The Metropolitan Corporate Counsel

Cybersecurity: Breaching The Boardroom

Articles *Cybersecurity: Breaching The Boardroom* has been updated.

Monday, March 17, 2014 - 15:12

Sheppard Mullin Richter & Hampton LLP

Ariel Yehezkel
Thomas Michael

Ariel Yehezkel

Thomas Michael

When the President of the United States calls something "one of the gravest national security dangers that the United States faces," it seems worthwhile to pay attention. The President's statement, on February 12, 2014, was not referring to the dangers of war or terrorism, but to the threat of cyber attacks on the nation's critical infrastructure and U.S. companies. Over the past couple of years, cybersecurity has become an important corporate governance issue, as recent cyber attacks, increased federal oversight, potential legal liability and economic risks have made paying attention certainly worthwhile.

Traditionally, cybersecurity has been a burden borne by management, but the board of directors of a company should also take an active role in implementing and coordinating reform. This article provides an overview of the current status of cybersecurity as it pertains to corporate governance, including regulations, policies, risks and recommendations for board action.

Recent Cyber Attacks

In December of 2013, Target Corporation was the victim of a cyber attack that exposed the private data of 110 million Target customers, including details of 40 million credit and debit card accounts. While the extent of Target's losses and liabilities in connection with the breach have not been fully realized, Target has already committed over $100 million to installing new card-reading devices in all of its stores, and some industry analysts estimate that Target's potential total costs could reach over $1 billion. Only a few weeks later, in January of 2014, retailer Nieman Marcus suffered a similar cyber attack that compromised 1.1 million of its customer accounts. Nieman Marcus waited nearly a month to notify customers of the breach, which stirred controversy in the media and prompted a statement by the Federal Trade Commission (the "FTC") in support of national breach notification laws. Later in January of 2014, Reuters reported that at least three other retailers had been victims of recent cyber attacks but that these incidents had not been made public. The debate surrounding disclosure

and notification of cybersecurity breaches extends beyond retailers and is a significant concern of companies facing the likelihood of new enforcement requirements.

Corporate Governance And Disclosure Requirements

Boards have generally resisted the idea of disclosing cyber incidents and cybersecurity practices, as such disclosures could harm public perception and create fear in the marketplace. The Securities Exchange Commission (the "SEC") does not currently have a rule that specifically addresses cybersecurity or the disclosure of cyber incidents; however, directors should be aware that the SEC has recently applied existing disclosure requirements to cybersecurity.

In October of 2011, the SEC Division of Corporate Finance released a guidance explaining how certain existing disclosure obligations may indirectly include cybersecurity risks under certain circumstances. According to the 2011 guidance, companies should consider whether the following disclosure requirements might apply to their cybersecurity activities:

- Investment Risk Factors – Regulation S-K Item 503(c) would require registrants to disclose on a prospectus if cybersecurity risks are among the most significant factors that make an investment in the company speculative or risky.
- Management's Discussion and Analysis of Financial Condition and Results of Operations – Registrants should disclose if costs and consequences associated with cybersecurity would materially affect the company's operations or financial condition.
- Description of Business – Regulation S-K Item 101 would require registrants to disclose on a Form 10-K if cyber incidents materially affect the company's products, services or relationships with customers or suppliers.
- Description of Legal Proceedings – Regulation S-K Item 103 would require registrants to disclose on a Form 10-K if cyber incidents resulted in material litigation.
- Financial Statements – registrants should consider how to account for the costs associated with preventing cyber incidents and how to measure efforts to mitigate damages following a cybersecurity breach. Cyber incidents could also result in diminished future cash flows and the impairment of assets.
- Disclosure Controls and Procedures – Regulation S-K Item 307 would require registrants to disclose on a Form 10-K if cyber incidents pose a risk to the effectiveness of disclosure controls and procedures.

During the two years since the guidance was released, the SEC has increased its attention to these requirements and has issued over 50 comment letters to companies regarding the adequacy of cybersecurity disclosures. To avoid a comment letter, the SEC recommends disclosing cybersecurity information that is specific to the company, including risks, costs, consequences and measures the company has taken to address such risks. The SEC emphasizes that generic risk factor disclosures are insufficient to allow investors to appreciate the nature of the cybersecurity risks faced by a particular registrant.

Corporate Governance And New Standards

Boards interested in implementing cybersecurity policies have previously faced the daunting task of determining what safeguards are necessary and appropriate for the company. On

February 12, 2014, the National Institute for Standards and Technology ("NIST") released the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework") in order to provide companies with a set of industry standards and best practices for managing their cybersecurity risks. The Framework is the product of extensive collaboration by public and private sector experts in response to the President's Executive Order 13636, which established "the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure." The Framework is designed to be applicable to all companies, not only critical infrastructure, and will likely become the national standard for corporate cybersecurity policies.

