The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 3 February 14, 2018

BOARDS OF DIRECTORS

Dynamic Regulations and Shareholder Actions Guide the Board's Shifting Role in Cyber (Part Two of Two)

By Jeewon Kim Serrato, Marc Elzweig, David Lee
Shearman & Sterling

As large-scale data breaches become regular occurrences, shareholder derivative suits, based on theories such as breach of fiduciary duties, mismanagement and material omissions, are increasingly used by investors seeking to be made whole after data breaches. Boards of directors need to take note and understand the increasing costs and risks of these suits. This article, the second in our series, provides five lessons boards can learn from recent cases.

One element behind the rise in shareholder suits is the increasing frequency of breaches. Headlines about data breach incidents have become almost routine. On September 21, 2017, a morning news item was titled: "The SEC has also been hacked." The news about the SEC data breach came on the heels of the consumer data exposure disclosed by Equifax on September 7, 2017, which affected 145.5 million consumers – a number equivalent to nearly half of the U.S. population.

A 2016 Forrester study commissioned by Hiscox Insurance Company found that 72 percent of larger U.S. companies experienced a cyber incident and 47 percent of all U.S. firms experienced two or more. According to the Identity Theft Resource Center (ITRC)'s most recent collection of confirmed data breach incidents by U.S. organizations, a total of 1,339 breaches affected approximately 174 million personal records as of December 2017, easily exceeding 2016's numbers. Cybersecurity risks are now a pressing reality for both large and small corporations.

The expenses of a breach are also climbing, adding to the impact. A 2017 Ponemon Institute study found that the worldwide average cost of a data breach is between $3.62 million and $4 million, though the average cost in the U.S. is nearly double that. And costs of significant data breaches can be much higher. Target, for example, indicated in its 2017 annual report that it has incurred net expenses of $202 million since a 2013 data breach.

See "Takeaways From State AGs' Record-Breaking Target Data Breach Settlement" (May 31, 2017).

Five Lessons From Shareholder Derivative Suits

Drawing from recent cases we examined in part one of this series – TJX, Wyndham, Target and Home Depot – we identified five trends and lessons. Although this article focuses on the impact of shareholder derivative suits, the lessons would be applicable to companies seeking to assess litigation risks related to data breach, and they also provide a practical starting point for managing cybersecurity risks in general.

See "Key Post-Breach Shareholder Litigation, Disclosure and Insurance Selection Considerations" (Aug. 3, 2016).

1) Have a Plan to Address Identified Security Vulnerabilities

When the board or a committee in charge of overseeing data security is informed of internal weaknesses or threats, it must take responsive action. It is not necessary for the response to be perfect, but it should be reasonable and appropriate.

In the Home Depot case, the company learned of various data security weaknesses well in advance of the data breach. In response, the board approved a plan to fix the weaknesses, but the plan would not be fully implemented until February 2015. (The breach occurred in April 2014.) The plaintiff in the case argued that the directors breached the duty of loyalty by failing to adequately respond to the known security weaknesses and that the company failed to immediately remedy the data security deficiency and correct its failure to comply with the PCI DSS.

Even the court admitted that one can "safely say that the implementation of [Home Depot's] plan was probably too slow" and that the plan likely would not have fixed all weaknesses, but the court emphasized that the directors had "a plan" in motion. And because the plan was approved prior to the breach and would have fixed many of the security weaknesses, the court found that the directors' actions were sufficiently reasonable under the business judgement rule and demand futility standards. In contrast, other courts have found the demand to be futile when directors received numerous

warnings about illegal practices by the company and chose to disregard them or when the directors failed to take any action for more than a year to address accounting deficiencies.[1]

When the board learns of data security weaknesses, it is important that the board act quickly and respond with a plan. Even if the response is not the perfect solution to the problem, it will help protect not only the consumers but also the directors. The board should engage experts and counsels to prepare a response quickly upon identifying such issues.

See "A CSO/GC Advises on How and When to Present Cybersecurity to the Board" (Feb. 22, 2017).

2) Meet Applicable Industry Standards

Retail companies are often obligated to comply with PCI DSS under agreements with payment card companies, such as Visa and MasterCard. PCI DSS is a set of cybersecurity standards that sets forth "a baseline of technical and operational requirements designed to protect account data." At a high level, PCI DSS requires that companies install and maintain certain firewall configurations, encrypt transmission of cardholder data and regularly monitor and test networks for weaknesses.

In shareholder derivative suits against retail companies, plaintiffs use non-compliance with PCI DSS to demonstrate breach of duties, including in claims brought against TJX, Target, Home Depot and Wendy's. In the Wendy's case, plaintiffs argued that directors breached their fiduciary duties by failing to comply with PCI DSS, in permitting franchise stores to use a point-of-sale system that had known security weaknesses, failing to install and maintain adequate firewalls, failing to segment payment card data from the company network and failing to encrypt payment card data.

