Bloomberg BNA

Privacy and Security Law Report®

Five Issues Directors of Consumer and Retail Companies Should Consider Immediately Following a Cybersecurity Breach

By Melissa Sawyer and Audra Cohen

If you are a director of a consumer or retail company, someday soon (if you haven't already) you will probably get that dreaded call from the chief executive officer informing you that your company has suffered a data security breach. Unfortunately, you will be in good company. In the past few years, Target Corp., Home Depot Inc., Neiman Marcus Group Ltd., Michaels Stores Inc., Sally Beauty Holdings Inc., Albertsons LLC, SuperValu Inc., Apple Inc., Sony Corp. and many others have all suffered various types of cybersecurity breaches.

Melissa Sawyer is a partner in Sullivan & Cromwell LLP's Mergers & Acquisitions Group in New York, focusing her practice on a variety of corporate governance, M&A and private equity matters. Her experience spans multiple industries, including consumer and retail, health-care and life sciences, cybersecurity, insurance and industrials.

Audra Cohen is a partner in Sullivan & Cromwell's Mergers & Acquisitions Group in New York. Her expertise includes public company mergers, negotiated sales of private companies and spin-offs and advising boards of directors on corporate governance matters, including with respect to cybersecurity issues. Cohen is co-head of the firm's Consumer & Retail Group.

The views and opinions expressed in this article are those of the authors and don't necessarily represent those of Sullivan & Cromwell or its clients.

There are many different types of cyberthreats, including cybercriminals, hactivists, nation states and employee thefts or intrusions. Many recent incidents involved theft of customers' personally identifiable information (PII). Retail companies in particular seem to be tempting targets for cyber thieves, perhaps because they have so much customer information and rely on public, user-friendly interfaces. Studies show that about 22 percent of known 2013 data breaches were in the retail sector, and in 2014 over 61 million records were stolen from retailers in cyberattacks.[1] Though the number of breaches reported by retailers dropped by 50 percent since 2012, the perpetrators were able to impact a far greater number of victims with each incident and the number of retail records reported compromised has soared.[2]

Much has been written recently about directors' responsibility to oversee a company's cybersecurity preparedness before a breach occurs. But what should directors do in the immediate aftermath of a breach? Directors are not expected to be experts in the technological aspects of cybersecurity, so their role usually is not to direct information technology employees' efforts to restore firewall protections, for example. They should, however, be prepared to direct management's overall response, and ensure adequate resources are dedicated to the issue and that information is communicated to stakeholders appropriately. More specifically, this article summarizes five areas where directors can and should provide oversight and input in the immediate aftermath of a cybersecurity breach, even if the directors do not have any special expertise in the relevant technological aspects of the breach.

1. Take Steps to Ensure That Management Is Implementing Its Response Plan

The board should confirm that management has prepared and is periodically reviewing a response plan for

[1] ICR, *It's Not a Matter of If, but When: Data Security Preparedness & Response*; Verizon, *2013 Data Breach Investigations Report* (2013); Press Release, IBM, IBM Study: Number of Cyber Attacks on Retailers Drops by Half; Criminals Still Stole Over 61 Million Customer Records in 2014 (Jan. 5, 2015).

[2] David McMillen, *IBM: Industry Overview: Retail, Research and Intelligence Report* (Jan. 5, 2015).

cybersecurity attacks. It is becoming best practice for companies to implement a self-assessment using the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Framework).[3] Among other things, the NIST Framework contemplates that companies should have procedures in place both to respond to and to recover from a cybersecurity breach. These procedures include designating who on the management team is responsible for monitoring and leading the company's response. Many companies now even test their response plans in advance through simulated cyberattack exercises. Companies that follow the NIST Framework typically rely on penetration or vulnerability testing.

The response plan likely will have very complex technological components designed to stop the breach and secure the company's networks. However, the plan should also include a sequence of other response protocols, such as:

- communications to any law enforcement or regulatory authorities the company is required to (or should otherwise) notify;
- communications with cyberattack information sharing platforms/industry groups;
- communications to customers, insurers, vendors (including any communications that the company is required to make under contracts with third parties whose systems may have been compromised by the attack on the company), employees and shareholders;
- notifications to potential victims of the cyberattack to the extent the breach resulted in a theft of customer, employee or other third-party PII or other data;
- notifications to appropriate external technical experts and other outside advisers, such as public relations firms and outside counsel, who should have been engaged in advance of the attack as part of the company's preparation of a response plan; and
- preserving evidence associated with the breach (crime).

