Davis Polk

SEC Cybersecurity Roundtable Panel Debate Public Disclosure and Board Roles

March 27, 2014 | Client Update | 3-minute read

The need for disclosure about cybersecurity breaches must be balanced against other factors, urged some of the panelists at the SEC's roundtable on cybersecurity when the discussion focused on this topic.

While the SEC in its own 2011 guidance for companies questioned whether disclosure of historical attacks would make companies more vulnerable to future breaches, at least one panelist was equally concerned that the disclosure was more likely, based on historical examples, to bring about a rash of litigation. That creates a strong disincentive to disclose breaches, especially if a company can conclude that it does not otherwise have a disclosure obligation. One of the panelists noted that through SEC comment letters, the staff is taking an unusual approach in asking companies to provide information regarding prior incidences of cyber attacks, even if the companies previously determined the consequences were not material. In terms of materiality assessments, at least one study has shown that companies' admissions of being attacked failed to cause any negative impact on stock price, so that the occurrence of breaches do not affect how investors evaluate companies, but instead may be limited to a brand and reputational issue at the moment.

Keith Higgins, the moderator of this panel, noted that the SEC does not want boilerplate disclosure but recognizes that cybersecurity is a common risk that almost all public companies face. While the SEC is not contemplating that companies provide a detailed roadmap of their individual vulnerabilities, the SEC is struggling with how to get companies to differentiate and explain the particular risks that affect them. The reasons for the disclosure may be more than just informational, as Commissioner Stein expressed that one of her reasons for getting companies to make the disclosure is for "moving the company to a better place." In response, one panelist noted that while the SEC has many different avenues for requiring the disclosure, there is at least a question whether the SEC should be tasked to do something simply because the matter becomes one of "public policy," and whether this issue even "belongs to the SEC."

The panelists also stressed the importance of distinguishing among types of attacks that companies face. The investor representative, Trillium, noted that it worried particularly about how certain types of companies collect personal or customer information, such as retail or media companies. However, the general counsel of an energy company stated that they have completely different concerns that lie with the possibilities of extreme infrastructure attacks from bad actors in other nations, as an example, that could cause major disruptions. The appropriate disclosure may therefore depend on the nature of the company's business and industry, and the SEC should be aware and recognize that there is a variety of cyber risks if it contemplates providing additional guidance.

The roundtable also discussed the board's role in assessing the risk of cybersecurity and companies' responses. Everyone agreed that boards are highly interested in the issues and there has been a significant increase in board awareness of the nature, extent and consequences of breaches, reacting with interest to the details of the attack, the competency of the security program and professionals and the use of the technology. However, there was some resistance to the notion that all companies need a director with particular cybersecurity expertise or a committee devoted to cyber issues.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Ning Chiu
+1 212 450 4908
ning.chiu@davispolk.com
