Westlaw Journal
DELAWARE CORPORATE
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 29, ISSUE 13 / JANUARY 5, 2015

EXPERT ANALYSIS

Shareholders, Regulators Clamp Down on Boards Over Corporate Governance of Cyberrisk

By William T. Um, Esq., and Paul T. Moura, Esq.
Hunton & Williams

Even as the dust begins to settle after the massive Target and Home Depot data breach revelations, those companies continue to face extraordinary expenses in responding to the breach events. The high cost of dealing with these events, including the cost of notifying consumers, identifying the source and paying for credit monitoring, have been widely publicized.

Consumer class-action lawsuits following these events are now so common that victimized companies have come to expect them. Moreover, lawsuits filed by financial institutions and credit card issuers seeking to recover costs incurred to rectify their customers' compromised financial information have added to the mix. At least one of these suits has survived a motion to dismiss.[1]

Amid these increasing costs, shareholders have begun to question the affected companies' leadership efforts to prevent, mitigate and respond to such breach events. Recent history suggests that derivative and shareholder actions alleging inadequate data security measures are likely to become more common.

In addition to shareholder actions, regulatory enforcement actions are on the rise. The Federal Trade Commission, and more recently the Federal Communications Commission, have begun to aggressively enforce data security requirements. These actions by shareholders and regulatory agencies raise the question of what steps companies and their boards should take to protect against the ever-increasing exposure to litigation costs arising out of corporate governance of cyberrisk. How much of a threat are they facing? And will directors' and officers' insurance cover such risks?

SHAREHOLDER ACTIONS ON THE RISE

Well aware of the playbook used in response to recent high-profile data breach events, companies affected by a massive data breach have come to expect class-action suits filed by consumers alleging privacy violations and unwarranted disclosure of their personal identification information. In addition, shareholder derivative actions are now adding a new front that companies will need to address.

The latest blockbuster data breach events have spurred criticism of corporate officers and directors regarding their policies on data security and allegedly lax efforts to prevent breaches.

In the Target case, the company announced that more than 100 million customers' credit and debit card information may have been compromised. One of the many lawsuits that followed accused the company of breaching its duty to implement procedures to detect and prevent the loss or unauthorized dissemination of consumers' private information while further claiming a violation of its duty to timely disclose the breach.[2]

Target's directors and officers were eventually hit with derivative lawsuits alleging breaches of fiduciary duty, gross mismanagement, waste of corporate assets and abuse of control.[3]

Target is not alone. In 2008, cybercriminals hacked into Heartland Payment Systems' network and recorded data from as many as 100 million credit and debit cards. Heartland soon faced class actions and various regulatory inquiries regarding the breach. Notably, Heartland was named in a shareholder suit alleging that its executives misrepresented the state of the company's computer network security and failed to disclose prior security incidents.[4]

The Wyndham hotel chain faced a similar shareholder challenge after hackers obtained the personal data of more than 600,000 of its customers. Shareholder Dennis Palkon filed a derivative lawsuit accusing Wyndham of failing to implement adequate cybersecurity measures. Palkon demanded that the company pursue a suit against the responsible executives. Although a New Jersey federal court granted the board members' dismissal motion — relying on the business judgment rule and the fact that the board took reasonable steps to investigate and consider Palkon's proposed measures[5] — company boards that fail to conduct such an investigation may not fare as well.

More recently, Home Depot suffered a similarly monumental data breach. Hackers apparently broke into the company's payment-card processing systems and stole data relating to as many as 40 million cards. Home Depot announced that, as of November, it was facing at least 44 breach-related lawsuits in addition to investigations by several states' attorneys general.[6]

These cases indicate that litigation costs for companies affected by large-scale data breach events will continue to increase because the plaintiffs' bar has added shareholder lawsuits to its collective response to breach events.

Target's directors and officers were hit with derivative lawsuits that alleged breach of fiduciary duty, gross mismanagement, waste of corporate assets and abuse of control.

