Board Tools for Oversight of Cybersecurity Risk

By Stewart M. Landefeld, Luis R. Mejia, and Allison C. Handy

Cyber attacks on US public companies have damaged business operations, compromised corporate intellectual property and the private data of consumers, and threatened national security. These attacks increased in 2014, culminating with North Korea’s attack on Sony Pictures Entertainment. As a result, boards cite cybersecurity as their number one risk-related concern. In exercising a board’s duty of oversight, the magnitude and complexity of cybersecurity risk present special challenges.

In this article, we present the cybersecurity risks that many public company boards will consider, from the business impact of a cyber attack to the litigation and regulatory exposure that may follow. We address the oversight duty of the board and propose a methodology for fulfilling that duty. In this context, the methodology is based on the board’s role of oversight as opposed to the day-to-day responsibility that

Continued on page 2

Stewart M. Landefeld and Luis R. Mejia are partners, and Allison C. Handy is an associate, of Perkins Coie LLP. Katherine A. VanYe, Esq., provided invaluable research and writing assistance. The authors gratefully acknowledge the review and contributions of Evelyn Cruz Sroufe, Esq., John A. Seethoff, Esq., John C. Sullivan, Esq., Jeffrey A. Christianson, Esq., and Sally Barian Yates, Esq.
rests with management. A board, by exercising the duty of oversight to ask the right questions and satisfy itself that appropriate internal controls are in place, can help to see that controls are in place and set an appropriate tone at the top with respect to cybersecurity matters.3

Framing the Problem: Why Cybersecurity Attracts Particular Board Oversight Attention in 2015

Impact on the Business

Incidents of large-scale cybersecurity incursion and theft picked up pace in late 2013 and grew throughout 2014 and into 2015. Two notable retailer breaches were attacks on Target in late 2013 and Home Depot in 2014. Other incursions include those on JP Morgan, the theft of US Postal Service employee data, the breach of health insurers Anthem’s and Premera Blue Cross’s customer data, including Social Security numbers, and North Korea’s attack on Sony.

The Target incursion reported in December 2013 compromised the records of as many as 70 million customers4 and resulted in $145 million in data breach-related expenses.5 Although CEO and Board Chair Gregg Steinhafel, a 35-year Target veteran, took a proactive role, Target announced his resignation in May 2014, linking it to the data breach.6

On September 18, 2014, Home Depot, North America’s largest home improvement retailer, confirmed that its payment data system had been breached.7 Home Depot noted that the breach would impact customers in the United States and Canada who had used payment cards between April and September 2014—a five-month period—putting up to 56 million credit and debit cards at risk. Home Depot, following lessons from Target, immediately pledged to provide free credit monitoring and other identity-protection services and to cover customer liabilities for fraudulent claims. The company explained that it had taken months over the course of 2014 for its cybersecurity team to understand the magnitude of the 2014 incursions—during a time that Home Depot was completing a major encryption improvement project.8 The company estimated that costs related to the breach could total $62 million (offset by $27 million in insurance recoveries). Although Home Depot said that it was not able, as of September, to estimate further costs or ranges of costs related to the breach, it also warned that the impact of the data breach could have a material and adverse effect on Q4 2014 and future fiscal periods.

Litigation Risk

In addition to the significant time, resources, and capital expenditures required to respond to a cybersecurity breach, there is the risk of litigation and regulatory scrutiny. For example, Target recently settled a consumer class action related to its data breach for $10 million.9 Target also is the subject of a class action by issuer banks whose customers’ data was stolen.10 Litigation also has resulted from cybersecurity breaches at other companies, including Sony, St. Joseph Services Corporation, Zappos, LinkedIn, and SAIC.11 Although some of the cases have been dismissed or settled, the companies have incurred substantial legal fees and the litigation has been a distraction to normal operations.

Regulatory Risk—Federal Consumer Protection

The Federal Trade Commission (FTC) enforces federal statutes and regulations that impose data security requirements on companies, including the Safeguards Rule (which implements the Gramm-Leach-Bliley Act),12 the Fair Credit Reporting Act,13 and the Children’s Online Privacy Protection Act.14 These acts and regulations govern data security requirements and disclosure and disposal of consumer information. The Federal Trade Commission Act’s prohibition against unfair or deceptive acts or practices also has been used by the FTC in cases of false or misleading claims about a company’s data security procedures, or failure to employ reasonable security measures that result
in substantial consumer injury.\textsuperscript{15} According to Jessica Rich, the director of the Bureau of Consumer Protection at the FTC, the FTC has brought such cases when a company’s practices as a whole demonstrated “multiple and systemic” failures.\textsuperscript{16} In congressional testimony, she noted that “the [FTC] has made clear that it does not require perfect security; that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.”\textsuperscript{17}

