Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity: What Directors Need to Know in an Era of Increased Scrutiny

BY KIMBERLY PERETTI AND JESSICA CORLEY

Since the financial crisis, corporate governance has increased the focus on risk management. And, in recent years, cybersecurity has increasingly become a key issue in risk management due in large part to the growing realization that most company's assets are digital, and that most systems are networked and connected to the Internet, leaving such assets subject to any number of targeted cyberattacks from increasingly sophisticated threat actors, including state actors with unlimited resources to conduct such attacks. In a recent study of 63,436 incidents investigated by Verizon Enterprise Solutions, 1,367 security incidents with confirmed data loss occurred in 2013.[1] Some of those attacks were large-scale attacks on payment card systems, resulting in unprecedented exposure for the victim companies.[2]

[1] Verizon, *2014 Data Breach Investigations Report* 6 (2014).
[2] *Id.* at 3.

Kimberly Peretti is a partner at Alston & Bird LLP in Washington. She is a member of the firm's White Collar Crime Group and co-chair of the Security Incident Management & Response Team.

Jessica Corley is a partner in Alston & Bird's Atlanta office and serves as the chair of the firm's Securities Litigation Group.

Kelley Barnaby, a senior associate in firm's Litigation & Trial Practice Group in Washington, and Lauren Tapson, an associate in the firm's Securities Litigation Group in Atlanta, contributed to this article.

As the number of data breaches increases, and the occasional breach with millions of records impacted continues to receive widespread and far-reaching publicity, so does scrutiny surrounding those breaches. Such scrutiny includes increased regulatory interest in the cybersecurity practices of companies, both before and after an incident. At the federal level, in the past several years, the Securities and Exchange Commission (SEC), in an effort to protect shareholders, has shown growing interest in cybersecurity issues, perhaps second only to the Federal Trade Commission (FTC).[3] Such interest has manifested itself through cyber risk disclosure guidance, round table discussions, cybersecurity enforcement actions, speeches (including those specifically addressing cyber risk and the Board), and importantly, proactive staff examinations focused on the cybersecurity practices of regulated companies.

"[B]oards that choose to ignore, or minimize, the importance of cybersecurity responsibility do so at their own peril."

LUIS A. AGUILAR, SEC COMMISSIONER[4]

In addition to increased regulatory scrutiny, companies are also facing a growing number of lawsuits related to data breaches and security incidents, including those brought by shareholders. In the past several months, two organizations victim to payment card breaches orchestrated by organized criminal groups have faced lawsuits seeking to hold corporate directors and officers liable for damages arising from these costly security incidents based on theories of breach of fiduciary duty and corporate waste.

In this era of increased cybersecurity scrutiny and litigation, it is imperative that directors educate themselves on the risks the company may face related to cybersecurity, as well as those risks that any director may

[3] Allison Grande, *SEC's the New Sheriff in Town on Cybersecurity*, Law360, June 16, 2014.
[4] Luis A. Aguilar, SEC Commissioner, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Speech at the New York Stock Exchange (June 10, 2014), *available at* http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.U59X4SgVe5N (13 PVLR 1063, 6/16/14).

 ISSN 1538-3423

face individually. Board members must also involve themselves in the company's cybersecurity strategy before and after a data breach. This article will discuss the developing cyber risk landscape, the increased regulator interest in cybersecurity, particularly from the SEC, and the impact on potential director liability of cybersecurity deficiencies (or perceived deficiencies). This article will conclude with practical guidance to help board members navigate the all-too-unfamiliar cyber risk and cybersecurity landscape.

I. The Cyber Risk Landscape

The risk exposure for cyberattacks continues to rapidly increase. Once a risk involving one-time smash and grabs by intellectually curious teenagers, cyber risk has quickly evolved into cybercrimes involving deep and prolonged access to hundreds of systems by various advanced-threat actors with a variety of malevolent motives. This shift has dramatically altered the risk profile presented by a cybersecurity incident, and such an incident is now more likely to result in heavy financial losses, enforcement actions and lawsuits against the company and its officers and directors.

