Fiduciary Duties of Directors Are Key to Minimizing Cyber Risk

By Michelle A. Reed, Natasha G. Kohne, and Jenny M. Walters

As news of data breaches fills the headlines, directors report that cyber risk is one of their greatest concerns. Yet in a recent survey, nearly 80 percent of the more than 1,000 information technology leaders surveyed had not briefed their board of directors on cybersecurity in the last 12 months, according to Ponemon Institute's *2015 Global Megatrends in Cybersecurity*.

Cybersecurity is viewed as a critical issue by regulators, but many companies have not stepped up enterprise-level risk management to address vulnerabilities. Securities and Exchange Commission (SEC) Commissioner Luis Aguilar cautioned, "[B]oards that choose to ignore or minimize the importance of cybersecurity oversight responsibility, do so at their own peril." The failure to maintain adequate risk oversight is a cybersecurity debt that will likely expose companies, officers, and directors to liability in the future.

> Directors who ignore their risk-management responsibilities for cybersecurity will thus have no protection under the business judgment rule.

Class Action Lawsuits

Class actions now go hand-in-hand with major data breaches, with lawsuits often filed within days after a breach is announced. Currently, there is no comprehensive federal privacy and data security law framework; thus, plaintiffs are left with a hodgepodge of federal and state laws to rely on in bringing claims associated with a data breach.

At the federal level, class action plaintiffs have been creative in bringing claims to extend to other statutes to cover data breaches, most commonly under the Stored Communications Act and the Wiretap Act. Other federal statutes, such as the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), are frequently cited, as well. In addition, almost all states have general data breach and security statutes, although many do not contain a private right of action, or the private right is limited to notice provisions and does not extend to the actual loss from the breach.

At the state level, class action plaintiffs generally bring claims for negligence, breach of express or implied contract, unjust enrichment, mitigation costs, and lost time and inconvenience, with varying levels of success. The recent Sony breach highlights that risk is no longer limited to the payment card industry or similar third-party cases—the loss of employee data will often result in employee class actions as well.

Derivative Suits

Lawsuits stemming from data breaches are not limited to the company itself. Directors and officers also face derivative liability in connection with data breaches. Directors owe fiduciary duties to their shareholders and have a significant role in overseeing the risk management of the company. (Though fiduciary duties have some variance by state, under Delaware law, directors owe fiduciary duties of care, loyalty, and good faith to the company. The duty of good faith is not an independent duty, but is subsumed within the duty of loyalty. The duty of oversight derives from the duty of good faith.)

The SEC, in its Dec.16, 2009, Proxy Disclosure Enhancements release, noted that "risk oversight is a key competence of the board," and that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company." In the context of cybersecurity, companies must also assess whether and how to disclose a cyberattack internally and externally to customers and investors.

These cases demonstrate the importance of director and officer oversight in ensuring companies have an adequate and tested cybersecurity program in place and are prepared to properly and quickly respond to a data breach, including under certain circumstances retaining counsel and third-party experts to appropriately advise on post-breach security measures. For example, plaintiffs last year filed four separate shareholder derivative lawsuits in the District of Minnesota against 13 directors and officers of Target

following its now-infamous data breach. The Target plaintiffs assert claims for breach of fiduciary duty and waste of corporate assets, among others. The suits challenge the directors' pre- and post-breach conduct, alleging that the directors failed to manage risk pre-breach (allowing the breach to occur) and post-breach (failing to properly disclose, investigate, and remediate the breach). Although the broader consumer class action has since settled, the derivative suits have been consolidated and remain pending.

Similarly, last year a derivative lawsuit naming 10 directors and officers of Wyndham Hotels was filed in the District of New Jersey. The Wyndham lawsuit asserted claims for breach of fiduciary duty, waste of corporate assets, and unjust enrichment. Similar to Target, the Wyndham plaintiffs alleged that directors failed to prevent and properly disclose, investigate, and remediate the breach. The Wyndham plaintiffs asserted that the company suffered three data breaches between April 2008 and January 2010, resulting in the compromise of personal information belonging to 600,000 customers. The plaintiffs also asserted that the directors did nothing to oversee lax information security at the company, including practices such as using unsupported software that was three years out-of-date and storing unencrypted payment card data on its servers.

The Federal Trade Commission (FTC) filed an enforcement action in connection with the breach in June 2012. Then, in June 2013, the shareholder plaintiff wrote a letter to Wyndham's board of directors, demanding that the board investigate the data breaches and sue the named directors and officers for the harm suffered by Wyndham as a result of the data breaches.

Wyndham's audit committee and board refused the demand, and the plaintiff filed a derivative lawsuit. In October 2014, the New Jersey federal district court promptly dismissed the lawsuit. The defendants had moved to dismiss the lawsuit arguing that the plaintiff lacked standing to bring the derivative lawsuit because his demand was considered and refused by Wyndham's board. The court found that the board's decision not to pursue an action was entitled to deference under the business judgment rule and that the decision was not made in bad faith or based on an unreasonable investigation.

The court held that the directors were not grossly negligent in conducting the investigation, noting key metrics for directors: Wyndham's board had discussed the cyberattacks at 14 meetings during the relevant time frame and the company's general counsel gave a presentation regarding the data breaches or data security at each meeting. The court also noted that the board's audit committee discussed these issues during at least 16 meetings over the same time period. Noting that the company had retained third-party technology firms to investigate each breach and recommend enhancements to Wyndham's systems, the court reasoned that the board had conducted a reasonable investigation. The court commented that the board's quick response to the demand was not unreasonable, given that the FTC investigation filed a year earlier had enhanced the board's understanding of the issues raised in the demand.

Directors will likely continue to see shareholder derivative suits brought following major data breaches. In assessing whether directors have met their duty of due care, the court will "look for evidence of whether a board has acted in a deliberate and knowledgeable way, identifying and exploring alternatives."

Importantly, the business judgment rule only operates in the context of director action: "Technically speaking, it has no role where directors have either abdicated their functions, or absent a conscious decision, failed to act," according to a 1984 Delaware decision in *Aronson v. Lewis*.

Directors who ignore their risk-management responsibilities for cybersecurity will thus have no protection under the business judgment rule.

Cybersecurity Risk Management

The best way to protect yourself and the company is by elevating cybersecurity to an enterprise-level risk management issue and ensuring proper follow-up. Before a breach occurs, directors should seek advice from knowledgeable counsel and information security consultants to review red flags and adequacy of insurance, conduct stress-testing, implement an effective record-retention policy, and craft and test a practical incident response plan. After a data breach, companies must be prepared to respond to the regulatory investigations, class actions, and derivative suits that are sure to follow.

The cybersecurity debt continues to accrue, with vulnerabilities and risk management lagging at most companies. But with proper due diligence and risk management, directors can begin to chip away at this enormous potential liability, transforming a company's greatest risk into one of its greatest strengths.

Michelle A. Reed is a partner at Akin Gump Strauss Hauer & Feld, focusing on complex civil litigation matters. Natasha G. Kohne is also a partner, focusing on U.S. and international or cross-border litigation, arbitration, and investigations. Together, they lead the firm's cybersecurity, privacy, and data protection practice. Jenny M. Walters is counsel at Akin Gump, where she focuses on representing clients in securities and privacy litigation, internal and regulatory investigations, and enforcement proceedings, as well as advising private equity and hedge funds on regulatory compliance and fund litigation strategies.