The Framework provides companies with guidelines for evaluating cybersecurity needs and distills this process into three main elements: Core, Tiers and Profile. The Core element establishes five key functions of cybersecurity planning: Identify, Protect, Detect, Respond and Recover. The Framework then places companies into one of four Tiers, ranging from companies with partial awareness of cybersecurity to companies with advanced adaptive security practices. With this context, the Framework is able to help companies create a Profile that includes actions the company can take to achieve its cybersecurity goals.

Corporate Governance And Risk

Without an SEC rule that specifically addresses cybersecurity and with a Framework that is merely a compilation of recommendations, boards may be inclined to hold off on reforming cybersecurity practices until it is absolutely necessary to do so. However, there are significant legal and economic risks that make immediate corporate action regarding cybersecurity advisable.

The obvious risk that cybersecurity policies seek to avoid is becoming the victim of a cyber attack and corresponding economic damages. A cyber attack can result in extensive direct costs associated with repaying customers and replacing corrupted software and hardware, as well as losses resulting from harm to customer confidence, reputation and stock price. It is unrealistic to hope to prevent all cyber attacks, but being proactive and having procedures in place for response and recovery can significantly mitigate the economic fallout.

Cyber attacks also expose companies to legal liability. Individuals whose personally identifiable information is compromised as a result of a data breach may bring civil privacy claims under state or federal laws. Shareholders injured as a result of cyber attacks could file derivative claims alleging that officers and directors breached their fiduciary duty of care by failing to exercise proper control and oversight. The FTC has even filed complaints against companies alleging that cybersecurity failures could constitute unfair or deceptive trade practices. Whatever the legal theory may be, it is possible (or even likely) that the Framework will become the standard courts use when considering the reasonableness of cybersecurity efforts, and it is in the best interests of companies to preemptively conform practices to that industry standard.

Corporate Governance Recommendations

The following are some examples of proactive measures that boards should consider:

- Boards should work with management to conform corporate policies to the

Framework guidelines. Applying the recommendations of the Framework will help to defend against lawsuits regarding fiduciary duties and to provide evidence that directors have exercised the appropriate standard of care.

- Boards should delegate to committees oversight of specific aspects of cybersecurity policy and require periodic reporting of risk assessment to management and directors. These committees should consider what safeguards are necessary and appropriate with respect to the degree of risk the company faces. Such committees promote communication within the company about cybersecurity and provide directors with an additional layer of insulation from claims alleging lack of oversight.
- Boards should prepare for worst-case scenario cybersecurity breaches and help management develop immediate response plans, including public disclosure procedures and economic recovery strategies, to mitigate potential damages.
- Boards should consider disclosing cybersecurity risks and protective measures on relevant SEC filings, as such disclosures can generate confidence in investors rather than fear. Shareholders are concerned about cybersecurity and have demanded disclosures of corporate cybersecurity measures. Preemptively revealing cybersecurity policies and risk analysis allows the board to better control the information that is disseminated and to avoid negative publicity from nervous shareholders.
- Boards and management should discuss whether it would be in the best interests of the company to purchase additional insurance (to the extent available) to cover data breaches, as traditional general liability policies may not cover risks associated with cyber attacks. Insurance companies could condition such coverage on a company's compliance with the Framework guidelines.

Looking To The Future

The conversation on cybersecurity will continue to progress at a rapid pace, and companies should seek to remain informed of current developments. New rules and regulations are on the horizon, which will add to the burden of managing compliance and cyber-threats simultaneously. Proactive measures by boards now will help ease this burden and protect companies from future threats.

Ariel Yehezkel is a Partner in the corporate practice group of Sheppard Mullin Richter & Hampton LLP. Mr. Yehezkel concentrates his practice on private equity and domestic and cross border business transactions, including mergers, leveraged acquisitions, follow on acquisitions, divestitures, debt financing, fund formation, PIPE investments, joint ventures, minority investments and other equity arrangements. Mr. Yehezkel also advises companies and boards of directors on a variety of corporate governance matters. He is a leading member of the firm's Israel practice and has extensive experience with legal and business issues involving Israel.

Thomas Michael is an Associate in the corporate practice group of Sheppard Mullin Richter & Hampton LLP. Mr. Michael has experience in a broad range of transactional matters, with a focus on representation of technology start-ups, corporate clients and private equity funds in connection with early-stage formation and corporate governance, mergers and acquisitions, mezzanine financings, equity investments and venture capital.

Please email the authors at ayehezkel@sheppardmullin.com or tmichael@sheppardmullin.com with questions about this article.