In early 2015, President Obama called for federal legislation—the “Personal Data Notification & Protection Act”—to mandate a single, national standard requiring companies to inform their customers within 30 days of discovering that their data has been hacked. The President has suggested this as a replacement to the many less-than-uniform state disclosure laws.\textsuperscript{18}

For telecommunications and other businesses in the communications industry, a committee tasked by the Federal Communications Commission (FCC) to give advice on implementation of cybersecurity risk management has focused on communications businesses as part of the national critical infrastructure. In March 2015, the committee issued a Cybersecurity Risk Management and Best Practices Final Report.\textsuperscript{19} The FCC Final Report’s goal was to provide cybersecurity best practices for the communications industry to assist with implementation on a voluntary basis of the “NIST Framework” (The National Institute of Standards and Technology’s Framework for Improving Critical Infrastructure Cybersecurity),\textsuperscript{20} developed pursuant to the President’s February 12, 2013, Executive Order No. 13636, Improving Critical Infrastructure Cybersecurity. The FCC Final Report identifies voluntary mechanisms to provide assurances that FCC-regulated companies are addressing cybersecurity risks, including voluntary meetings with the FCC and the Department of Homeland Security (DHS), and participating in a DHS program on integrating and coordinating critical infrastructure cross-sector efforts.

### Regulatory Risk—The SEC’s Interest in Cybersecurity

The Securities and Exchange Commission (SEC) has shown interest in cybersecurity, but to date has not brought an enforcement action against a public company related to cybersecurity. Enforcement activity has been limited to registered broker-dealers and investment advisors, that is, entities that are subject to specific regulations governing the security and confidentiality of customer records and information.\textsuperscript{21}

In October 2011, the SEC’s Division of Corporation Finance provided guidance on disclosure obligations relating to cybersecurity risks and cyber incidents, stating that the existing disclosure structure under SEC regulations provides for both timely and sufficient disclosure of material cybersecurity attacks, risks and events. Existing disclosure requirements have at least six areas in which disclosure in periodic reports on Forms 10-K and 10-Q (and certain other disclosure documents) may call for cybersecurity disclosure.\textsuperscript{22} The SEC’s 2011 guidance stresses that only material information need be disclosed; however, the SEC’s actions have been somewhat inconsistent with its guidance. In several comment letters, the SEC has pushed for disclosure of all cybersecurity events, regardless of materiality.\textsuperscript{23} Boards should anticipate some dialogue between the company and the SEC on this issue in the event of a cyber attack.

Examples of recent disclosures of cybersecurity risks in the six areas identified in the 2011 guidance include:

- **Risk Factors.** The 2011 guidance specifically called out Risk Factors as appropriate for disclosure of material cybersecurity risks and this section is currently the most frequent home for such disclosures. For example, Target discussed specific risk factors related to its data breach, and candidly stated that it might not be able to prevent future breaches given that the techniques for attacks change frequently and are difficult to detect.\textsuperscript{24}

- **MD&A.** Cybersecurity risk could constitute a classic “trend” or “material event,
trend or uncertainty reasonably likely to have a material impact on the organization’s operations, liquidity, or financial condition” that would be required to be discussed in Management’s Discussion and Analysis of Financial Condition and Results of Operation (MD&A). Home Depot, for example, in its first Form 10-Q after its data breach, included an extensive discussion of the breach in its MD&A. This disclosure included discussions of the expenses incurred, litigation, claims, and government investigations, future costs, and insurance coverage.25

• Description of Business. If cybersecurity risks materially affect products, services, relationships with customers or suppliers, or competitive conditions, a registrant should disclose the cybersecurity risks in the Description of Business section. Target, in its first Form 10-K after the data breach, highlighted the breach with a brief description and cross reference to its MD&A discussion.26

• Legal Proceedings. Data breaches or cybersecurity incidents can result in material regulatory investigations or private actions that will require discussion in the Legal Proceedings section. Both Target and Home Depot, in the Form 10-Q and 10-K that each company filed after their respective data breaches, incorporated by reference the legal proceedings discussion from the MD&A in the Legal Proceedings section.27 In the case of Target, this cross-reference was included despite the company’s assessment that these legal proceedings did not rise to the level of materiality generally required for disclosure in the Legal Proceedings section.

