LAW.COM
An ALM Website
July 9, 2015

Director Liability for Data Breaches: How Real is the Risk?

By Timothy A. Miller, Marc S. Gerber and Richard S. Horvath, Jr.

Timothy A. Miller

Marc S. Gerber

Richard S. Horvath, Jr.

Most public company directors are by now well aware that cybersecurity is a critical part of the business landscape. In the wake of attacks against virtually every type of government and business entity, from the White House to health insurers, the question that remains is whether public company directors will, in fact, face real legal exposure resulting from a malicious and criminal cyberattack?The answer under Delaware law, at least according to the plaintiffs' bar, depends on whether directors failed to satisfy the duty of oversight. Consistent with a board's oversight duties, directors should give regular attention to whether the corporation has instituted adequate controls and procedures tomitigate the risk and harm of a data security breach. The failure to undertake such efforts could, in theory, expose directors to liability for the corporation's costs arising from a data security breach, including the costs from investigating a possible cyberattack, potential legal penalties, and the reputational harm suffered by the corporation. This article will discuss the potential legal basis for such liability and suggest some practical steps a board of directors can take in the discharge of its oversight duties in the cybersecurity arena.

Directors bear the ultimate responsibility for managing and overseeing the business and affairs of a corporation. Day-to-day responsibility is typically delegated to officers and employees, requiring director oversight for strategic direction and risk management, and approval of significant transactions. In the seminal case *In re Caremark Int'l, Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996), then-Chancellor William T. Allen held that, in discharging their duty of oversight, directors must assure themselves that a corporation's reporting systems will enable the board to reach informed business judgments "concerning both the corporation's compliance with law and its business performance." See *Caremark*, 698 A.2d at 970.

Since Chancellor Allen's decision in Caremark, Delaware courts have made clear that directors' oversight duties are grounded in concepts of good faith and loyalty. The typical provision in a company's certificate of incorporation under 8 Del. C. § 102 (b)(7) exculpating directors from monetary damages resulting from conduct amounting to a breach of the duty of care will preclude any attempt to base liability on an alleged failure to exercise due care in overseeing the company's cybersecurity controls and procedures.

Under the duty of good faith, which Delaware courts have made clear is rooted in the duty of loyalty, only an extreme set of facts beyond gross negligence can expose directors to oversight liability. To establish a failure of oversight, a shareholder must plead and prove that: "(a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention." *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

It seems unlikely, in light of the high profile cyber attacks of the past few years, that directors of a public corporation could be found liable for utterly failing to implement any reporting or information system or controls for data security. In recent years, corporations have expanded their efforts to promote data security by increasing resources dedicated to such security and clarified responsibility for those efforts. Even relatively modest efforts to enhance management's data security, with board involvement or awareness, are likely to preclude a claim premised on the first Stone factor requiring an "utter failure" to implement controls.

A different issue is posed by the second *Stone* factor for an oversight claim: whether "having implemented such a system or controls, [directors] consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention." Stone, 911 A.2d at 376. In attempting to show this conscious failure to monitor operations, shareholder plaintiffs' lawyers frequently allege that directors knowingly ignored "red

flags" alerting them to misconduct or defects with the corporation's controls. Such claims are rarely successful, reflecting the adage that an oversight claim is "possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment." *Caremark*, 698 A.2d at 967.

But ignoring "red flags" is not the only route to a possible oversight violation. Indeed, the second factor of Stone says nothing about "red flags." *Stone*, 911 A.2d at 364. Rather, the Delaware Supreme Court framed the test in Stone as creating oversight liability when, having implemented a system of internal controls, directors consciously failed to monitor or oversee its operation. Accordingly, a crucial factor explored by courts in dismissing purported oversight claims is the efforts undertaken by directors to monitor a corporation's internal systems or controls. Such efforts can defeat a claim for oversight liability even if those efforts ultimately failed to prevent a corporate trauma. Nevertheless, continuously monitoring a corporation's data security efforts presents unique challenges because cyber issues continue to evolve and a corporation may never be "done" securing its data.

Courts have yet to address the merits of an oversight claim arising from a data security breach. For example, in response to oversight claims arising from the data security breach during the 2013 holiday shopping season, the Target board of directors appointed a special litigation committee to investigate, in part, the derivative allegations and whether Target should pursue the claims. That investigation is pending.

In another shareholder action arising from data security breaches at Wyndham Worldwide Corporation occurring between April 2008 and January 2010, the court noted that the Wyndham board and its audit committee understood the facts surrounding the data security breaches due to repeated presentations and discussions from 2008 through 2012. Relying in part on the directors' understanding of the facts underlying the plaintiff's pre-suit litigation demand, the court rejected the plaintiff's arguments that the board's investigation into the demand was unreasonable or that the board wrongfully rejected the demand. Because of the procedural posture in each of these cases, however, the courts in both the Target and Wyndham litigation have not ruled on the merits of the oversight claims.

In overseeing data security efforts, directors should consider those efforts as falling into two broad categories: (1) risk mitigation designed to prevent or minimize the impact of a cyber attack; and (2) crisis management once an attack occurs. Board oversight of both aspects is recommended. Although courts have yet to establish guiding principles in the application of oversight duties to data security, we suggest that directors and corporate counsel consider the following factors and practical steps in discharging the board's oversight duties:

- Whether the entire board of directors or a committee should oversee the corporation's data security controls;
- Whether the board should have a member with data security experience;
- Which officers should have responsibility for the corporation's day-to-day data security efforts, including if the primary focus of that officer's responsibilities should be on such efforts;
- Whether internal or external experts are needed to promote the corporation's data security efforts;
- Whether the corporation's data security efforts comply with industry standards or best practices, and, if not, where and why the corporation's efforts deviate;
- The need for insurance to cover the costs associated with a data security breach;
- Receiving regular reports regarding both the corporation's ongoing compliance with data security laws and the corporation's efforts to maintain the security of its own data; and
- Implementing a cyberattack response plan as a contingency for a data security breach, including conducting "war games" to test and refine the plan.

Not all of these measures are appropriate for every organization, and it is important to recognize that the appropriate oversight system for data security is a question of business judgment. *Caremark*, 698 A.2d at 970.

Moreover, the board of directors and corporate counsel should keep in mind two critical principles:

- If any red flags or security breaches are reported to the board or its designated committee, those directors should also understand the corporation's response efforts and consider whether additional action is needed; and,
- Board or committee minutes should carefully document the board's or committee's exercise of its business judgment, including the attention given to reports about data security and the consideration of actions taken or not taken in response to potential red flags or security breaches.

While internal controls and the monitoring of data security will not prevent all attempts to breach a corporation's cyber-defenses, the oversight by directors before such a breach occurs will be a powerful tool in shielding them from oversight liability arising from such a breach.

Richard S. Horvath, Jr. *is a litigation associate in the Palo Alto office of Skadden, Arps. He focuses his practice on complex shareholder litigation, including corporate governance disputes, shareholder derivative litigation, M&A litigation and securities class action defense.* **Marc S. Gerber** *is corporate partner in the Washington, D.C. office of Skadden, Arps. He concentrates his practice in the areas of mergers and acquisitions, corporate governance and general corporate and securities matters.* **Timothy A. Miller** *is a litigation partner in the Palo Alto office of Skadden, Arps. He focuses his practice on corporate and securities litigation, M&A litigation, shareholder derivative litigation, trade secret misappropriation, unfair business practices and unfair competition actions, as well as business tort litigation*