Westlaw Journal
SECURITIES LITIGATION & REGULATION
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 20, ISSUE 4 / JUNE 26, 2014

EXPERT ANALYSIS

Cyber Governance: What Every Director Needs To Know

By Paul A. Ferrillo, Esq.
Weil Gotshal & Manges

The number, severity and sophistication of cyber attacks — whether on our retail economy, health care sector, educational sector, or even our government and defense systems — grows worse by the day.[1]

Among the most notable cyber breaches in the public-company sphere was that hitting Target Corp. Allegedly 40 million estimated credit and debit cards were stolen, along with 70 million or more pieces of personal data. The total estimated cost of the Target attack to date is $300 million.[2]

Justified or not, Institutional Shareholder Services has just issued a voting recommendation against the election of all members of Target's audit and corporate responsibility committees (seven of its 10 directors) at the upcoming annual meeting. ISS' reasoning is that, in light of the importance to Target of customer credit cards and online retailing, "these committees should have been aware of, and more closely monitoring, the possibility of theft of sensitive information."[3]

Unlike many other aspects of directing the affairs of a public company (*e.g.*, overseeing its financial reporting function and obligations) "cyber" is new for many directors and is certainly far from intuitive. Public company directors must know their responsibilities for the cyber security program within the framework of the company's enterprise risk management structure. Directors should ask basic questions about their company's cyber security, incident response and crisis management program. Finally, they should consider the potential value of a stand-alone cyber insurance policy to transfer some of the risk of a cyber attack to a reputable insurance carrier.

DIRECTORS' DUTY OF OVERSIGHT WITH RESPECT TO CYBER SECURITY

A public company director's "duty of oversight" generally stems from the concept of good faith. As noted in the seminal case *In re Caremark International Inc. Derivative Litigation,* 698 A.2d 959 (Del. Ch. 1996), as a general matter:

> A director's obligation includes a duty to attempt, in good faith, to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that the failure to do so in some circumstances may, in theory, at least render a director liable for losses caused by noncompliance with applicable legal standards.

The business judgment rule protects a director's "informed" and "good faith" decisions unless the decision cannot be attributed to any rational business purpose. In today's world, it would be hard to question that cyber security should not be part of any organization's enterprise risk management function, and thus, by inference, part of any director's duty of oversight.

Indeed, the plaintiffs' securities-class-action bar has recently filed two shareholder derivative actions against the boards of both Target and Wyndham Worldwide Hotels as a result of their publicly reported cyber breaches. In these complaints, the plaintiffs alleged, among other things, that the directors "failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner."[4]

As made clear by the questioning of the panelists in the recent Securities and Exchange Commission Cyber Roundtable on March 26, there are other reasons for directors to be intimately involved with decisions concerning a company's cyber security (*i.e.*, "the regulators").[5] Not only has the SEC been more active with cyber "thinking" and security issues, but the Office of Compliance, Inspections and Examinations of the SEC (governing investment advisers and asset managers) and the Financial Industry Regulatory Authority are also involved.[6]

The Federal Trade Commission, as well as state regulators, such as the New York State Department of Financial Services, have also been tackling the issue. Each of these organizations has its own exhaustive list of factors or areas of examination. We have yet to see whether the SEC will issue additional guidance to public companies concerning what information is required to be disclosed to investors concerning cyber security incidents.[7]

Allegedly, 40 million estimated credit and debit cards were stolen in the Target attack, along with 70 million or more pieces of personal data. The total estimated cost of the attack to date is $300 million.

CYBER GOVERNANCE QUESTIONS FOR DIRECTORS TO CONSIDER

Here are some basic questions public company directors should be asking when reviewing their company's cyber security framework:

- What part of the board should handle examination of cyber security risks? Should it be the whole board? Should this responsibility be assigned to the audit committee or the risk committee (if there is one)? Should the board create a "cyber committee" to exclusively deal with these issues? Should additional board members be recruited who have specific cyber security experience?
- How often should the board or committee be receiving cyber security briefings? In this fast-paced world in which cyber breaches are reported daily, are quarterly briefings enough? Should the board be receiving monthly briefings or more, given the industry type of the company (*e.g.*, tech/IP company)?
- Given the sheer complexity and magnitude of many cyber security issues, should the board hire its own "cyber advisers" to consult on cyber security issues and to be available to ask questions of the company's senior management, CTOs and CIOs?
- What are the greatest threats and risks to the company's highest-value cyber assets? Does the company's human and financial capital line up with protecting those high-value assets?
- What is the company's volume of cyber incidents on a weekly or monthly basis? What is the magnitude or severity of those incidents? What is the time taken and cost to respond to those incidents?
- What would the worst-case cyber incident cost the company in terms of lost business (because of downtime of systems that were attacked and need to be brought back and the harm to the company's reputation as a result of the attack)?
- What is the company's specific cyber incident plan and how will it respond to customers, clients, vendors, the media, regulators, law enforcement and shareholders? Does the company have a crisis-management plan to respond to all these various constituencies, as well as the media (both print and electronic/high-activity bloggers)? Finally, has the cyber incident plan been tested so it is ready to be put into place on a moment's notice?
- What cyber security training does the company give its employees?
- What sort of "cyber due diligence" does the company perform with respect to its third-party service providers and vendors?[8]

- In a mergers-and-acquisitions context, what is the level of cyber due diligence done as part of the consideration of any acquisition?
- Has the company performed an analysis of the "cyber-robustness" of the company's products and services to analyze potential vulnerabilities that could be exploited by hackers?
- Finally, should the company consider adopting, in whole or in part, the National Institute of Standards and Technology cyber security framework as a way of showing affirmative action to protect the company's IP assets?