Indeed, in the past two years the cost of a data breach to a company has increased. A breach costs on average $201 per record, totaling, on average, $5.9 million, including $3.2 million in costs associated with above-normal customer turnover, increased customer acquisition activities, reputation losses and diminished goodwill.[5] Above-normal customer turnover following a data breach has increased 15 percent over the prior year.[6]

With the increase in the number of breaches and the number of consumers or individuals impacted comes increased interest from local and national media. More than 254 data breaches have been publicized in 2014, a 233 percent increase from last year.[7] Media scrutiny not only contributes to the potential damages to a company's reputation, but also increases the likelihood of claims against the company. For example, Target Corp.'s much-publicized breach has led to at least 30 bank cases, more than 80 consumer cases and four shareholder cases, all of which have been consolidated into one multidistrict litigation proceeding.

Even where the incident does not involve an immediate notification obligation guaranteed to bring media attention, federal law enforcement's expansion of the types of cybercrimes and bad actors it investigates and prosecutes *criminally* means companies should increasingly expect future publicity of previously unreportable events—for example, by being named as victims in criminal indictments. Recently, three U.S. public companies were among the victims named in the first-ever criminal indictment of state-sponsored actors for cyber espionage activities.[8] The companies found themselves receiving scrutiny for not previously disclosing the cyberattacks after the Department of Justice indicted several Chinese officials for carrying out the attacks, which involved the theft of trade secrets and other data, to investors in filings.[9] Although the companies have maintained that the thefts were not ''material,'' U.S. Attorney General Eric Holder stated when announcing the indictment that information ''stolen in this case is significant.''[10] These events create opportunity for increased investor scrutiny.

This increased attention is being felt in the boardroom. Following Target's much-publicized 2013 data breach, proxy advisory firm Institutional Shareholder Services Inc. (ISS) urged shareholders to vote out seven of Target's 10 board members for allegedly mishandling the data breach. In a report supporting the recommendation, ISS focused on ''the board's alleged failure to manage risk and protect Target from the massive data breach.''[11]

However, investor reaction to data breaches is unpredictable. For example, following eBay Inc.'s May 2014 notice of a data breach affecting consumer information, investors appeared unfazed, leading some analysts to conclude that investors ignore these events.[12] While investors may be apathetic to the continued stream of incident reporting, causing what many have labeled as ''breach fatigue,'' they certainly are likely to pay more attention to an enforcement action or private litigation regarding an organization's security practices that is the result of proactive or reactive assessments of cybersecurity practices by regulatory authorities.

II. Increased Regulator Scrutiny

While previously an almost exclusive domain for reactive inquiries following a publicized security incident, recently regulators across industries at the federal and state level have increased their proactive inquiry of cybersecurity practices of companies. Examples include the Federal Communications Commission (FCC) (announcing a ''new regulatory paradigm'' in which the FCC will develop a risk assessment tool for the telecommunications industry),[13] the Food and Drug Administration (FDA) (actively analyzing cybersecurity threats related to medical devices)[14] and the New York Depart-

---

[5] Ponemon Institute, *2014 Cost of Data Breach Study: United States* 1–2 (May 2014). The total cost increased eight percent.

[6] *Id.* at 1.

[7] Press Release, SafeNet Inc., Data Breaches Surge in 2014 with 200 Million Data Records Stolen in First Three Months of the Year (Apr. 29, 2014).

[8] Devlin Barrett & Siobhan Gorman, *US Charges Five in Chinese Army With Hacking*, Wall St. J., May 19, 2014, http://online.wsj.com/news/articles/SB10001424052702304422704579571604060696532 (13 PVLR 905, 5/26/14).

[9] Chris Strohm, Dave Michaels, et al., *Chinese Hacking Raises Cyber Attack Disclosure Issue for Companies*, Ins. J. (May 21, 2014), *available at* http://www.insurancejournal.com/news/national/2014/05/21/329707.htm.

[10] *Id.*

[11] Linda Chiem, *7 Target Board Members in ISS' Crosshairs Over Data Breach*, Law360, May 28, 2014. All Target directors were re-elected June 11. Press Release, Target Corp., Target Announces Voting Results from 2014 Annual Meeting of Shareholders (June 13, 2014), *available at* http://pressroom.target.com/news/target-announces-voting-results-from-2014-annual-meeting-of-shareholders.

