CORPORATE COUNSEL
An ALM Website
corpcounsel.com | August 6, 2014

# Director Liability for Cybersecurity Risks

## From the Experts

*David L. Barres and Dominic J. Picca*

If a corporation is the target of a cyberattack resulting in a data breach, its board may be the target of a shareholder derivative action claiming breach of fiduciary duty. A recent example is *Palkon v. Holmes*, No. 14-cv-01234 (D.N.J.), in which a shareholder of Wyndham Worldwide Corporation sued its directors and senior officers, claiming that their failure to implement adequate information-security policies allowed three data breaches, resulting in theft of over 600,000 customers' personal and financial data. Shareholder derivative actions like *Palkon* allow plaintiffs to avoid one of the major obstacles to a data-breach class action against the corporation: proving that the purported class members suffered common damages resulting from theft of their personal information. In a derivative action against the board, damages are suffered proportionally by all shareholders based on the harm to the corporation through, for example, decreased stock prices. Because damages from privacy breaches often are not covered by directors and officers (D&O) insurance, directors may face significant personal exposure.

This article addresses the potential liability of directors arising from a data breach, and how they can help protect themselves and their company from liability. We focus on Delaware law because, practically speaking, it states the national standard for director fiduciary duty.

### Legal Standards

Under Delaware law, directors owe fiduciary duties of care, loyalty and good faith to their corporation. The first two duties result directly in liability, if violated. The third duty—good faith—is not an independent fiduciary duty but rather an element of the duty of loyalty, as a director cannot act loyally toward the corporation unless she acts in the good faith belief that her actions are in its best interests. *Stone v. Ritter* (Del. 2006). Following a data breach, claims against the board probably will be for (a) breach of the duty of care, and (b) breach of the duty of oversight (which derives from the duty of good faith contained within the duty of loyalty).

Liability under the duty of care is governed by the business judgment rule, which derives from the principle, codified in 8 Del. C. § 141(a), that the business and affairs of a corporation are managed by or under its board of directors. The rule presumes that, in making a business decision, the

directors "acted on an informed basis, in good faith and in the honest belief that the action was in the best interests of the company." *Smith v. Van Gorkom* (Del. 1985). Under the business judgment rule, director liability is based on gross negligence.

In evaluating due care, the court will "look for evidence of whether a board has acted in a deliberate and knowledgeable way identifying and exploring alternatives." *Citron v. Fairchild Camera and Instrument Corp.* (Del. 1989). Although directors may rely on reports prepared by others, they cannot rely solely on hired experts and management without taking an active and direct role. Therefore, the board that fails to manage and monitor cybersecurity probably does not satisfy its duty of care.

Also, the business judgment rule operates only 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." *Aronson v. Lewis* (Del. 1984). Thus, a board that ignores cybersecurity breaches its duty of care.

Such a board probably also breaches its duty of oversight. The requirements for such liability are "(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*. In either case, the directors must have known that they were not discharging their fiduciary obligations.

While it is not easy to prove a breach of either the duty of care or oversight, plaintiffs are starting to succeed, at least in early stages of litigation, under these legal standards.

**Recent Cases**

Two New York cases recently found potential liability for data breaches under the gross-negligence and oversight-liability standards. In *Baidu v. Register.com* (S.D.N.Y. 2010), the Chinese-based search engine provider Baidu Inc. alleged that the service representative of Register Inc. (a domain-name registrar) allowed an intruder to change Baidu's email address on file after failing to compare the intruder's inaccurate security code to the real code. The intruder accessed Baidu's account, routed Internet traffic to a rogue site and caused a two-day business disruption that allegedly cost Baidu millions of dollars. Judge Denny Chin held that Register's alleged failure to follow its security protocols was sufficient to plead grossly negligent or reckless conduct. This liability standard, contained within the parties' services agreement, is substantially the same as the gross-negligence standard governing board liability.

Register was potentially liable because, while it had adequate cybersecurity protocols, it failed to follow them. The result, presumably, would have been the same if Register had never established adequate protocols.

In *Transeo S.A.R.L. v. Bessemer Venture Partners IV* (S.D.N.Y. 2013), a shareholder filed a derivative claim against the President/CEO/Director of a software company who allegedly relocated his company's web services, associated IP and cash from France to the United States. This allegedly disrupted the company's services, compromised client security, facilitated hacking of its website and violated European data-privacy laws. Judge Cathy Seibel held that a claim for breach of the duty of loyalty, based on failure to act in good faith, was adequately pled under Delaware law.

Although *Transeo* did not identify the data-privacy laws allegedly violated, it provides a useful warning in this developing area of litigation. If a director intentionally violates the law or causes the company to do so, she breaches her fiduciary duty of good faith. By now, the federal government and most states have enacted laws protecting data privacy. After a data breach, plaintiffs may allege the directors caused a violation of some jurisdiction's data-privacy law, thus heightening the risk of director liability.

