Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

SEC Continues To Target Cybersecurity Disclosures

Law360, New York (November 01, 2013, 12:51 PM ET) -- Over the past two years, the U.S. Securities and Exchange Commission's Division of Corporation Finance (Corp Fin) has highlighted the importance of cybersecurity disclosures in filings with the SEC. Corp Fin's initiative appears likely to stay steady and even to escalate. Proper attention to cybersecurity disclosures can help a company avoid a comment letter on this issue from Corp Fin and decrease the likelihood of facing a securities class action or shareholder derivative action, or both, in the wake of a cyber attack or data breach.

Corp Fin's Disclosure Guidance

With cybersecurity garnering more attention, in October 2011 Corp Fin issued "disclosure guidance" regarding cybersecurity disclosures.[1] Corp Fin stated that its intent was to assist companies "in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each company's specific facts and circumstances."

Corp Fin acknowledged that no "existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents," but stated that (1) various disclosure requirements may impose an obligation to disclose cybersecurity risks and incidents, and (2) material information about cybersecurity risks and incidents could be required to be disclosed to make other required disclosures not misleading. Corp Fin advised companies to review the adequacy of their disclosures on these topics "on an ongoing basis."

In an Oct. 15, 2013, speech to the National Association of Corporate Directors Leadership Conference, SEC Chairwoman Mary Jo White referred to cybersecurity as "a hot topic from many perspectives."[2] Chairwoman White stated that, "even in the absence of a line item requirement" in the disclosure rules regarding cyber attacks, the materiality standard governs disclosures about such attacks. As Chairwoman White put it: "Depending on the severity and impact of the cybersecurity attacks, disclosure is either required or not."

Corp Fin has signaled that it is not looking for boilerplate in the risk factors or for one-size-fits-all disclosures. The guidance encourages companies to look not only at their disclosures of "risk factors," but also at management's discussion and analysis of financial condition and operations, the description of the business, the description of legal proceedings and financial statement disclosures.

The disclosure guidance implicitly assumes that all or most companies face cybersecurity risks and possibly even that all or most companies have been attacked, as the guidance advises that companies "should not present risks that could apply to any issuer," refers to disclosing "successful" or "material" attacks rather than all attacks, and states that companies should "avoid generic risk factor disclosure."

Instead of generic disclosures, the guidance advises that a company's disclosures may include discussion of particular aspects of the business that give rise to material cybersecurity risks and their potential costs and consequences; the material cybersecurity risks associated with outsourcing functions and how the company is addressing those risks; a description of individual or aggregated cyber incidents that are material; the risks of cyber incidents that may remain undetected for an extended period; and a description of relevant insurance coverage.

The guidance recognizes the tension between providing sufficient disclosure "to allow investors to appreciate the nature of the risks faced by the particular registrant" and not disclosing information "that itself would compromise a registrant's cybersecurity." Corp Fin did not provide any bright line dos or don'ts for resolving this tension. It did, however, "reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity."

The guidance's reference to the "nature of the risks" appears to contemplate disclosure of which aspect of the business a cyber attack might target (e.g., millions of consumer financial accounts), but not a description of a particular security risk (i.e., that there are recurring security issues with the XYZ servers that hold customer account information).

The Disclosure Guidance in Practice

Corp Fin stated that the guidance reflects only its views on cybersecurity disclosures, that it is not a rule, regulation or statement of the SEC, and that the commission has neither approved nor disapproved the guidance. But the guidance is no mere academic piece.

Corp Fin has issued comments to approximately 50 companies about cybersecurity since it issued the disclosure guidance.[3] These comments reflect the Staff's sustained interest in the topic, encouraging disclosures that go beyond a rote warning that a cyber problem could have some type of adverse impact on the business.

For example, Corp Fin asked a company that referred to cyber attacks as "unlikely" to review the disclosure guidance and consider revising the statement, and to describe for Corp Fin what consideration it gave to its disclosures. Another company, which had disclosed what "could" happen from a cyber attack, was asked to disclose whether it had experienced "any security breaches, cyber attacks or other similar events in the past." And a company in the construction materials business that noted it was subject to cybersecurity risks was asked to describe what consideration it had given to the disclosure guidance.

