June 3, 2014

Weil

Alert
Cyber Security, Cyber Governance, and Cyber Insurance

What Every Public Company Director Needs to Know

By Paul A. Ferrillo

The number, severity, and sophistication of cyber attacks – whether on our retail economy, our healthcare sector, our educational sector or, in fact, 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 Corporation (40 million estimated credit and debit cards allegedly stolen, 70 million or more pieces of personal data also stolen, and a total estimated cost of the attack to date of *approximately $300 million*).[2] Justified or not, ISS has just issued a voting recommendation against the election of all members of Target's audit and corporate responsibility committees – seven of its ten directors – at the upcoming annual meeting. ISS's 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., like overseeing its financial reporting function and obligations), "cyber" is new for many directors, and is certainly far from intuitive. For this reason, this article will focus specifically on the responsibilities of public company directors to oversee their company's cyber security program (within the framework of the company's enterprise risk management structure); the basic questions directors should be asking about a company's cyber security, incident response, and crisis management program; and lastly, 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/Other Duties and Regulations Lurking About for Directors

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 Int'l, 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 non-compliance with applicable legal standards."

However, 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 directors 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 was made clear by the questioning of the panelists in the recent SEC Cyber Roundtable, on March 26, 2014,[5] there are other reasons for directors to be intimately involved with decisions concerning a company's cyber security, i.e., "the regulators." Over the last several months, not only has the SEC been more involved generally with cyber "thinking" and security issues, but also the Office of Compliance, Inspections and Examinations of the SEC (governing investment advisors and asset managers), and the Financial Industry Regulatory Authority (FINRA) are all in the game.[6] So is the Federal Trade Commission, as well as state regulators, such as, the New York State Department of Financial Services. Each of these organizations has their own exhaustive list of factors or areas of examination/consideration. They are long and extensive. And 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]

Cyber Governance Questions for Directors to Consider

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

1. 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? 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?
2. How often should the Board (or Committee) be receiving cyber security briefings? In this world, which moves at light-speed and 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 on whose board they sit, e.g., tech/IP company)?
3. 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?
4. 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?
5. What is the Company's volume of cyber incidents on a weekly or monthly basis? What is the magnitude/severity of those incidents? What is the time taken and cost to respond to those incidents?
6. 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 because of harm to the Company's reputation as a result of the attack)?
7. 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

(or "war-gamed") so that it is ready to be put into place on a moment's notice?

8. What cyber security training does the Company give its employees?
9. What sort of "cyber due diligence" does the Company perform with respect to its third-party service providers and vendors?[8]
10. In a mergers and acquisitions context, what is the level of cyber due diligence that is done as part of the consideration of any acquisition?
11. 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?
12. Finally, should the Company consider adopting, in whole or in part, the NIST cyber security framework as a way or method of showing affirmative action to protect the company's IP assets?

This list could go on for pages. But it won't, since we believe it serves its purpose, i.e., there are plenty of tough questions that directors need to ask of its senior management and senior IT staff. And directors may need their own advisors and professionals to help them fulfill their oversight duties in helping to assess and ask the tough 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 or not the Company should be purchasing cyber insurance to mitigate its cyber risk, including its 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 standalone cyber insurance policies. For example, such policy may cover:

1. Loss arising from third party claims resulting from a security or data breach (i.e., a lawsuit by a financial institution against a retailer following a breach for damages, or regulatory actions in connection with a cyber breach);
2. The direct first party costs of responding to a breach, like the forensic costs of determining what caused the cyber breach;
3. Loss income and operating expenses ("business interruption insurance") resulting from a cyber breach;
4. 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 that is available to help guide companies through a cyber breach. Additionally some policies will help reimburse the costs attendant to the incident itself, including paying 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 after a breach to help minimize reputational harm.

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 that it can. Further, as certain very large scale cyber security breaches have also resulted in shareholder derivative actions alleging breach of fiduciary claims against directors, it would be wise for directors to consider the sufficiency of the Company's directors and officers liability insurance program.

Finally, given the reported costs of certain companies that have had to respond to cyber breaches, directors should question how much cyber insurance is available in the marketplace for a company to purchase. The Company's insurance broker should be consulted, and bench-marking 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 company's overall cyber risk mitigation plan.

---

1. *Report: Growing Risk of Cyber Attacks on Banks* (noting that "A yearlong survey of New York bank security has found that cyber thieves are using increasingly sophisticated methods to breach bank accounts"), *The Wall Street Journal*, May 6, 2014, *available at* http://online.wsj.com/article/AP05cf3e82176f4e7fb3aa644ee4b37db9.html.
2. *See* "The Target Breach: By the Numbers," *available at* http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.
3. Paul Ziobro and Joann S. Lublin, *ISS's View on Target Directors Is a Signal on Cybersecurity*, *The Wall Street Journal*, May 28, 2014, *available at* http://online.wsj.com/articles/iss-calls-for-an-overhaul-of-target-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, March 26, 2014, *available at* http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml.
6. John Reed Stark, *Cybersecurity and Financial Firms: Bracing for the Regulatory Onslaught*, April 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*, October 13, 2011, *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
8. *Trustwave 2013 Global Security Report* (noting that 63% of all investigations showed that a cyber breach emanated from a third-party vendor or IT administrator), *available at* http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.

If you have questions concerning the contents of this issue, please speak to your regular contact at Weil, or to:

Paul A. Ferrillo (NY) Bio Page paul.ferrillo@weil.com +1 212 310 8372