We expect participation in information sharing platforms will proliferate in light of the Feb. 13 executive order, ''Promoting Private Sector Cybersecurity Information Sharing,'' which fosters the development of ''information sharing and analysis organizations'' on the basis of sector, sub-sector and other affinities.[4] Currently, for example, the Retail Cyber Intelligence Sharing Center (R-CISC) functions as a forum for retailers to share threat information and best practices with each other.[5] In late March 2015, the R-CISC launched a cyber-sharing portal supported by the financial services information sharing and analysis center. Helpfully, the Department of Justice and the Federal Trade Commission have both confirmed that they do not believe antitrust is a roadblock to legitimate cybersecurity information sharing between private entities.[6] Companies should take advantage of the potential for more sharing of cybersecurity information and use the information they can now obtain through the ISACs to refine their own response plans.

It is critical that the company speak with "one voice" in all public communications concerning the incident.

2. Expect the Stock Price to React

A 2013 study reported that companies lose 0.4-0.5 percent of their market value whenever a privacy breach is announced.[7] However, it is possible the market will punish a company even more if it perceives that the company's response to the attack is being mishandled. For this reason, it is critical that the company speak with ''one voice'' in all public communications concerning the incident.

Following a cyberattack, the board should discuss with management what information, if any, the company should provide to the market regarding the attack's impact on business continuity, revenues, customer relationships, remediation costs and the other costs of implementing the company's response plan, as well as what other economic and reputational exposures the company may suffer as a result of the attack. The Securities and Exchange Commission has published disclosure guidance that details public companies' disclosure obligations in their SEC reports relating to cybersecurity risks and incidents, so SEC-registered companies need to consider what level of detail they will provide on an ongoing basis on cyber breach risks, incidents and consequences in their SEC filings.[8] Even so, according to a recent Willis North America Inc. survey, 9 percent of retail companies in the Fortune 1000 were silent on cyber risks in their annual reports on Form 10-K.[9] This may be because determining whether risk of a breach is sufficiently ''material'' to be disclosed is not always straightforward, and companies understandably may fear disclosing system vulnerabilities in a manner that can make the system even more vulnerable. In addition, companies may need to balance trans-

[3] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014) (13 PVLR 281, 2/17/14).

[4] Office of the Press Secretary of the White House, Promoting Private Sector Cybersecurity Information Sharing (Feb. 13, 2015) (14 PVLR 324, 2/23/15).

[5] Retail Cyber Intelligence Sharing Center, http://www.r-cisc.org/; Willis North America, Inc., *Willis Special Report: 10K Disclosures—How Retail Companies Described Their Cyber Liability Exposures* (April 2014).

[6] DOJ & FTC, *Antitrust Policy Statement on Sharing of Cybersecurity Information* (Apr. 10, 2014) (13 PVLR 653, 4/14/14).

[7] ICR, *It's Not a Matter of If, but When: Data Security Preparedness & Response*; Will Gangewere, Assessing the Impact of a Privacy Breach on a Firm's Market Value (Dec. 2013) (unpublished thesis, Duquesne University).

[8] SEC Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2: Cybersecurity* (Oct. 13, 2011) (10 PVLR 1495, 10/17/11).

[9] Willis North America, Inc., *Willis Special Report: 10K Disclosures—How Retail Companies Described Their Cyber Liability Exposures* (Apr. 2014). According to the report, the retail sector was much less likely to be silent on the issue than the Fortune 1000 as a whole (19 percent).

  PVLR ISSN 1538-3423

parency in disclosures with respect to a cyber breach against law enforcement needs in relation to the attack.

3. Prepare for Litigation; Consider Potential Litigation in Formulating Your Response

As all directors are aware, litigation is a predictable result of a company's announcing bad news. Recent experience has shown that plaintiffs have many potential angles to pursue remedies in connection with a cybersecurity breach.

