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

Cybersecurity And The SEC: Disclosure Tips

Law360, New York (February 24, 2012, 1:37 PM ET) -- Headlines about cyberattacks and data security breaches are becoming distressingly commonplace. In 2011, cyberattackers targeted retailers, online sellers and financial firms to steal customer data and technology, life science companies to steal intellectual property, and corporate websites to disrupt operations and corrupt data.

In response to the increase in cybersecurity breaches, and at the request of members of Congress, the staff of the U.S. Securities and Exchange Commission's Division of Corporate Finance recently issued CF Disclosure Guidance: Topic No.2 — Cybersecurity.

The cybersecurity guidance did not pronounce new rules or create new disclosure obligations, but rather outlined how the SEC considers cybersecurity risks to apply to existing public disclosure obligations, including the obligation to evaluate and disclose to investors risk factors that are likely to have a material effect on the company's financial results. Public companies will want to consider this cybersecurity guidance not only in the context of SEC review of periodic filings, but also in the context of hindsight review by plaintiff's counsel following an actual cybersecurity event.

Cybersecurity and Risk Factors

In evaluating whether a cybersecurity disclosure is needed, a company should assess all relevant information specific to its business, including prior breaches, the severity and frequency of data security incidents, the direct and indirect costs such as remediation and litigation, the impact of possible theft of intellectual property or customer information, and reputational damages. The CF guidance suggests that, depending on the company's particular circumstances, appropriate disclosures may include:

- A discussion of aspects of the registrant's business that give rise to material cybersecurity risks and the potential costs and consequences of a breach;
- A description of outsourced functions that present material cybersecurity risks and how the company addresses those risks;
- A description of past cyber incidents experienced by the company that are material, either individually or in the aggregate, and a description of the known or potential costs and other consequences;
- A description of risks related to data breaches that remain undetected for an extended period; and

- A description of the relevant insurance coverage.

The cybersecurity guidance is clear that companies should not make risk disclosures of generic risk factors applicable to any issuer or any offering. Additionally, the CF guidance acknowledges the need to balance the obligation to provide sufficient information to allow investors to appreciate the nature of the risks against the inadvertent creation of a roadmap that could compromise the company's cybersecurity.

Cybersecurity and Other Disclosure Obligations

The cybersecurity guidance also states that cybersecurity incidents and risks should be addressed in the Management's Discussion and Analysis of Financial Condition where there is an event, trend or uncertainty that is reasonably likely to have a material effect on future results of operations, liquidity or financial condition. The MD&A should disclose the effects on operating results of cyber incidents and whether such incidents might cause reported financial information to not be indicative of future operating results or financial conditions.

A public company should include in its Description of Business a disclosure if one or more cyber incidents materially affect its products, services, relationships with customers or supplies, or its competitive condition. Legal proceedings concerning material cybersecurity incidents must be disclosed. Additionally, cybersecurity risks and events that may impact a company's financial statements must be addressed.

Finally, companies are required to disclose conclusions about the effectiveness of disclosure controls and procedures. If a cyber incident were to affect a company's information systems, which in turn could pose a risk to the company's ability to record, process and timely file the information required by the SEC, the disclosure controls and procedures could be deemed ineffective.

Practical Guidance on Steps to Take

Given the increased prevalence of cloud computing, outsourcing and Internet-based technologies, many public companies will need to address cybersecurity in their SEC filings going forward. Now that the cybersecurity guidance has been issued, companies should anticipate that the SEC will keep a close eye on cybersecurity disclosures over the next year and will look back at those disclosures when significant and costly breaches impact investors.

Accordingly, we recommend that companies:

- Disclose any cybersecurity incidents that either result in material costs or consequences or indicate material future cybersecurity uncertainties, trends or events. Be sure that prior announcements or press releases concerning data breaches are accounted for in the company's disclosure.

- Companies should also be prepared to assess and disclose to investors the impact of a cybersecurity incident at or near the time of discovery of the breach. A significant cybersecurity incident may need to be disclosed in the next periodic filing or sooner through a press release or Form 8-K. Accordingly, we recommend that data security plans or protocols are updated to reflect the SEC's cybersecurity guidance.

- Companies can incur substantial costs in order to remediate data breaches, mitigate the impact on customer and business relations and put in place long-term prevention measures. These costs should be brought to the attention of the company's auditors.

- It is advisable to keep abreast of reported cybersecurity incidents and the risk disclosures made by competitors and others in the industry. Although the determination of whether the company needs to make cybersecurity risk disclosures depends on the particular facts and circumstances of the issuer, industry vulnerabilities should also be taken into account. Disclosure preparedness and policies should be integrated into a company's overall data security program, which should also encompass network technology, information access and accounting controls, insurance coverage and employee training.

--By Michael T. Gass and Christine M. O'Connor, Choate Hall & Stewart LLP

Michael Gass is chairman of Choate's securities litigation and corporate governance group in Boston. Christine O'Connor is an associate in the firm's securities litigation and corporate governance group in Boston.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360. This article is for general information purposes and is not intended to be and should not be taken as legal advice.