[12] Eric Chemi, *Investors Couldn't Care Less About Data Breaches*, Bloomberg Businessweek (May 23, 2014), *available at* http://www.businessweek.com/articles/2014-05-23/why-investors-just-dont-care-about-data-breaches.

[13] *See* Lou Dennig, *FCC Chairman Outlines Industry-Led ''New Regulatory Paradigm'' for Cybersecurity Leveraging NIST Framework*, Alston Privacy + Security Blog (June 14, 2014), http://www.alstonprivacy.com/blog.aspx?entry=5337.

[14] *See Cyber Attacks on Human Health? FDA Urges Manufacturers to Tighten Cybersecurity on Medical Devices*, Alston

  PVLR ISSN 1538-3423

ment of Financial Services (launching an initiative to assess insurance companies' cybersecurity policies by sending out so-called ''308'' letters).[15] Notably, the SEC's Office of Compliance Inspections and Examinations (OCIE) has launched an initiative to assess the cybersecurity preparedness of 50 registered broker-dealers and registered investment advisers,[16] and focuses on:

> the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.[17]

In conjunction with the announcement of the initiative, the OCIE published a sample list of requests for information that the OCIE may use in conducting the examinations—a rare disclosure.[18] Notably, this list provides valuable insight into the types of inquiries that regulators may make and the types of practices that they may expect organizations to have in place related to cybersecurity matters.

In the midst of this proactive interest, the National Institute of Standards and Technology (NIST) finalized a year-long process to create a Cybersecurity Framework (''Framework'') in response to Executive Order 13636.[19] Directly applicable to the 16 identified critical infrastructure sectors,[20] the Framework is a voluntary tool for reducing cybersecurity risk that identifies beneficial cybersecurity practices and creates a common language for discussing those practices. Whether the Framework is truly voluntary for critical infrastructure entities is a matter of much debate. Recent regulator statements suggest that regulators will look to the Framework as instructive guidance and expect companies to be actively considering its relevance to their organization. Such a position was recently articulated by SEC Commissioner Luis A. Aguilar, who stated that ''boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines—and whether more may be needed.''[21] Moreover, while the broader adoption of the Framework outside of critical infrastructure sectors remains to be seen, the Framework foretells potential increases in the expectations for baseline security for organizations across the board.

III. Impact on Potential Director Liability for Cybersecurity Deficiencies

Because cybersecurity is in the spotlight in both the public and private sector, corporate directors and officers are expected now more than ever to be fully engaged in overseeing their companies' cybersecurity protections and responses.

A. Important Legal Standards and Recent Trends in Cybersecurity Litigation

Lawsuits against individual directors and officers will most likely arise in the form of shareholder derivative actions and securities fraud class actions. In derivative actions, claimants typically assert that the directors breached their duties of care to the company. The duty of care is an oversight obligation that entails ''a duty to attempt in good faith to assure that a corporate information reporting system, which the board concludes is adequate, exists, and that the failure to do so . . . may . . . at least render a director liable for losses caused by non-compliance with applicable legal standards.''[22] Another possible derivative claim is that directors' actions wasted corporate assets. For both claims, directors' decisions are protected by the business judgment rule if the decisions are informed and made in good faith.

After a widespread data breach jolted Target in 2013, four derivative suits have been consolidated against Target's directors and officers in the U.S. District Court for the District of Minnesota.[23] These cases allege breach of fiduciary duty, waste of corporate assets, gross mismanagement and abuse of control. Under similar circumstances, a shareholder for Wyndham Worldwide Corp. filed a derivative lawsuit earlier this year after three data breaches allegedly resulted in the theft of more than 619,000 consumer payment card account numbers.[24] The complaint alleges breach of fiduciary duties, corporate waste and unjust enrichment against certain directors and officers for failing to implement adequate security policies or update the company's security systems, and for aggravating the damage by failing to timely disclose the data breaches in the company's public filings.[25] As discussed below,

---

& Bird Cyber Alert, (June 20, 2013), http://www.alston.com/publications/cyber-alert-FDA-tighted-cybersecurity-medical-devices/ (12 PVLR 1055, 6/17/13).