These and other tough questions should be asked by directors of senior manage-ment and senior IT staff. Directors may need their own advisers and professionals to help fulfill their oversight duties in assessing the answers to these questions.

AVAILABILITY OF CYBER INSURANCE TO MITIGATE CYBER-RELATED RISKS AND COSTS

Given the past two years of major cyber breaches, one additional question directors should consider is whether the company should be purchasing cyber insurance to mitigate its cyber risk. This could cover forensic costs, incident and crisis management response costs, and the litigation costs, expenses and settlements that could be incurred as a result of a major cyber breach.

Though in the past many companies tried to insure cyber breaches through their comprehensive general liability policies, today's "gold" standard is to purchase stand-alone cyber insurance coverage. Though some in the industry have called the area of cyber insurance the "Wild West," rules of thumb have started to emerge regarding coverages frequently found in stand-alone cyber insurance policies. For example, such a policy may cover:

- Loss arising from third-party claims resulting from a security or data breach (*i.e.*, a lawsuit for damages by a financial institution against a retailer following a breach or regulatory actions in connection with a cyber breach).
- The direct, first-party costs of responding to a breach, like the forensic costs of determining what caused the cyber breach.
- Loss of income and operating expenses ("business interruption insurance") resulting from a cyber breach.
- Cyber extortion threats against a company.

The better stand-alone cyber insurance policies go even further. Some will provide a rapid response team staffed by IT experts to consult with a company and help manage their response to the cyber incident. Some have a 24/7 hotline available to help guide companies through a cyber breach. Additionally, some policies help reimburse the costs of required customer notification, as well as the cost of a crisis management team to help the company communicate with its key customers and vendors to help minimize reputational harm after a breach.

Because stand-alone cyber insurance policies are relatively new phenomena, it would be important to check if your cyber carrier has a good claims-handling and claims-paying reputation, or a reputation as a "strict constructionist" of exclusions. No two policies are alike, so offered terms, exclusions and endorsements should also be compared.

Experts, like sophisticated insurance brokers or insurance coverage lawyers, can be consulted here to make sure the company gets the best policy. Further, as certain large-scale cyber security breaches have also resulted in shareholder derivative actions alleging breach-of-fiduciary-duty claims against directors, it would be wise for directors to consider the sufficiency of the company's directors and officers liability insurance.

Finally, given the reported costs of companies that have had to respond to cyber breaches, directors should question how much cyber insurance is available in the marketplace for a

In today's world, it would be hard to question that cyber security should not be part of any organization's enterprise risk management function, and thus, part of any director's duty of oversight.

company to purchase. The company's insurance broker should be consulted, and benchmarking information may be available on a company- or industry-specific basis to advise how much insurance other similarly situated companies are purchasing.

We are told by the brokerage community that up to $300 million in cyber insurance may be available for a company to purchase if it truly wants to transfer some of its cyber-related risk to a good insurance carrier. Risk-transfer mechanisms like cyber insurance are certainly no substitute for a robust cyber security and battle-tested incident response plan, along with rigorous training of all employees, but it can be an important component of a comprehensive cyber risk mitigation plan.

NOTES

[1] *Report: Growing Risk of Cyber Attacks on Banks,* WALL ST. J., May 6, 2014, *available at* http://online.wsj.com/article/AP05cf3e82176f4e7fb3aa644ee4b37db9.html (noting that "a yearlong survey of New York bank security has found that cyber thieves are using increasingly sophisticated methods to breach bank accounts).

[2] *See* Brian Krebs, *The Target Breach: By the Numbers*, KREBS ON SECURITY (May 14, 2014), *available at* http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

[3] Paul Ziobro & Joann S. Lublin, *ISS' View on Target Directors Is a Signal on Cybersecurity*, WALL ST. J., May 28, 2014, *available at* http://online.wsj.com/articles/iss-calls-for-an-overhaul-of--board-after-data-breach-1401285278?mod=_newsreel_4.

[4] Kevin LaCroix, *Wyndham Worldwide Board Hit with Cyber Breach-Related Derivative Lawsuit,* THE D&O DIARY (May 7, 2014), *available at* http://www.dandodiary.com/2014/05/articles/cyber-liability/wyndham-worldwide-board-hit-with-cyber-breach-related-derivative-lawsuit/.

[5] *See* Webcast of SEC Cybersecurity Roundtable (Mar. 26, 2014), *available at* http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml.

[6] John Reed Stark, *Cybersecurity & Financial Firms: Bracing for the Regulatory Onslaught* (Apr. 21, 2014), *available at* http://www.strozfriedberg.com/wp-content/uploads/2014/04/Cybersecurity-and-Financial-Firms-Bracing-for-the-Regulatory-Onslaught_BloombergBNA_Stark_April2014.pdf.

[7] CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[8] Trustwave 2013 Global Security Report, *available at* http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf (noting that 63 percent of all investigations showed that a cyber breach emanated from a third-party vendor or IT administrator).

Paul Ferrillo is counsel in the litigation department at **Weil Gotshal & Manges** in New York, where he focuses on complex securities and business litigation. He has substantial experience in the representation of public companies and their directors and officers in shareholder class and derivative actions, as well as in internal investigations. This article was first published on the Harvard Law School Forum on Corporate Governance and Financial Regulation blog.