The Legal Intelligencer

Cybersecurity and Securities Laws: Addressing the Risks

by Katayun I. Jaffari and and Andrew D. McCarthy

Cybersecurity: the risks are no longer "some other" company's problem. All companies, and in particular public companies, must take care in assessing and reporting on cybersecurity risks. Just last week, the U.S. Securities and Exchange Commission (SEC) hosted a roundtable on the topic. SEC Chair Mary Jo White stated, in her opening remarks for the roundtable, that the threats from cybersecurity come from many directions with the ability to attack the financial markets and economy, as demonstrated by the recent private data breaches of U.S. consumers occurring at a retail chain this past holiday season. White emphasized that the SEC's formal jurisdiction over cybersecurity is focused on disclosure by reporting companies of material information, as well as on the integrity of market systems and the protection of customer data. Reports of cyberincidents, in the form of deliberate attacks or unintentional events, have become a recurring feature in headlines over the past several years. Companies that are subject to U.S. securities laws face a host of emerging compliance challenges as a result of the increasing prevalence and frequency of cyber-risks. This article discusses some of the more prominent compliance issues relating to cyber-risks and incidents and required disclosures.

Disclosures under U.S. Securities Laws

Federal securities laws require public companies to disclose risks and events that a reasonable investor would consider material. Generally, a fact is material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision. Although the SEC has not issued any regulation that specifically refers to cybersecurity, the SEC did provide guidance with respect to the obligations of companies to disclose cybersecurity risks and events in 2011 (CF Disclosure Guidance: Topic No. 2). For purposes of disclosure, the SEC has defined "cybersecurity" as the "body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access."

The interpretive guidance highlighted five disclosure items under Regulation S-K that could call for disclosure of cybersecurity matters depending upon a company's particular circumstances. These items include Item 303, requiring a "management's discussion and analysis" (MD&A) of the company's financial condition and results of operations, and Item 503(c), requiring a discussion of the most significant risk factors that the company faces. Additional items consist of Item 101, description of business; Item 103, legal proceedings; and Item 307, disclosure controls and procedures, to the extent material to the company. Besides these specific disclosure requirements, a company may have to disclose information regarding cybersecurity risks and incidents if necessary to make other statements not misleading. Also, cybersecurity incidents may

impact a company's financial statements, and as such, disclosure would be required in the financial footnotes.

Over the last two years, the SEC staff issued comment letters to public companies that include many comments with respect to the deficiency of disclosure with respect to cybersecurity matters. In particular, the comment letters addressed the adequacy of disclosures in companies' risk factors and MD&A. The comments focused on the need for: (1) disclosures about whether data breaches have actually occurred and how the company responded to such breaches; (2) discussions that address cybersecurity risks separately from discussions of other risks; and (3) additional information about why a company believes a cyberincident was not sufficiently material to warrant disclosure.

In addition, current state laws require companies to provide notice about cybersecurity breaches. Such laws, however, vary from state to state; thus, it is challenging for businesses that operate in multiple states to fulfill their statutory requirements. Such difficulties have led to efforts, some of which are discussed below, by the federal government and industry groups to advocate nationwide standards.

A recent industry report that studied cyberdisclosures of Fortune 1000 companies in their public documents such as Form 10-Ks found that 12 percent of the Fortune 500 remained silent on their cyber-risk, while 22 percent of the Fortune 501 to 1000 remained silent on the topic. The top three most frequently listed exposures were privacy/loss of confidential data, reputation risk and malicious acts. Only slightly more than half of the Fortune 500 disclosed the use of technical risk-mitigation tactics, such as firewalls, intrusion detection, or encryption. A mere 1 percent of reporting companies disclosed actual cyberincidents.

Legislative and Industry Activity

Besides the disclosure obligations currently in force under federal securities laws and state laws, various efforts are under way at the federal level to address cybersecurity disclosures and risks. Industry groups are also engaging in efforts to address these matters.

Senators are currently considering a bill, the Data Security Act of 2014, which would impose obligations relating to security, investigation and notification with respect to personal information and payment account information, and any breaches of such information. Members of the House of Representatives are working on a bill, the National Cybersecurity and Critical Infrastructure Protection Act of 2013, which would provide for a voluntary program under which private sector firms would provide the federal government with information on cybersecurity threats to critical infrastructure.

In February 2013, President Obama issued an executive order that, among other things, directed the National Institute of Standards and Technology (NIST) to work with various stakeholders, including agencies of the federal government and private sector entities and experts, to develop a voluntary framework for addressing and mitigating cybersecurity threats to critical infrastructure. In February 2014, the NIST released the first version of the Framework for Improving Critical Infrastructure Cybersecurity. The

framework is a set of voluntary guidelines that sets forth steps companies can take to improve cybersecurity.

In the summer of 2013, the Securities Industry and Financial Markets Association (SIFMA) held an exercise that simulated a cyberattack on U.S. equities markets to provide a chance for participating organizations to use and assess their crisis response and communications plans. In November 2013, the American Bankers Association, the Financial Services Roundtable and SIFMA wrote to senior members of the Senate Select Committee on Intelligence, urging action to pass cybersecurity legislation.

Since 2011, the SEC continues to recognize the importance of cybersecurity. SEC Commissioner Luis Aguilar, who recommended that the SEC convene the roundtable noted above, stated that dialogue is needed among regulators and industry about what the SEC's role should be in the area of cybersecurity. He noted two distinct aspects of the discussion—dialogue regarding issues potentially impacting public companies and dialogue regarding issues impacting capital market infrastructure and SEC-regulated entities. Many congressmen, including Sen. Jay Rockefeller, D-W.Va., have urged the SEC over the past three years to enhance and clarify cybersecurity disclosure obligations.

Steps to Satisfy Disclosure Obligations

To satisfy its obligations under U.S. federal securities laws, a company should start by reviewing and understanding the SEC staff's 2011 guidance discussed above. This guidance did not purport to create new disclosure obligations. Rather, it aimed to be consistent with preexisting disclosure considerations applicable to any business risk. In keeping with the principle that companies must disclose risks that are material, a company should consider the following factors, among others, when determining whether to include risks and events in its disclosures: the severity and frequency of previous cyberincidents, the probability of future cyberincidents, the risks relating to undiscovered cyberincidents, insurance coverage for cyberincidents, and the expense of cyberprotection measures.

The rising rate of cyberincidents that companies are suffering, and the increasing attention that authorities and companies are paying to the related risks, indicate that companies will need to continue to monitor the adequacy of their disclosures regarding cybersecurity. These disclosures should of course correspond to the vigilant development and implementation of actual cybersecurity programs designed to prevent, mitigate and respond to cyberthreats. A company's ability to manage these challenges successfully will be a competitive advantage in the years ahead.

Katayun I. Jaffari *is a partner in Ballard Spahr's business and finance department. She has experience counseling public and private companies in the areas of corporate governance and securities law and compliance, as well as executive compensation and general corporate law matters. She can be reached at jaffarik@ballardspahr.com or 215.864.8475.*

Andy McCarthy *is an associate in the firm's business and finance department and a member of the investment management and mergers and acquisitions/private equity groups. He can be reached at mccarthya@ballardspahr.com or 215.864.8337.*