[15] *See* Kimberly Peretti, *New York State Inquires into Insurance Company Cybersecurity Practices: A Signal of Increased Proactive Regulator Interest in Data Security?*, Alston & Bird Cyber Alert (June 4, 2013), http://www.alston.com/Files/Publication/b9785fea-f457-46b8-9739-e1c558ff2d63/Presentation/PublicationAttachment/61c0d644-bb3f-49f9-a1f4-ecea6a9defce/Cyber-Alert-New-York-State-Inquiries-into-Insurance-Company-Cybersecurity-Practices.pdf (12 PVLR 970, 6/3/13).

[16] OCIE, *National Exam Program Risk Alert* 1 (Apr. 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf (13 PVLR 673, 4/21/14).

[17] *Id.* at 2. The Financial Industry Regulatory Authority (FINRA), which regulates brokers and brokerage firms, is coordinating with the SEC and is also conducting a broad assessment of firms' approach to cybersecurity. FINRA, *Target Examination Letters Re: Cybersecurity* (Jan. 2014), http://www.finra.org/Industry/Regulation/Guidance/TargetedExaminationLetters/P443219 (13 PVLR 291, 2/17/14).

[18] *See National Exam Program Risk Alert*, *supra* note 16, at 3.

[19] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (13 PVLR 281, 2/17/14).

[20] For a list of critical infrastructure sectors, *see* http://www.dhs.gov/critical-infrastructure-sectors.

[21] Aguilar, *supra* note 3.

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

[23] *See* Verified Shareholder Derivative Complaint, *In re Target Corporate Shareholder Derivative Litig.*, No. 0:14-cv-00203-PAM-JJK (D. Minn. Jan. 21, 2014).

[24] *See* Verified Shareholder Derivative Complaint, *Palkon v. Holmes*, No. 2:14-cv-01234-SRC-CLW (D.N.J. May 2, 2014) (13 PVLR 839, 5/12/14).

[25] *Id.* The Wyndham derivative action was filed on the heels of a widely publicized FTC proceeding against the company for the cyber breaches (13 PVLR 1161, 6/30/14). In fact, the de-

the claims in these cases stem from the directors' and officers' conduct before, during and after the breach. Although Target and Wyndham are not the first to endure fallout derivative litigation—TJX Companies Inc. dealt with similar suits arising from their 2007 data breach—the tendency for these cases to settle means there is little guidance from the courts in the cybersecurity context.

Securities fraud class actions are most likely to arise when a company's stock price drops proximate to disclosure of a data breach. In these lawsuits, shareholders allege that they relied—to their detriment—on a company's material misrepresentation, which in the context of a data breach could derive from, among other things, public statements about a company's cybersecurity protective measures, its risk level for a breach or the effect or pervasiveness of a breach once it has occurred. Liability in these cases is predicated in part on a showing that the misrepresentation was both material and made knowingly or recklessly.[26] Securities fraud actions can also be asserted against individual officers who make or have authority over the misrepresentation, such as in press releases or SEC filings.[27]

In securities class actions, courts may require a ''statistically significant'' decline in the company's stock price.[28] As a result, nonsignificant drops are less likely to give rise to securities class action suits. For example, when Apple Inc. announced attacks on its system in 2013, it did not experience a significant stock price drop and was not sued in a securities class action.[29]

On the other hand, where a significant stock decline occurs, companies should prepare for shareholder litigation. One example is Heartland Payment Systems Inc., a bank card payment processing services company that suffered a breach from which 130 million debit and credit card numbers were stolen in 2009.[30] Shortly after the data breach was disclosed, Heartland's stock price declined, peaking at an 80 percent drop.[31] The Heartland shareholders brought suit alleging that the company concealed a past cyberattack on its network and made fraudulent statements about the state of the company's cybersecurity.[32] The court dismissed the complaint, holding in relevant part that (1) the company's failure to disclose a past cyber incident was not a material omission; and (2) plaintiffs failed to allege with the requisite particularity that Heartland's directors and officers knew that Heartland's security systems were deficient or that the prior cyberattack was not adequately addressed.[33] Although *Heartland* is an example of the uphill battle faced by plaintiffs pleading federal securities fraud claims, courts consider a failure to disclose cyber incidents a material omission in light of recent SEC disclosure guidance, discussed below.