**Recommendations to Protect Against Liability**

If a data breach occurs, plaintiffs' lawyers will evaluate the board's decisions and actions concerning cybersecurity. They also will evaluate whether the board appointed and supervised well-qualified officers and committees to safeguard information.

To minimize the risk of liability, the board must become well-informed of the company's cybersecurity practices and its protocols for dealing with a data breach. An informal, working understanding, based on occasional communication with management, is not sufficient.

There are several ways the board can become adequately informed. It should appoint officers with expertise in cybersecurity, including a chief information officer (CIO), chief information security officer (CISO) and/or chief privacy officer (CPO), and regularly meet with them to ensure their vigilance and to understand their expectations and plans. These officers should head a department whose sole or primary responsibility is information security, and which includes employees whose sole responsibility is cybersecurity.

The board also should appoint a committee responsible for privacy and security. Its members can include the above officers, plus senior management from various departments. The committee should meet regularly and afterward report directly to the board.

The board should recruit and hire at least one tech-savvy member who can be responsible for monitoring and reporting on cybersecurity. This way, the board will not be entirely dependent on nonmembers for relevant information. The "cybersecurity" director can sit on the privacy/security committee described above.

To follow best industry practices, the board should investigate how its competitors address cybersecurity and read the

best-known cybersecurity recommendations, such as the National Institute of Standards and Technology (NIST) framework. With the aid of qualified management, the board should assess corporate policies against these standards.

The board also should ensure that the company has identified and classified its data. Some data—such as personal identifying information, health information and financial information—is particularly sensitive and requires greater attention to security. Depending on the nature and volume of the company's data, the board may engage an outside vendor to help manage cybersecurity. If the board does so, the contract with the vendor must address key issues, including security requirements, warranties, audit rights, backup systems, data-destruction policies and breach notification. But even if the company can protect its data without outside experts, the board periodically should engage them to audit the company's cybersecurity practices and report their findings directly to the board. The board then should review any differences between the recommendations of outside consultants and company officers.

Before any cyberattack occurs, the board should ensure that the company has written security standards and practices. The company's CIO, CISO and/or CPO can prepare them, with the aid of outside experts if necessary, and counsel should review them. Among other things, the written standards should address (a) identification and classification of the company's data; (b) where and how it is stored; (c) who has access; (d) who is permitted to transfer data and how; (e) anticipated exposure from a data breach, and available insurance coverage; and (f) breach response protocol. These security standards must be periodically reviewed and updated by the appropriate officers or committee, under the board's supervision.

The written breach-response protocols also must be periodically reviewed and updated under board supervision. Among other things, they should provide for (a) stopping the breach and securing the company's networks; (b) identifying the response team and allocating each member's responsibilities; (c) providing for internal notification and communication regarding the breach; (c) providing notice, if required, to law enforcement, regulators and potential victims; (d) contacting counsel and outside technical experts, when necessary, to manage the breach; and (e) preserving evidence. The board should require yearly rehearsal of the protocols.

**Indemnification and Insurance**

Delaware law permits a corporation's certificate of incorporation to include a provision eliminating the personal liability of a director for monetary damages for breach of the duty of care. 8 Del. C. § 102(b)(7). It also permits a corporation to indemnify a director for liability arising from a breach of the duty of care. 8 Del. C. § 145(a)-(b).

These protections, while useful, must be supplemented by insurance. The board can arrange for coverage of privacy-related risks in the company's D&O and comprehensive general liability (CGL) policies, or it can have the company purchase a separate cyber-insurance policy. CGL and cyber policies, however, cover only the company, not the board.

For their own protection, directors must review the company's policies, preferably with the aid of insurance counsel. Many D&O policies contain, in sections that an untrained eye might overlook, exclusions to liability resulting from a privacy breach. The exclusionary language often resembles the following:

> **Exclusions:**
> The **Insurer** shall not be liable to make any payment for **Loss** in connection with a **Claim** made against an **Insured**:
> (k) for emotional distress of any person, or for injury from libel, slander, defamation or disparagement, or for injury from a violation of a person's right of privacy.

The phrase "right of privacy" arguably could trigger the exclusion after a data breach. Before any cyberattack or breach occurs, the board should attempt to renegotiate the coverage or require supplemental insurance specifically for privacy-related liability. Also, the company can soften a privacy exclusion by adding qualifying language that covers, for example, oversight liability or securities claims. But even a well-negotiated policy may not offer complete protection.

Although D&O policies usually cover damages resulting from acts of gross negligence, they typically exclude intentional or willful wrongdoing. The board, therefore, should (a) follow the above recommendations to protect against cyberattacks and liability; and (b) check the company's formation documents and insurance policies to ensure maximum protection against personal exposure.

*David L. Barres and Dominic J. Picca are members in the litigation section of Mintz Levin Cohn Ferris Glovsky and Popeo in New York.*