Shareholder Derivative Litigation. Importantly, directors themselves may become defendants in shareholder derivative actions relating to cyberattacks. The theory of these suits, which have been filed against both Target and Wyndham Worldwide Corp. in connection with cyberattacks, for example, is that the directors failed to comply with their duty of ''oversight''.[10]

''Oversight'' claims (sometimes known as *Caremark*[11] claims) may be styled as breach of duty of loyalty claims, rather than duty of care claims. This is a very important distinction from a director's perspective, because directors are usually insulated from personal liability for duty of care claims, but companies cannot exculpate directors from personal liability for duty of loyalty claims. Further, the very deferential business judgment standard of review under which duty of care claims are typically reviewed is not applicable to breach of duty of loyalty claims.

Lately, more states have adopted or tightened consumer protection statutes to protect consumers' PII, and as a result future consumer suits may gain more traction.

That being said, some of the same facts that a director may use to defend a due care claim can also help to show that directors properly oversaw the company's cyber risk profile. ''Oversight'' claims usually rest on the presumption that directors allowed a situation to develop and continue, causing the company to suffer a loss, and failed to be active monitors of the company's performance. It is helpful in these cases to demonstrate that the board was informed and reviewed with management the steps being taken to prevent a cybersecurity breach from occurring and that the company had in place a rapid response plan to address any such cybersecurity breach.

Stock Drop Litigation. Another category of potential shareholder suits relating to cyberattacks is so-called ''stock drop'' litigation. The plaintiffs' theory in these cases is usually that the defendant company suffered a steep drop in its share price that is attributable to the company's alleged misstatements concerning its cybersecurity protections. Such cases may gain more traction now in the wake of the SEC's enhanced disclosure guidance in SEC reports for cyber risks, consequences and incidents.

Negligence Claims by Third Parties, Including Claims by Financial Institutions/Card Issuers. The Target data breach also generated claims by card issuers against Target. The claims alleged that Target negligently disabled a data security feature and that the card issuers suffered harm as a result.[12] A district court upheld the claims under state law, finding that the financial institutions were foreseeable victims of Target's alleged negligence.[13] Target's $19 million dollar settlement proposal to MasterCard Inc. was recently rejected by MasterCard's three largest U.S. credit-card issuers (Citigroup Inc., Capital One Financial Corp. and JP Morgan Chase & Co.) because it was considered insufficient to cover the costs of fraudulent unauthorized purchases and reissuance of cards that resulted from the breach.[14] In general, these types of actions should be viewed as a subset of potential claims by third parties that do business with a company and could suffer losses in connection with a cyberattack against the company. Theoretically, vendors and others whose systems connect with those of an affected company could also make claims for negligence if a company's cyber vulnerabilities result in a proliferation of a virus or other cyberthreat into a third party's systems.

Consumer Claims. To date, consumer claims have not gained significant traction in cyberattack situations. For example, a Delaware consumer protection statute requires companies to destroy records containing consumer PII, but consumers have to show that they incurred actual damages due to a reckless or intentional violation of the statute before they can succeed in a civil action to obtain damages.[15] Plaintiffs have had difficulty convincing courts that the risk of data being misused in the future is a sufficiently concrete and particularized, or actual and imminent, source of harm to warrant the recovery of damages.[16] Lately, however, more states have adopted or tightened consumer protection statutes to protect consumers' PII, and as a result future suits may gain more traction.

FTC Enforcement Actions. Section 5(a) of the FTC Act prohibits ''acts or practices in or affecting commerce'' that are ''unfair'' or ''deceptive.''[17] The FTC has brought Section 5 claims over 50 times against companies that employ what the FTC labels ''weak data practices'' that put consumers' PII at risk.[18] Most companies settle with the FTC.[19] However, one of these cases, in-

[10] Amended Complaint, *Kulla v. Steinhafel*, No. 14-cv-00203 (D. Minn. July 18, 2014); Complaint, *Palkon v. Holmes*, No. 2:14-cv-01234 (D.N.J. May 2, 2014) (13 PVLR 839, 5/12/14); Francis J. Burke, Jr. & Steven M. Millendorf, *Cybersecurity and Privacy Enforcement: A Roundup of 2014 Cases*, American Bar.