B. Increased Scrutiny of Disclosures

The growing risk of cyber incidents has the attention of both the plaintiffs' bar and various regulators. As a result, the sufficiency of corporate disclosures is under the microscope, and companies should be mindful of the increased risk of SEC comment letters, enforcement actions and private litigation that may arise in this context.

Although existing disclosure requirements do not explicitly mention cybersecurity, the SEC issued disclosure guidance in 2011 that explains the importance of incorporating cybersecurity issues into public disclosures.[34] Cybersecurity disclosures must address both cybersecurity risks and the company's history of breaches and attacks.[35] When disclosing cybersecurity risks, the SEC's guidance directs registrants to tailor their disclosures to their particular circumstances in order to ''provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant.''[36] Therefore, a boilerplate disclosure of general threats posed to cybersecurity will not be sufficient.[37]

Additionally, past material breaches must be disclosed, potentially in addition to past immaterial and attempted breaches.[38] The SEC guidance warns that ''a registrant may need to disclose known or *threatened* cyber incidents to place the discussion of cybersecurity risks in context.''[39] Companies should consider the prevalence of cybersecurity in preparing their registration statements, periodic reports and other required SEC filings, including disclosures of risk factors, management discussion and analysis (MD&A), description of business, legal proceedings disclosures and financial statements disclosures.[40]

The SEC highlighted its continued focus on cyber disclosures by holding a Cybersecurity Roundtable in March 2014, during which a panel on public company disclosure reiterated the importance of director involvement with cybersecurity decisions. SEC Chair Mary Jo White commented during opening remarks that ''[t]he SEC's formal jurisdiction over cybersecurity is directly focused on the integrity of our market systems, customer data protections, *and disclosure of material information*.''[41] Thus, although it is uncertain whether

---

rivative suit identifies the expense of defending the FTC's claims among its claimed damages. *See id.* at *24–26.

[26] *Matrixx Initiatives, Inc. v. Siracusano*, 131 S. Ct. 1309, 1317–18, 1323-24 (2011).

[27] *See Janus Capital Group, Inc. v. First Derivative Traders*, 131 S. Ct. 2296, 2301–03 (2011).

[28] *See, e.g., Greenberg v. Crossroads Sys., Inc.*, 364 F.3d 657, 653–55 (5th Cir. 2004); *In re Novatel Wireless Securities Litig.*, 830 F. Supp. 2d 996, 1019 (S.D. Cal. 2011).

[29] Apple announced the attacks on its system Feb. 19, 2013. Nicole Perlroth, *Apple Computers Hit by Sophisticated Cyberattack*, N.Y. Times Bits Blog (Feb. 19, 2013), http://bits.blogs.nytimes.com/2013/02/19/apple-computers-hit-by-sophisticated-cyberattack. That day Apple's stock opened at $461.10 and closed at $459.99. Yahoo! Finance, *Historical Prices, Apple Inc.*, http://finance.yahoo.com/q/hp?s=AAPL&a=01&b=1&c=2013&d=01&e=28&f=2013&g=d.

[30] *In re Heartland Payment Sys., Inc.*, No. 09-1043, 2009 BL 263160 (D.N.J. Dec. 7, 2009) (8 PVLR 1758, 12/14/09).

[31] *Id.*

[32] *Id.* at 1–2.

[33] *Id.* at 5–13.

[34] SEC, *CF Disclosure Guidance: Topic No. 2—Cybersecurity* (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (10 PVLR 1495, 10/17/11).

[35] *Id.* at 2–3.

[36] *Id.* at 3.

[37] *Id.*

[38] *Id.*

[39] *Id.* (emphasis added).

[40] *Id.* at 4–5.

[41] *See* Mary Jo White, Chair, SEC, Opening Statement at SEC Roundtable on Cybersecurity (Mar. 26, 2014), *available at* http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468 (emphasis added) (13 PVLR 550, 3/31/14).

  PVLR ISSN 1538-3423

the SEC will implement formal rules governing cybersecurity, disclosures on this topic are fully expected, and companies should defer to the available SEC guidance and other commentary in the meantime.

