CYBERSECURITY AND DIRECTOR AND OFFICER ACCOUNTABILITY

by Frances Floriano Goins, Ulmer & Berne LLP

In the ever-expanding world of risk management, corporate directors and officers may find themselves facing potential liability for failing to adequately oversee and supervise cyber risk. Recently, at least two shareholder derivative complaints were filed against the directors and certain executive officers of Target, based on their alleged failure to prevent and subsequently manage massive data breaches at the company resulting from the activity of hackers in the pre-holiday retail season. In the wake of what has been termed the "worst data breach" in American retail history, these complaints allege Target's directors and officers breached duties of loyalty and good faith to the company by failing to implement preventive practices and procedures. Plaintiffs also claim the defendants allowed Target to release false and misleading statements about the scope and the extent of the breaches after the fact, resulting in serious reputational, brand, and goodwill damage, depression of the company's stock price, exposure to costly customer class action litigation and regulatory investigations, and other costs incurred by Target as a result of the breaches, including notifying and dealing with customers. Based on early reports, such damages are likely to be in the hundreds of millions of dollars.

The underlying theory of director and officer liability articulated in the Target complaints dates back to the 1996 *Caremark* decision. *In re Caremark Int'l, Inc. Derivative Litig.*, 698 A2d 959 (Del. Ch. 1996). In *Caremark*, the Delaware Chancery Court noted, "it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility. . . ." However, the Chancellor was careful to note that,

"only a *sustained or systemic failure of the board to exercise oversight* – such as an utter failure to attempt to assure a reasonable information and reporting system exists – will establish the lack of good faith that is a necessary condition to liability. Such a test of liability – lack of good faith as evidenced by sustained or systemic failure of a director to exercise reasonable oversight – is quite high." *Id.* at 970-71 (emphasis added). *See also Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006) ("We hold that *Caremark* articulates the necessary conditions predicate for director oversight liability: (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. In either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations."). This "quite high" bar, however, does not make plaintiffs' lawyers shy about filing such complaints. The good news for directors and officers is that the *Caremark* standard continues to result in the early dismissal of many such cases. The minority that have survived a motion to dismiss allege specific facts indicating prior board knowledge and warnings about the precise problem and activity at issue, coupled with a failure to act. *See, e.g., La. Muni. Police Employees' Retirement Sys. v. Pyott*, 46 A. 3d 313 (Del. Ch. 2012); *rev'd on other grounds*, No. 380, 2012 (Del. April 4, 2013).

Directors are not unaware of the growing risk. In the recent NYSE Governance Services, *What Directors Think 2014 Survey* (https://www.spencerstuart.de/research-and-insight/what-directors-think-2014), twenty percent of directors reported a lack of confidence in their board's understanding of cyber risk, and cited a background in information technology as one of the top four attributes such directors would look for in a new board candidate. Directors

also identified IT strategy as one of the top five items they would choose if setting the agenda for their next meeting. These responses may reflect an awareness of not only growing litigation risk, but also increased regulatory attention to cyber security. The December 31, 2010 FTC "Red Flags Rule" (16 CFR § 681), for instance, addressed Identity Theft Protection Programs, and required their adoption by any company that is a financial institution or "creditor" – a term defined broadly to include any company that permits deferred payment. Guidance issued by the SEC's Division of Corporation Finance in October 2011 ("CF Disclosure Guidance: Topic No. 2 - Cyber Security") (http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm) summarizes the SEC's views on public company disclosure obligations of cyber security risks and breach incidents. Recently, on February 12, 2014, the National Institute of Standards and Technology issued a *Framework for Improving Critical Infrastructure Cyber Security*, designed to provide a cost-effective mechanism for critical infrastructure companies, including energy, financial services, emergency services, health care and public health, and critical manufacturing to manage cyber security risk. (See http://www.ulmer.com/news-events/alerts/striving-for-security-understanding-the-new-cyber.)

In light of this burgeoning area of potential director and officer liability, companies must seriously address both the potential for and the risk of data breaches and other possible cyber risks. The team tasked with addressing cyber risks can no longer be limited to IT personnel, but must include senior management, legal, risk management, public relations, and compliance/audit. While this is an area where one size does not fit all, boards may consider designating oversight responsibility for cyber risk management to a particular board committee, with clear lines of reporting and authority, and at least annual review by the entire board. Cyber security risk assessments, either conducted internally, or utilizing the services of an outside

vendor, are becoming recognized as the logical starting point for addressing these matters. Regular education and training programs are essential, not only for personnel directly involved in data security, but also for supervisory management and for directors, who may not be as "tech-savy" as plaintiffs' attorneys would argue they should be.

Lastly, a review of the company's insurance coverage for cyber risk is essential. Existing D&O policies may provide coverage for such risk, absent a data breach claim exclusion. Commercial general liability policies may also provide limited coverage for the expense of compensating customers whose information is breached. Specialty privacy and data breach insurance policies are becoming more prevalent, and should be investigated if gaps appear in existing insurance.