[11] *In re Caremark Int'l, Inc. Deriv. Litig.*, 698 A.2d 959 (Del. Ch. 1996).

[12] *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304 (D. Minn. Dec. 2, 2014) (13 PVLR 2058, 12/8/14).

[13] *Id.*

[14] Robin Sidel, *Three Banks Put Kibbosh on Target Pact*, Wall St. J., June 3, 2015.

[15] Safe Destruction of Records Containing Personal Identifying Information, Del. Code Ann. tit. 6, § § 5001C, 5002C, 5003C, 5004C (2014).

[16] Dana Post, *Plaintiffs Alleging Only ''Future Harm'' Following a Data Breach Continue to Face a High Bar*, The Privacy Advisor, Jan. 28, 2014.

[17] 15 U.S.C. § 45(a).

[18] Allison Grande, *Wyndham, FTC Data Security Row Heads to Mediation*, Law360, Nov. 19, 2014.

[19] *Id.*

volving Wyndham, is currently on interlocutory appeal in the U.S. Court of Appeals for the Third Circuit.[20] The FTC has alleged Wyndham failed ''to maintain reasonable and appropriate data security for consumers' sensitive personal information.''[21]

Tort Claims. As consumer companies increasingly develop the ''Internet of things'' (the connection of physical devices such as home appliances and cars to the Internet), the potential for cyber breaches to result in physical harm increases. The media is already speculating about the ability of terrorist hackers to take control of aircraft and autos, for example.[22] Should that happen, the litigation risk profile of consumer companies will undoubtedly increase.

Other. In addition, companies subject to cyberattacks that result in the theft of employees' personal information may be subjected to employee claims. Companies could also find themselves involved in criminal probes relating to the attack.

4. Consider Other U.S. and Non-U.S. Compliance Issues

State laws relating to data security issues continue to evolve. Therefore, directors confront a moving target in terms of the types of compliance issues they need to ensure are taken into account by management in the wake of a cyberattack. These issues should all be addressed as part of the company's response plan, but they are worth mentioning here in more detail. For example, California adopted legislation to require any owner or licensor of computerized data that includes personal information (e.g., Social Security number, driver's license number, etc.) belonging to a California resident to notify that California resident in the event that his or her personal information is, or is reasonably believed to be, acquired by an unauthorized person.[23] Forty-six other states and the District of Columbia have subsequently adopted similar legislation, which is sometimes even more stringent than California's original statute.[24] California itself subsequently added additional notification requirements and requires the source of the breach to offer identity theft prevention mitigation services at no cost to the affected person for no less than 12 months if a Social Security number or driver's license number is stolen.[25]

Just as the legal and compliance landscape is evolving, so are ''best practices'' for addressing cybersecurity. For example, the California attorney general has released a data breach report with specific recommendations for retailers.[26] In addition, PCI DSS (the Payment Card Industry Data Security Standard, an information security standard for organizations that process debit and credit cards) includes 12 comprehensive requirements ranging from encrypting cardholder data to assigning a unique ID to each person with computer access to auditing network access.[27] Failure to meet those requirements can result in fines. Some states (including Washington, Minnesota and Nevada) have incorporated all or parts of PCI DSS into their state statutes, providing that businesses are exempt from liability for certain types of security breaches if they are PCI DSS compliant.[28] The PCI DSS standards continue to evolve (for example, in October, the PCI Security Standards Council published new recommendations for how to train staff to protect sensitive payment information).[29] To the extent PCI DSS releases additional protocols regarding steps to take in the aftermath of a breach, directors should make sure management includes compliance with those additional protocols in the company's rapid response plan.

Some states have incorporated all or parts of PCI DSS into their state statutes, providing that businesses are exempt from liability for certain types of security breaches if they are PCI DSS compliant.

Directors of companies that have sales, assets or employees in jurisdictions outside the U.S. should also make sure that management is familiar with the data protection requirements of those jurisdictions. Europe in particular has extensive data privacy protections that extend, among other things, to data about employees.