REGULATORS STEP IN

In addition to shareholder lawsuits, federal agency enforcement actions have added to the cost of cyberincidents. The Federal Trade Commission has been leading the pack. In its latest actions , the FTC has emphasized the importance of establishing security practices to detect potential breaches before they occur.[7]

The FTC alleged that debt brokers Bayview Solutions LLC and Cornerstone & Co. LLC exposed consumers' personal information in interactive online marketplaces used for exchanging information about debt portfolios, all without any encryption, redaction or other measures to protect data security. The FTC concluded that the failure to implement adequate security measures constitutes an unfair or deceptive act or practice under the Federal Trade Commission Act.

With these and other enforcement actions, the FTC has clarified that companies holding vast amounts of personal data should be incorporating data security measures as part of their regular corporate management. In addition, companies should be creating breach response policies before breaches occur.[8]

More recently, the Federal Communications Commission joined the enforcement barrage by addressing data security measures as part of its regulation of telecommunications carriers. The FCC recently fined carriers TerraCom Inc. and YourTel America Inc. a total of $10 million for failing to adequately protect the privacy of phone customers' personal information.[9] TerraCom and YourTel allegedly stored Social Security numbers, names, addresses, driver's licenses and other personal identification information belonging to their customers on unprotected Internet servers that could be accessed through a simple Google search.[10]

Following the FTC's lead, the FCC found that a telecommunications carrier's failure to maintain appropriate security measures in violation of the FTC Act constitutes an unjust and unreasonable practice under Section 201(b) of the Communications Act.[11]

This forfeiture decision marks the beginning of the FCC's rigid enforcement of data security requirements in the communications industry. The agency has commented that it "is committed to aggressive enforcement of unlawful practices related to cyber security and data protection."[12]

Even the U.S. Department of Health and Human Services has become an active voice with respect to data security breaches. Relying on its enforcement authority under the Health Insurance Portability and Accountability Act, HHS recently reached a $4.8 million settlement with Columbia

University and New York Presbyterian Hospital after patient information became available via Google searches.[13] HHS said the hospitals failed to conduct an adequate risk analysis of their patient data security practices prior to the breach and failed to comply with their own policies on patient data access management.

CORPORATE GOVERNANCE OF CYBERRISK

The common theme of these shareholder grievances and regulatory enforcement actions is an alleged failure to meet the standard of care in preventing and mitigating cyberrisks. Recent regulatory initiatives confirm that comprehensive data security policies are increasingly becoming a standard part of corporate governance.

The Securities and Exchange Commission, for example, requires corporations registered with the agency to disclose to investors information that a reasonable investor would consider important to an investment decision.[14]

The SEC takes the position that cyberrisks may constitute "material information" that must be disclosed to investors. Required disclosures may include a "[d]escription of cyberincidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences."

Similarly, the National Institute of Standards and Technology has echoed the importance of transparency of cybersecurity practices as a critical component of corporate governance. On Feb. 12, 2014, NIST released its Framework for Improving Critical Infrastructure Cybersecurity.[15] The framework recommends the creation of a "current profile" that organizations can use to describe their existing cybersecurity state, including current practices that pose risks.[16] The profile may be used to communicate cyberrisks among all stakeholders who help to deliver essential services supporting the enterprise.[17]

Although the NIST framework is not binding law and is targeted at critical infrastructure systems, many consider it to be the best existing model of a "standard of care" for data security, as well as a benchmark for future legislation.

On Nov. 17, NIST released its "Guide to Cyber Threat Information Sharing," in which it proposes the creation of networks that would allow organizations holding large amounts of personal data to share information about cyberattacks and breaches.[18] The intent is to gather and analyze information from internal and external sources in order to better detect data security threats before breaches occur. This initiative demonstrates the ongoing efforts to develop a more concrete "standard of care" for data security that companies will be expected to follow.

