Banking Law

December 6, 2011

Cybersecurity and the Public Company: Keeping Your Disclosures Safe and Sound After Cyber Monday

Author: Craig D. Miller

Click here if you would like to have your personal financial information compromised and your credit card numbers shared with criminals around the world.[1] Such are the implicit invitations many of us receive on a regular basis from emails purporting to represent our credit card companies, financial institutions, customers and business partners. Unfortunately, too many unsuspecting individuals do "click here" and too many criminals are trying to compromise the digital technology we have all faithfully put our trust in over the last two decades.

For many public companies, the risks associated with cybersecurity[2] have increased, and the attendant disclosure of those risks has become an important area of focus in periodic reports filed under the Securities Exchange Act of 1934, as amended (the Exchange Act). As companies begin the preparation of their year-end periodic reports, they are cautioned to closely review the Securities and Exchange Commission's (SEC's) recent guidance on disclosure obligations relating to cybersecurity risks and cyber incidents.[3]

The Nature of an Attack and Its Impact

A cyber incident can take a number of forms, including operational disruption, misappropriation of personal information, denial-of-service attack and data corruption. Insiders with a public company can cause a cyber incident just as well as outsiders. The impact of such an incident can be significant, including increased costs associated with addressing the incident on both a system basis and a personnel basis, lost revenues as a result of customer disaffection, reputational loss, and the onset of new litigation. For securities law purposes, a reasonable investor would consider the impact of a cyber incident important in making an investment decision on whether or not to invest in certain public companies. Accordingly, public companies must carefully evaluate the risks associated with cyber incidents in fulfilling their disclosure obligations.

Where Are the Disclosure Obligations Relating to Cybersecurity?

Although public companies are not subject to specific cybersecurity disclosure obligations, the SEC has identified a number of existing areas of the securities laws that may necessitate the disclosure of both cyber incidents and the accompanying cybersecurity risks.

First and foremost, public companies must disclose the risk of cyber incidents "if these issues are among the most significant factors that make an investment in the company speculative or risky." [4] Each registrant must evaluate both the impact prior cyber incidents have had

Newsletter Editors

Katerina H. Bohannon
Partner
Email
650.812.1364

Harold P. Reichwald
Partner
Email
310.312.4148

Practice Area Links

Practice Overview
Members

Author

Craig D. Miller
Partner
Email
415.291.7415

on the company and the impact a potential cyber incident may have on the company going forward. Executives should ask themselves what the costs associated with a successful cyber incident would be on their business and the consequences such an effective cyber incident could have. For those companies that have experienced a successful material cyber attack, the mere disclosure of the hypothetical risk associated with a cyber incident may not be sufficient. Instead, such companies may need to disclose the nature of the actual, specific attack and the impact of such an attack.

Management's discussion analysis of financial condition and results of operations is another area where disclosure of cybersecurity risks and cyber incidents may be appropriate if the impact or effects associated with a particular cyber incident or the threat of a cyber incident "represent[s] a material event, trend or uncertainty that is reasonably likely to have a material effect on . . . results of operations, liquidity or financial condition . . ." As an example, if a particular cyber incident will decrease revenues and increase costs (including litigation costs), a public company may need to disclose the impact of such an incident in MD&A .

Other areas where disclosure of cyber incidents and/or the costs associated with protecting against such incidents may be appropriate include financial statement disclosures (disclosures of loss contingencies and the impairment of intangible assets) and, depending on the timing of a cyber incident, appropriate subsequent event disclosure.

Remembering the Context

With the evolving technological landscape and ever-increasing dependence on technology as the engines of many businesses, public companies must review the importance of cybersecurity in keeping their businesses safe and remember that investors will rely on disclosure for adequately assessing the attendant risk associated with cyber incidents on an operating business. Effective disclosure can't mitigate the risk associated with an actual cyber attack but can mitigate the risk of successful claims of failing to comply with securities disclosure obligations.

---

[1] OK. You can just continue reading the article instead.

[2] The SEC defines "cybersecurity" as the body of technology, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access.

[3] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[4] Id.

Unsubscribe