Other industries are also subject to data security standards, such as the Health Insurance Portability and Accountability Act (HIPAA) for the health industry and the NYDFS Cybersecurity Requirements for Financial Services Companies. Boards should seek expertise in applicable industry standards and ensure the company's compliance with such standards.

See "Preparing to Meet the Deadlines of DFS' Revised New York Cybersecurity Regulation" (Jan. 25, 2017).

3) Ensure the Board or a Committee Has Authority and Responsibility for Cybersecurity

In 2007, Home Depot established an infrastructure committee and determined that it would oversee IT and information security. After dissolving the infrastructure committee in 2012, the company did not reassign data security responsibilities. In the subsequent case against Home Depot, plaintiffs argued that directors breached duties by failing to explicitly delegate the data security protection tasks to a committee or the board. The court rejected the argument on the grounds that the audit committee was in fact receiving reports on data security issues, and the committee and the board believed that the audit committee held responsibility for data security issues. The court clarified that the relevant demand futility analysis is fact-based and, rather than confining its inquiry to documented responsibilities, the court focused on the company's understanding that the audit committee was actually responsible for data security oversight.

While this analysis helped Home Depot, it should also be understood that it is not sufficient to merely document responsibility for data security matters if the board or committee charged with that responsibility does not actively pursue such responsibilities. In addition to ensuring that a company's charters and protocols provide authority oversight over data security matters, it is also important for a board or committee to oversee data security issues in practice.

4) Train and Educate Directors and Employees

It is important that the employees as well as board members are trained in data security matters. The board members, especially members with specific responsibilities to oversee data security, should have sufficient expertise to evaluate data security reports and understand material risks. Such training may also help the company avoid shareholder derivative suits by avoiding or reducing data breach incidents through better management of security measures. Alternately, if a breach occurs, the company has likely strengthened its arguments that its directors acted pursuant to their fiduciary duties of care, loyalty and good faith.

Employees should also receive training regarding the importance of reporting data security issues noticed on the job and processes for addressing such issues. In the Wendy's case, plaintiffs noted that a senior engineer at Wendy's headquarters raised concerns about known data security vulnerabilities due to the company's use of outdated Windows XP systems, but

nothing was done to rectify the problem. If there had been proper training and protocols in place, the issues raised by the senior engineer may have been escalated properly and resolved, which could have avoided the breach itself or at least removed those grounds for plaintiffs' derivative suit.

See "SEC Report Cites Cybersecurity Progress Along With Gaps in Training and Compliance" (Aug. 23, 2017).

5) Have a PR Strategy

When there is a major data breach incident, the media and regulators typically emphasize the faults and missteps of the company's media response, most frequently focusing on whether the company was too slow in disclosing the breach to the public. Once a breach occurs, it can be difficult to control how the breach is made public. There are numerous cybersecurity experts and researchers who may identify and announce data breaches, such as Brian Krebs, who made the first public announcement of the Home Depot breach. Similarly, Target's data breach was first made public by third-party reports, and the company's official disclosure came afterwards. In the suit against Target, plaintiff highlighted this fact in its complaint and argued that the directors aggravated the damage to the company by failing to provide adequate and prompt notice to consumers.

How the data breach gets reported by third parties is not within the company's control. What the company, and its board of directors, can do is to control its PR strategy once it has been detected and carefully plan and roll out disclosures to consumers, customers and employees. Given the reputational risk and potential impact on how the breach response will be evaluated by regulators and the courts in the aftermath, a data breach response team should include PR firms and outside counsel specialized in crisis management and data breaches to assist in the strategy and rollout of any public statements or disclosures.

See "Cyber Crisis Communication Plans: What Works and What to Avoid (Part One of Two)" (Jun. 14, 2017); Part Two (Jun. 28, 2017).

Jeewon Kim Serrato is counsel and head of the privacy and data protection practice group at Shearman & Sterling LLP. She advises companies on privacy, cybersecurity, data protection and crisis management issues. She has extensive experience in developing and structuring comprehensive data and trade secrets protection programs, implementing and testing information security controls, and helping companies mitigate cyber risks and handle data breaches. Previously, she served as chief privacy officer of Fannie Mae. She currently serves on the Department of Homeland Security Data Privacy and Integrity Advisory Committee and is a Certified Information Privacy Professional (CIPP).

Marc Elzweig and David Lee are associates in the privacy and data protection practice group at Shearman & Sterling LLP.

[1] For instances where the court has found the demand to be futile, see In re Pfizer Inc. S'holder Deriv. Litig., 722 F. Supp. 2d 453, 460 (S.D.N.Y. 2010) and Veeco Instruments, Inc. v. Braun, 434 F. Supp. 2d 267 (S.D.N.Y. 2006).