What does all this mean for companies that hold sensitive personal data? Addressing cyberrisk is a critical component of corporate governance, as the risk can lead to liability for corporate boards. The costs to companies in the wake of a breach will only increase, because affected companies will need to deal with remediation costs, increased cybersecurity protection costs, lost revenue, litigation costs and reputational damage.

Moreover, as regulatory corporate standards become more solidified, companies can add derivative action and enforcement defense costs to the mix.

In addition to considering newly available cyberinsurance products, affected companies should look to D&O insurance coverage to help mitigate and offset some of the costs of defending shareholder lawsuits and government enforcement actions.

CYBERRISK COVERAGE AND THE STANDARD OF CARE

Because most D&O insurance policies covering "wrongful acts" define the term broadly, alleged "acts, errors or omissions" by corporate boards will likely encompass cyber-related claims absent an express exclusion. Although data breach exclusions are becoming more common in traditional general liability policies, D&O policies typically do not contain such exclusionary language and should provide some relief for losses arising from cyberliability risks.

Home Depot announced that, as of November, it was facing at least 44 breach-related lawsuits, as well as investigations by several state attorneys general.

D&O policies generally provide coverage for any neglect or breach of duty by directors and officers acting in their capacities as fiduciaries to the corporation. Directors and officers generally owe three duties to a corporation: a duty of care, a duty of loyalty and a duty of obedience. The requisite duty of care is the amount of care that ordinarily careful and prudent people would exercise in similar circumstances, considering all material information reasonably available.[19]

Courts may refer to industry practices and standards to determine whether a duty of care has been breached.[20] A duty of care can be breached by a director's act or failure to act, or as a result of a board's unconsidered failure a to act when due attention arguably would have prevented the loss.[21]

CONCLUSION

Cyberrisk is not an abstract concern — it is real and should be on the minds of directors and officers. The Target data breach exemplifies how the duty of care comes into play in the online context. It also confirms the importance of maintaining company-wide policies on cyberrisks as part of a wider corporate governance strategy. In the Target case, the delay in notifying consumers served as an impetus for many class action claims.

In addition, the failure to disclose security risks fueled ire among shareholders. Shareholders lamented that Target "significantly downplayed its true significance" and "withheld the truth about the breach, put millions more customers at risk and had the effect of significantly increasing the damage to Target's goodwill and brand trust."[22] D&O policies should respond to cyber-related claims based on these allegations of securities fraud, breach of fiduciary duty and alternative theories of liability.

Coverage for regulatory enforcement actions poses potential additional challenges.

Coverage for regulatory enforcement actions poses potential additional challenges. Because most D&O policies exclude fines and penalties, carriers typically argue that governmental actions, which seek to impose fines, are not covered. Nonetheless, where regulators allege that a data breach occurred because cybersecurity measures taken by corporate leadership fell below the applicable standard of care, some D&O and professional liability policies providing broad coverage for "wrongful acts" may be triggered.

Indeed, in the Bayview and Cornerstone enforcement actions, the FTC pointed to specific acts taken by high-level officers that undermined the security of customer data. Carriers and policyholders litigated the issue of coverage for regulatory enforcement actions well before the recent wave of cyber-related investigations, and there is nothing unique about the cyberrisk arena that would suggest that these new enforcement actions are more or less likely to be covered under typical D&O policies.

Insurance policies can mitigate the growing consequences of cyberrisk. Specialized "cyberinsurance" policies are still evolving. Though these policies may eventually help shape cybergovernance standards, their development has been slowed by the general lack of understanding of cyberthreats. In this dynamic market, it is vital for companies to involve insurance coverage counsel and experienced insurance brokers in the insurance-buying process.

Counsel can assist policyholders in matching their unique cyberrisk profile to coverage offered by various cyberinsurance products. They may also assist in evaluating whether existing coverage, including D&O policies, may be sufficient to guard against such risks. In addition to helping policyholders avoid any gaps in coverage and exposure risks, these professionals can help companies avoid coverage overlaps.