• Financial Statement Disclosures. When the risks or damages have a material financial impact on the registrant, cybersecurity risks and incidents that represent substantial costs in prevention or response should be included in financial statement disclosures. Target, for example, has updated its financial statement disclosures each quarter to quantify expenses incurred due to the data breach.

• Disclosure Controls and Procedures. If a cybersecurity incident impairs a registrant’s ability to record or report information that must be disclosed, it may impact Disclosure Controls and Procedures. (The authors have not yet seen an example of a discussion of a failure or weakness in disclosure control and procedures caused by a cybersecurity incident.)

Current Report on Form 8-K. In addition to these areas that the SEC highlighted in periodic reports, a registrant might also determine that it needs to file a current report on Form 8-K in connection with a cybersecurity incident. Some companies that have complied with the state-mandated consumer notification laws mentioned previously also have determined that the breach rises to the level of materiality of a report on Form 8-K. For example, in August 2014, Community Health Systems filed a Form 8-K to disclose a data breach affecting 4.5 million customers.28 The compromised data included patient names, addresses, birthdates, telephone numbers, and Social Security numbers.29 Unlike Community Health Systems, however, Anthem did not file a Form 8-K in connection with its February 5, 2015 notification to its members of a cyber attack that resulted in exposure and theft of up to 80 million records, including Social Security numbers. (Anthem did include discussion of the data breach in its Form 10-K filed February 24, 2015.)

Board and Committee Oversight of Risk and Cybersecurity

Board Oversight of Risk

A board’s responsibility to oversee cybersecurity risks arises from the “duty of oversight” developed under Delaware law. Oversight grows out of what Delaware courts consider the fundamental fiduciary obligations of directors: the duties of care and of loyalty.30 Since the 1996 Delaware Court of Chancery decision, In re Caremark International Inc. Derivative Litigation,31 directors have understood that they do not fulfill their oversight duties by passively receiving information from management.
Instead, boards must assure themselves that information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation’s compliance with law and its business performance.\(^{32}\)

The Caremark court postulated that a board could potentially be liable for violations of law by the corporation, even if the directors had no knowledge, or even grounds for suspicion of the wrongdoing, if its failure to establish systems designed to detect such violations amounted to bad faith.\(^{33}\)

In 2006, a decade after Caremark, the Delaware Supreme Court, in Stone v. Ritter, clarified when the Caremark framework will result in director oversight liability. When a claim of director liability is based on ignorance of corporate wrongdoing, “only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists—will establish the lack of good faith that is a necessary condition to liability.”\(^{34}\)

Litigation and SEC enforcement actions springing from the financial crisis of 2008 have further explored the board oversight responsibility described in Stone in 2006. For example, when may a board be liable for failure to monitor business risk that did not involve corporate wrongdoing?\(^{35}\) In In re Citigroup Inc. Shareholder Derivative Litigation, the Delaware Court of Chancery rejected claims of personal liability against the Citigroup board for failure to monitor and address the risks posed by the bank’s exposure to the subprime mortgage market, stating: “Oversight duties under Delaware law are not designed to subject directors, even expert directors, to personal liability for failure to predict the future and to properly evaluate business risk.”\(^{36}\) Despite this forceful Delaware statement in support of directors who exercise their oversight duties in good faith, plaintiffs have begun more recently to bring claims against boards for failure of oversight in some of the major cyber attacks of later 2013–2014.\(^{37}\)

Wyndham Worldwide Corporation’s board provided an illustration of a board satisfying its oversight obligations. The district court described the board’s actions surrounding Wyndham data breaches in Palkon v. Holmes.\(^{38}\) A shareholder had filed a derivative action against the board and others, claiming that Wyndham’s failure to implement adequate cybersecurity measures and to disclose the data breaches in a timely manner caused damage to shareholders. The shareholder also alleged that the board wrongfully refused to sue the company’s officers. The Palkon court found that the board’s refusal to pursue litigation was a good-faith exercise of business judgment, made after a reasonable investigation. Although the court did not reach the merits of the underlying claim, it noted that the plaintiff conceded that security measures existed when the first breach occurred, and that the board had repeatedly addressed security concerns. The full board had discussed the cyber attacks, the company’s security policies, and proposed security enhancements at 14 meetings over a four-year period, and the audit committee had addressed the same issues in at least 16 committee meetings during the same time period. The company had hired technology firms to investigate each breach and to issue recommendations on enhancing the company’s security, and it followed those recommendations. Under these circumstances, the court, following Caremark and Stone, found that it would have been difficult for the plaintiff to establish that the board “utterly failed to implement any reporting or information system…[or] consciously failed to monitor or oversee its operations thus disabling themselves from being informed.”\(^{39}\)

