Skadden

Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates

March 28, 2014

SEC Holds Roundtable on Cybersecurity

The Securities and Exchange Commission recently held a roundtable on the issues and challenges cybersecurity presents for market participants and public companies. The roundtable is a means by which the SEC Commissioners can hear a variety of viewpoints and become better informed. Armed with this knowledge, the Commissioners will consider whether the SEC should take additional steps, in terms of regulation or other guidance, either to public companies generally or to entities regulated by the SEC, such as exchanges, investment advisers, broker-dealers and transfer agents. There is no timetable for further SEC action.

Although panelists' views may have varied on particular matters, there was universal agreement that cybersecurity threats are varied, constantly evolving, omnipresent and present critical issues for government agencies, public companies and market participants.

A number of themes of particular relevance to public companies were discussed by panelists, including:

- cybersecurity is not "just an IT issue" but an enterprise-wide operational risk;
- planning for cybersecurity threats is never "done," and there are no solutions that make the issue go away;
- companies should develop plans for how to address cyber incidents, including mitigation and business resiliency/recovery, internal communications and external communications to consumers, regulators and law enforcement and/or intelligence agencies;
- companies should develop a culture of cybersecurity where employees at all levels and across functions take responsibility for considering vulnerabilities and mitigating cyber threats;
- like other enterprise risks, cybersecurity is an area requiring oversight by a board of directors or a board committee. Cybersecurity expertise is not a criteria for board membership, but directors should ask questions and satisfy themselves that management has developed systems to monitor, address, remediate and recover from cybersecurity incidents;
- cybersecurity threat assessments should be risk-based and solutions have to consider other operational imperatives; and
- planned responses to cyber threats should be drilled or "war-gamed" and cannot simply sit on the shelf to be pulled out when the need arises.

A particularly difficult question for the SEC and for public companies relates to company disclosures regarding cybersecurity risks and incidents. The SEC's Division of Corporation Finance published guidance in October 2011, as a result of which risk factor disclosure has become common place. An investor representative on one panel observed that the disclosure has become boilerplate and that more disclosure would be useful to investors. Other panelists observed that company disclosure of cyber

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Marc S. Gerber
Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Stuart D. Levi
New York
212.735.2750
stuart.levi@skadden.com

Joshua F. Gruenspecht
Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

* * *

1440 New York Avenue, N.W.
Washington, D.C. 20005
Telephone: 202.371.7000

Four Times Square, New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

incidents is typically driven by consumer protection laws rather than a view that the information is material to investors. Many panelists cautioned against disclosure requirements that would increase company vulnerabilities to cyber-attacks, and a former SEC Commissioner on the panel observed that more company disclosure may not be in the public's interest. While the SEC, among other questions, is likely to give further consideration to the question of whether public companies should be required to provide additional cybersecurity disclosures, there was a clear message from the majority of panelists to tread lightly.

It is also clear that cybersecurity will continue to be a topic of significant interest to the SEC and other government agencies, market participants, and public companies and their boards of directors.