NOTES

[1] *In re Target Corp. Customer Data Security Breach Litig.*, No. 14-md-02522, 2014 WL 6775314 (D. Minn. Dec. 2, 2014).

[2] *Kirk v. Target Corp.*, No. 13-cv-5885, *complaint filed* (N.D. Cal. Dec. 19, 2013), at ¶¶ 50, 51.

[3] *Collier v. Steinhafel (Target Corp.)*, No. 14-cv-00266, *complaint filed* (D. Minn. Jan. 29, 2014).

[4] *In re Heartland Sec. Litig.*, No. 09-cv-01043-AET-TJB, *complaint filed* (D.N.J. Dec. 7, 2009), at 3.

[5] *Palkon v. Holmes,* No. 14-cv-01234, 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

[6] Form 10-Q, Home Depot Inc., Securities and Exchange Commission (quarter ending Nov. 2, 2014).

[7] *See Fed. Trade Comm'n v. Cornerstone & Co. LLC et al.,* No. 1:14-cv-01479, *preliminary injunction order issued* (D.D.C. Sept. 10, 2014); *Fed. Trade Comm'n v. Bayview Solutions LLC et al.,* No. 1:14-cv-01830, *stipulation to entry of preliminary injunction filed* (D.D.C. Nov. 3, 2014).

[8] Lesley Fair, *Buying or selling debts? 7 steps for keeping data secure,* Fed. Trade Comm'n Business Ctr. Blog (Dec. 3, 2014, 12:41 PM, http://www.business.ftc.gov/blog/2014/11/buying-or-selling-debts-7-steps-keeping-data-secure.

[9] *In re TerraCom Inc. et al.,* FCC 14-173, File No. EB-TCD-13-00009175, *notice of apparent liability for forfeiture issued* (F.C.C. Oct. 24, 2014).

[10] *Id.* at ¶ 1.

[11] *Id.* at ¶ 38 n.83.

[12] *Id.* at ¶ 35 n.74.

[13] Press Release, U.S. Dep't of Health and Human Servs., Data breach results in $4.8 million HIPAA settlements (May 7, 2014).

[14] *See* Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9; *Basic Inc. v. Levinson,* 485 U.S. 224 (1988); *TSC Indus. v. Northway, Inc.,* 426 U.S. 438 (1976).

[15] Nat'l Inst. of Standards & Tech., Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[16] *Id.* at 13.

[17] *Id.* at 15.

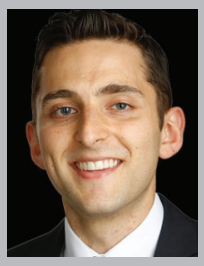
[18] Chris Johnson, Lee Badger & David Waltermire, Guide to Cyber Threat Information Sharing (Draft), Nat'l Inst. of Standards & Tech. Special Publication 800-150 (October 2014).

[19] *Rafool v. Goldfarb Corp. (In re Fleming Packaging Corp.),* 370 B.R. 774 (Bankr. C.D. Ill. 2007); *In re Caremark Int'l Derivative Litig.,* 698 A.2d 959, 967-68 (Del. Ch. 1996).

[20] *See Francis v. United Jersey Bank,* 432 A.2d 814 (N.J. 1981).

[21] *Caremark*, 698 A.2d at 967.

[22] *Collier* complaint at ¶ 5.



William T. Um (L) is an attorney in the Los Angeles office of **Hunton & Williams**, where he has more than 20 years of experience representing policyholders in complex insurance coverage disputes. He can be reached at 213-532-2175 or WUm@Hunton.com. **Paul T. Moura** (R) is an associate at the firm. His practice area includes representation of policyholders in insurance coverage disputes. He can be reached at 213-532-2177 or PMoura@Hunton.com.