In describing Corp Fin's efforts on cybersecurity disclosures in a letter earlier this year to Sen. Jay Rockefeller, D-W.Va., Chairwoman White stated that Corp Fin is continuing "to prioritize this important matter in its review of public company disclosures."

Cybersecurity Litigation Risks

It may be just a matter of time before two factors align: (1) news of a successful cyber attack that sends a company's share price plunging, and (2) the company's public statements about its cyber defenses appear in hindsight (at least to a plaintiff's attorney) to have been clearly erroneous. When this happens, the company and its officers and directors likely will find themselves named in one or more complaints asserting securities, fiduciary duty and other claims on behalf of a class, derivatively or both.

The strict pleading requirements of the Private Securities Litigation Reform Act of 1995 should bar any securities complaint that does not plead facts supporting a strong inference of fraud. However, winning a dismissal could take one or two years and cost hundreds of thousands of dollars. If the complaint survives the motion to dismiss and reaches the expensive open waters of discovery, defense costs could be in the millions of dollars.

A derivative claim, alleging that officers and directors breached their fiduciary duties, is another type of claim that could follow a cyber attack or breach. In such a claim, a shareholder likely would allege that the defendants violated their duty of care and, if any defendants sold shares before the attack occurred or before the risk was fully disclosed to the corporation, they violated the duty of loyalty by profiting from the sale of those shares.

The linchpin of the duty of care claim would be that the officers and directors failed to exercise proper oversight, allowing vulnerabilities to go unfixed and ultimately exploited. This would be what is known as a Caremark claim,[4] one that the Caremark court called "possibly the most

difficult theory in corporation law upon which a plaintiff might hope to win a judgment." This difficulty has not stopped many a plaintiff from trying. Another potential claim would be that the directors purportedly breached a "duty of disclosure," a claim that has been made in recent cases targeting say-on-pay votes and approvals of increases in shares for equity plans.

The quality of the company's cybersecurity disclosures could be important to deter or defeat such claims. Management should make sure that the company's cybersecurity disclosures and public statements are made with as much care as the typically well-vetted statements regarding financial results, growth prospects and unique business risks.

The Directors' Oversight Role

Directors, of course, are not expected to write code to block hackers. In performing their oversight role, directors should work in good faith to stay informed about the corporation's cybersecurity defenses and the process by which management builds and maintains those defenses. In satisfying themselves that management is taking due care on cybersecurity issues, directors should consider whether management has reported on topics like the following:

- What are the typical and worst-case risks, how were those identified, what is the company doing to defend against them, and what are the contingency plans in case an attack succeeds?

- Is management deferring recommended security measures? If so, why?

- If the company is experiencing recurring types of attacks, is that normal? Or does it indicate that the company is perceived as particularly or uniquely vulnerable, and is that perception correct?

- Have attacks succeeded or almost succeeded, and to what effect? What vulnerabilities did they reveal, and have the necessary corrections been made?

These matters might be delegated to an appropriate board committee, with the committee or management reporting to the full board periodically and as circumstances warrant.

Looking Ahead

In April 2013, Sen. Rockefeller asked Chairwoman White to elevate Corp Fin's guidance to commission-level guidance.[5] Chairwoman White responded that she has asked the staff to brief her on current disclosure practices and to provide any recommendations it has regarding further action in this area, leaving the door open to further pronouncements by the SEC.

The degree of disclosure that Corp Fin, or the commission, will require on cybersecurity is still evolving, but the past two years clearly signal that Corp Fin, with the chairwoman's support and with congressional encouragement, is going to give cybersecurity disclosures careful attention for the foreseeable future.

--By Anthony Rodriguez, Morrison & Foerster LLP

Tony Rodriguez is a partner in Morrison & Foerster's San Francisco office.

advice.

[1] http://www.sec.gov/divisions/Corp Fin/guidance/cfguidance-topic2.htm

[2] http://www.sec.gov/News/Speech/Detail/Speech/1370539878806#.UmaAW1NdDsY

[3] http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=7b54b6d0-e9a1-44e9-8545-ea3f90a40edf

[4] In re Caremark Int'l, Inc., Deriv. Litig., 698 A.2d 959 (Del. Ch. 1996).

[5] http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51