To the extent the board, in consultation with counsel, determines it makes sense to conduct an internal investigation into the source of a cyberattack, the board should consider having the company engage outside counsel first and then having that outside counsel engage contractors to conduct the investigation to help ensure attorney-client privilege remains available.

5. Confirm What Coverage Is Available Under Insurance Policies

Prior to a cyberattack, directors should ensure that management has assessed the company's insurance

[20] *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (13 PVLR 619, 4/14/14), appeal docketed, No. 14-3514 (3d Cir. argued March 3, 2015) (14 PVLR 9, 1/5/15). The appellants have challenged the FTC's authority to police corporate cybersecurity practices. *Id. See also* Steven Caponi, *Wyndham Secures Interlocutory Appeal Challenging the FTC's Authority to Regulate Cybersecurity Practices*, Cyber Security Law Watch, June 27, 2014.

[21] *FTC v. Wyndham Worldwide Corp.*, No. 13-1887 (ES), 2014 BL 173985 (D.N.J. June 23, 2014) (13 PVLR 1161, 6/30/14).

[22] Alex Hern, *Wi-Fi on Planes Opens Door to In-Flight Hacking, Warns US Watchdog*, The Guardian, Apr. 15, 2015; *Defending the Digital Frontier*, The Economist, July 12, 2014; Eric Tegler, *Cyber Threats Targeting Your Car*, AutoWeek, Oct. 14, 2013.

[23] Cal. Civ. Code § 1798.29.

[24] Tom Kemp, *Buckle Up with Cybersecurity . . . It's the Law*, Forbes, Feb. 1, 2012.

[25] Cal. Civ. Code § 1798.82.

[26] Kamala D. Harris, Attorney General, California Department of Justice, *California Data Breach Report* (Oct. 2014) (13 PVLR 1912, 11/3/14).

[27] *Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures*, version 3.1 (Apr. 2015) (14 PVLR 762, 4/27/15).

[28] Minnesota Plastic Card Security Act, Minn. Stat. § 325E.64 (2007); Nev. Rev. Stat. § 603A (2010); Nev. S.B. 227 (2009); Wash. H.B. 1149 (2010); Kemp, *supra* note 24.

[29] PCI Security Standards Council, *Information Supplement: Best Practices for Implementing a Security Awareness Program* (Oct. 2014) (13 PVLR 1940, 11/10/14).

  PVLR ISSN 1538-3423

coverage with respect to cyber-related matters. Historically, some business interruption, crime and fidelity policies have contained exclusions for cyberattacks, and it may be appropriate to secure additional coverage for cyber-related matters.[30] Likewise, directors and officers (D&O) policies may not provide full coverage for directors in the event of ''oversight'' claims against directors in the wake of a cyberattack. In any event, directors should challenge management to continually review insurance policy coverage and developments as part of the company's response plan. After a breach occurs, the board should task management with exploring all potential avenues for insurance recoveries.

* * *

Over the longer term, in the wake of a cyberattack and more generally as incidents are reported and the landscape changes, the board should certainly review ''lessons learned'' with management. These post-mortem and other reviews may include assessing whether the company would benefit from additional or different technology investments, better employee training and enhanced protocols for dealing with third-party providers, among other things. And, of course, public and investor relations will continue to be critical as the directors will inevitably have to deal with a certain degree of company-wide and personal reputational fallout from an attack on the company or similar companies. For example, Institutional Shareholder Services (ISS) recommended against Target's board members in the 2014 proxy season on account of their alleged failure to manage cybersecurity risks.[31] ISS's recommendation focused on directors who served on Target's audit and corporate responsibility (i.e., risk management) committees. ISS opined that Target's board's reaction to its data breach appeared ''largely reactionary.'' The more directors can demonstrate that their company had well-considered response plans prepared in advance and that they were proactive in the wake of a breach, the better directors (and shareholders) will fare.

[30] Taylor Armerding, Cyber Insurance: *Worth It, But Beware of the Exclusions*, CSO, Oct. 20, 2014.

[31] Paul Ziobro & Joann S. Lublin, *ISS's View on Target Directors Is a Signal on Cybersecurity*, Wall St. J., May 28, 2014.