5] Guidance at 4-5.

[6] *Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Sec. & Exch. Comm'n (Feb. 21, 2018), ***https://www.sec.gov/news/public-statement/statement-stein-2018-02-21***.