Directors and officers should also expect that shareholders will look to the company's SEC disclosures when drafting their complaint. For example, the Target shareholders point to a cybersecurity risk disclosure in Target's 2012 SEC Form 10-K to assert that the directors and officers were aware of the risks posed and failed to take preventative measures to address those risks.[42] Attempts to use a company's risk factors to support a claim turn the safe harbor protections of the Private Securities Litigation Reform Act on their head and should be rejected as a matter of law. As the Target case demonstrates, however, directors and officers should review their cyber risk disclosures very carefully and vet them fully with those employees responsible for cybersecurity.

IV. Practical Guidance

It is important for board members to be aware of their role in both pre-breach cybersecurity preparedness and post-breach oversight of the security incident and any follow-up on remediation measures.

A. Pre-Breach Oversight Responsibility

1. Cybersecurity and Corporate Governance

At the outset, and because information technology and cybersecurity are particularly technical disciplines, board members need to ensure that they have at least a basic knowledge or familiarity with the technical language to be able to ask the right questions and become adequately informed of the issues. SEC Commissioner Aguilar mentioned mandatory cyber risk education for directors or ensuring representation by directors with a good understanding of IT issues as two recommended practices.[43] He further suggested that boards may improve their technical expertise by establishing a separate enterprise risk committee.[44] Boards may also supplement their knowledge by hiring external consultants, but even if external consultants are engaged, the board should seriously consider creating a special committee to deal exclusively with cybersecurity and to ensure that the board is frequently and adequately briefed on cybersecurity issues. Identifying ways to overcome the obstacles presented by technical jargon and a technical discipline should be an initial first step for boards in tackling their pre-breach cybersecurity oversight role.

The board of directors should be particularly cognizant of its oversight responsibilities before a breach has occurred because shareholder plaintiffs are likely to target the strength and sufficiency of a company's cybersecurity measures as a cause of their losses. Accordingly, the board of directors should periodically evaluate the company's current cybersecurity procedures, protective measures and risk profile, and stay informed as risks, threats and other issues arise. The board should also consider the strength of the current system with respect to the level of risk to which the company is exposed and whether the company is equipped to handle these issues internally or if an external adviser should be engaged. If cybersecurity is handled externally, the board should further evaluate the process and diligence involved in selecting the company's vendors and other service providers (to the extent cyber issues are implicated) and the adequacy of employee training on these issues.

These considerations fall within the five key principles to govern oversight of cyber risks recently promulgated by the National Association of Corporate Directors, in conjunction with American International Group Inc. (AIG) and the Internet Security Alliance:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given regular and adequate time on the board meeting agenda.

4. Directors should set the expectation that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget.

5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.[45]

In addition, given the challenges of responding to security incidents with far-reaching exposure, one additional key principle is that the board should ensure that a specific cyber incident response plan is in place, has been properly tested and is ready for swift execution before a breach occurs.

2. Insurance Coverage

Given the increasing frequency of cybersecurity incidents, directors should consider purchasing cyber insurance to assist with the potentially massive costs of a data breach. Indeed, the SEC's 2011 guidance requires companies to describe mitigation techniques employed, including cyber insurance. General policies may not be sufficient to address the unique circumstances of cybersecurity, and some may have specific exclusions for data breaches. Stand-alone cyber insurance is tailored to cover security breach fallout, such as the costs of responding to a breach, lost income and operating expenses and losses arising from third-party claims. Additional services and coverage are also available, and like other types of insurance, cyber insurance coverage can vary in important ways. For example, some policies will only cover legally required notice to customers and will not cover voluntary notice. Another important consider-

[42] Verified Shareholder Derivative Complaint, *Collier v. Steinhafel*, No. 0:14-cv-00266 (D. Minn. Jan. 29, 2014), *consolidated as In re Target Corporate Shareholder Derivative Litig.*, No. 0:14-cv-00203-PAM-JJK (D. Minn.).

[43] Aguilar, *supra* note 3.

[44] *Id.*

[45] Larry Clinton, *Cyber-Risk Oversight*, at 4 (Nat'l Ass'n of Corp. Directors, Director's Handbook Series, 2014).

ation is whether the policy covers the cost of a post-breach forensics investigation and legal counsel.