In addition to the state law duty of oversight, companies have sharpened their focus on board oversight of risk in light of the disclosure requirement under SEC Regulation S-K Item 407(h), which was added in the SEC’s proxy disclosure enhancements in 2009.\(^{40}\) This item, which is required in proxy statements and certain other public filings, calls for disclosure of the extent of
the board’s role in risk oversight. In a June 2014 speech, SEC Commissioner Luis Aguilar noted that boards’ increasing focus on risk oversight must encompass oversight of cybersecurity risks.41

**Board and Committee Oversight of Cybersecurity**

Boards exercise their risk oversight responsibilities through a variety of ways. Generally, management provides periodic briefings on significant risks that a company faces and how it seeks to control risk. Board and executive team discussions of risk occur both at regular meetings and with a specific risk analysis of new ventures at an annual strategic planning session. Often, the board exercises direct oversight of certain specific risks, and delegates oversight of other specific risks to a committee (for example, compensation plan risks to the compensation committee, financial reporting risk to the audit committee, and so on). Committees can provide effective oversight by devoting close and sustained attention in a small group—a compelling benefit when dealing with complex matters having a short time fuse. Large public company board meetings are scheduled a year or more in advance, although committees can meet with greater frequency and flexibility. Committees can be more responsive and, in small group discussion, can better take advantage of the special skills and backgrounds of committee members.

Risk committees (for financial institutions) and audit committees monitor many risks for most companies and could take on delegated oversight of cybersecurity. Boards alternatively delegate cybersecurity oversight to a regulatory affairs committee or to another committee with appropriate mandate and membership. It is rare for a company to have a cybersecurity risk committee.42

In delegating to a committee, both the Delaware General Corporation Law and the Model Business Corporation Act require appropriate board oversight of the committee’s work. The SEC has brought enforcement actions against board members who were not diligent and attentive to matters that they had delegated to a committee.43

**Best Practices for the Board in Managing Cybersecurity Risk**

Boards, and the assigned committee (often audit), can think of their task of overseeing cybersecurity in three stages. The methods are similar to those of overseeing other enterprise-wide operational risks.

First, what is the frequency and depth with which the board or committee will review cybersecurity issues? Because cybersecurity is one of a number of important operational risks, the board, together with the CEO, chief financial officer, and general counsel, can set an appropriate frequency, such as twice-a-year presentations on cybersecurity to the assigned committee. The committee would then “report out” on the topic to the full board as a stand-alone report or as part of a broader report on operational risks. The full board could choose to have a detailed discussion when it conducts its annual in-depth review of enterprise-wide risk issues. The board or committee also will want to address cybersecurity (and review a response plan to cyber incursions) as part of its periodic review of the company’s crisis management plan.

Second, what are the resources available to the board or committee and on whom do the directors rely for their review? Generally, the first resource is senior management. Management can educate the board on cybersecurity generally, help the board to assess threats specific to the company, and explain the company’s current defenses and mitigations to those threats. Usually, the appropriate person to present to the audit committee is the internal owner of cybersecurity, for example, a chief information officer. He or she can present an agenda that could include

(1) the cybersecurity environment of threats and how this environment fits into the company’s overall operational risk framework;

(2) attacks on the company in the last 12 months and how they were addressed;
(3) the program for the coming year, including the structure, operation, and testing of security and privacy programs;

(4) a multiple-year program roadmap (past and forward) and budget;

(5) a comparison of the company program to the current NIST Framework or other appropriate industry standard;

(6) known trends of industry risks and efforts to enhance cybersecurity in the coming year; and

(7) emerging issues including monitoring and mitigating device (e.g., smartphone or tablet) threats, and managing the risks of big data.

Some boards use a third-party consultant as an additional resource. The advisor could assist the assigned committee to understand best practices in the company’s industry. Third parties can help to bring perspective, aiding directors in assessing the management team as a source other than the team itself. If a change in leadership of the cybersecurity function occurs, having a consistent third-party advisor can help the board or committee assess whether the program has maintained continuity.