Directors should also revisit their existing directors and officers (D&O) policy with inside or outside counsel to assess whether it is sufficient to cover the risk of derivative claims and shareholder class actions incident to a breach. Depending on the size of the company and its inherent cyber risks, directors should take time to assess the various policies on the market to ensure coverage sufficient for the company's unique needs.

3. Prepare for Potential Use of Internal Policies in Litigation

Shareholders may also use internal guidelines and policies around cybersecurity against companies and their directors in litigation. In the Target derivative litigation, the shareholders allege that the very fact Target had cybersecurity policies and advisory committees was evidence that the board was aware of the risks of an incident and failed to fulfill their fiduciary duties and prevent a breach.[46] Because the Target audit committee was charged with monitoring cybersecurity policies and procedures, members of the committee were specifically targeted for the breach of fiduciary duty claim.[47] Thus, boards should review company policies with advisers to ensure they are thorough and up-to-date. The board should also confirm with appropriate company management that the policies are being implemented and followed.

4. Consider Director Exculpation Clauses and Indemnification Agreements

Director exculpation clauses and indemnification agreements are important protections against personal liability for private suits arising from cyber incidents. An exculpatory provision in a company's corporate charter or bylaws can preclude certain cybersecurity claims altogether, which can protect directors not only from personal liability, but also from the stress and expense of lengthy litigation. Indemnity agreements are equally important because they can provide for advancement of defense costs during litigation and cover any settlements or monetary judgments when the case concludes. Therefore, directors should check the language of their exculpation clauses and indemnification agreements to ensure that cybersecurity fallout litigation is protected. Directors should bear in mind that exculpation clauses are typically limited by state law to duty of care violations and will not cover acts in bad faith. Indemnification agreements can vary widely in their coverage and also sometimes have exclusions for ''bad'' acts.

[46] Verified Shareholder Derivative Complaint, *Collier v. Steinhafel*, No. 0:14-cv-00266 (D. Minn. Jan. 29, 2014), *consolidated as In re Target Corporate Shareholder Derivative Litig.*, No. 0:14-cv-00203-PAM-JJK (D. Minn.).

[47] *Id.*

B. Post-Breach Oversight Responsibility

Although recent cybersecurity lawsuits are focused on the systems and controls that failed to prevent a breach, a company's response to a material breach can give rise to liability in both a disclosure and a due care context and should thus be treated with equal vigilance. For example, public comments made after a breach about the state of a company's security or the incident's repercussion could later be the subject of a securities class action.[48] Similarly, any alleged failure of oversight that could have caused or exasperated losses to the company could give rise to a derivative action. The board should take care to understand the incident response plan so that it may oversee its proper implementation. Indeed, during a response to a cybersecurity incident of any legal significance, the board of directors needs to become engaged and involved in directing the response and approving any proposed remediation plan. Moreover, understanding the nature of this role in advance of a breach will go a long way to effectively carrying out these oversight responsibilities in the wake of a cyber crisis firestorm.

V. Conclusion

Cybersecurity has become a spotlight issue, one which corporate directors and officers are expected to consider and manage. The increasing number and sophistication of cyberattacks has resulted in increased costs and increased scrutiny, and both regulators and shareholders have demonstrated a keen interest in cybersecurity issues. Federal regulators, such as the FCC, FDA and SEC, and state regulators are proactively inquiring into the cybersecurity practices of companies. This will likely expand the scope of companies that should consider adoption of NIST's Cybersecurity Framework. At the same time, private litigation has also been a growing avenue for addressing cybersecurity issues. Shareholder derivative actions and securities fraud class actions assert claims against directors and officers for breaches of the duty of care and waste of corporate assets stemming from cyberattacks. Regulator and shareholder interest also means increased scrutiny of disclosure statements, which now must address both cybersecurity risks and the company's history of breaches and attacks. In this landscape of increased exposure and increased scrutiny, directors and officers must be particularly cognizant of the oversight responsibilities they have for the company's cybersecurity.

For more information, please contact Alston & Bird's Security Incident Management & Response Team or Securities Litigation Group.

[48] *See, e.g., In re Heartland Payment Sys., Inc.*, No. 09-1043, 2009 BL 263160 (D.N.J. Dec. 7, 2009).

  PVLR ISSN 1538-3423