Questions for the Audit Committee to Ask the Manager of Cybersecurity Risk

Third, at the heart of any board oversight exercise are thoughtful questions from its directors. These questions, paired with management’s responses over time, are the essence of oversight, and can lead to process improvements. (A general counsel can help the board develop these questions as a starting point for its inquiry.) In the same way that Warren Buffett has suggested four questions to assist an audit committee in discussions with its outside auditors, the board or audit committee can pose this basic set of a half-dozen questions as tools to understand and oversee the management of cybersecurity:

1. **Ownership.** Who owns the cybersecurity risk for our company? To whom does she report? Has she assessed the scale and probability of attacks or incursions, as well as the most likely areas of vulnerability (internal threats, third-party vendors) against the company?

2. **Controls.** Have we designed and implemented strong internal controls that address our cybersecurity risks and ensured that our internal controls are well documented, communicated, and updated as needed? Have our controls identified attempted or successful cybersecurity breaches or attacks?

3. **NIST Framework.** Does the company use the NIST Framework or, if not, what other appropriate framework is used? How do our framework and controls compare with those of others in our industry?

4. **Budget.** Does the company have the appropriate budget to manage the cybersecurity function and develop a satisfactory team? Are there needs that have not been met due to budget? Does the company use a third party for a security audit?

5. **Crisis Response.** Do we have an incident response plan in place? Does the plan include all the relevant stakeholders as owners with specific responsibilities? Does the plan incorporate what we have learned from attacks against us and our competitors? Are we prepared to respond to legal, reputational, and commercial risks and obligations? Are we satisfied with our insurance coverage?

6. **Disclosure.** Does the company have a form of consumer notice and Form 8-K prepared for an incursion? Does the company provide an investor reading our Form 10-K a clear picture of our risk profile and how our company’s operations impact our cybersecurity risk profile?

**Conclusion**

Cybersecurity will continue to evolve as a risk and will demand increasing oversight by boards of public companies. Boards have
available to them the tools required to oversee this key operational risk. A successful plan for oversight will be to first determine the scope of board review and then to establish the resources available to the board in making its inquiries. Developing key questions for management, and responding thoughtfully to such questions, are at the heart of this oversight process. Finally, applying this process over time will allow the board to see how cybersecurity threats to the company evolve with the company’s changing business. A board using these tools effectively can become as confident as reasonably practical that the company is taking appropriate steps to address the evolving cybersecurity risk.

Notes


3. Cybersecurity is a contingent risk, that is, one whose impact on a business is uncertain, because it is contingent on future outcomes. More than many other contingencies that may hinge on one or two events, cybersecurity repays board attention over time, as cybersecurity-related threats will adapt to changes in the business itself. See Gregory F. Treverton, “Risks and Riddles,” Smithsonian Mag., June 2007, available at http://www.smithsonianmag.com/people-places/risks-and-riddles-154744750/, last accessed March 29, 2015 (discussion of complex contingencies).


15. See Discussion Draft of H.R. __, Data Security and Breach Notification Act of 2015 Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. on Energy and Commerce, 114th Congress 3 n.8 (2014) (statement of Jessica Rich, Director, Bur. of Consumer Prot., Fed. Trade Comm’n) available at https://www.ftc.gov/system/files/documents/public_statements/630961/150318EncryptionofPaymentDatainAllUSStores.pdf, last accessed March 29, 2015 (“If a company makes materially misleading statements or omissions about a matter, including data security, and such statements or omissions are likely to mislead reasonable consumers, they can be found to be deceptive in violation of Section 5 [15 U.S.C. § 45]. Further, if a company’s data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and violate Section 5.”).


27. See id.; Home Depot, Quarterly Report supra n.25.


29. Id.

30. See Stone ex rel. AmSouth Bancorporation v. Ritter, 911 A.2d 362 (Del. 2006); see also Mills Acquisition Co. v. Macmillan, Inc., 559 A.2d 1261 (Del. 1989); Aronson v. Lewis, 473 A.2d 805 (Del. 1984), overruled in part by Brehm v. Eisner, 746 A.2d 244 (Del. 2000). Similarly, the Model Business Corporation Act § 8.30(b) (3d ed. 2003) provides that board members “shall discharge their duties with the care that a person in a like position would reasonably believe appropriate under similar circumstances.”


32. Id. at 979.

33. Id. at 971.

34. Stone, 911 A.2d at 364 (quoting Caremark, 698 A.2d at 971).


36. 964 A.2d at 131.


38. 2014 WL 5341880.

39. Id. at *6 n. 1.


41. Aguilar, supra n.35.


