DELAWARE BUSINESS COURT INSIDER

August 20, 2014

An ALM Website

Board of Directors Duty of Oversight and Cybersecurity

By Eduardo Gallardo and Andrew Kaplan,
Delaware Business Court Insider

Over the last two years, cyberattacks have continued to grow in both number and severity. In 2013, the FBI notified 3,000 companies in the United States that they had been victims of cyberattacks. Indeed, a recent report issued by the Center for Strategic and International Studies has estimated that cybercrime cost the global economy up to $575 billion annually and approximately $100 billion in the United States alone. And recent headline-grabbing cybercrime incidents involving diverse companies such as Target and Wyndham have demonstrated that cybersecurity is a matter to be taken seriously by management and the board of directors of every publicly traded company.

U.S. government officials and regulators have taken note of the significant effects of cyberattacks. For example, in 2011, following a joint letter from five U.S. senators to U.S. Securities and Exchange Commission Chairman Mary Schapiro, the SEC released disclosure guidelines regarding a public company's obligation to address cybersecurity threats. More recently, in June 2014, SEC Commissioner Luis Aguilar gave a speech at the New York Stock Exchange in which he noted that "board oversight of cyberrisk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks."

With cybersecurity attacks occurring with greater frequency and government regulators turning a sharper focus toward cybersecurity issues, corporate boards and their advisers should consider applicable case law in addressing the board's fiduciary duties to monitor and minimize cybersecurity risk. In *In re Caremark International Derivative Litigation*, 698 A.2d 959 (Del.Ch. 1996), and its progeny, Delaware courts articulated the scope of a board's duty to monitor and oversee corporate risk. Importantly, liability for failure to monitor risk can only be imputed to individual board members where: "(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

Eduardo Gallardo and Andrew Kaplan

knew that they were not discharging their fiduciary obligations," according to *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006), citing *Caremark*.

Since *Caremark*, the good-faith duty to monitor risk has been addressed in hundreds of cases, according to Charles R. Ragan in "Information Governance: It's a Duty and It's Smart Business." While courts have considered potential liability for failure to monitor risks, Delaware courts have been careful not to allow plaintiffs to use the duty to monitor as a vehicle to second-guess a well-informed board's business decisions, including well-informed decisions regarding risk-taking. Notably, in *In re Citigroup Shareholder Derivative Litigation*, 964 A.2d 106 (Del. Ch. 2009), then-Chancellor William B. Chandler III rejected the plaintiffs' claims that Citigroup board

members breached their fiduciary duty by failing to prevent the losses incurred by Citigroup as a result of its substantial exposure to the subprime mortgage market. The court held that the alleged warning signs cited by the plaintiffs were insufficient to imply knowledge of the need to oversee subprime mortgage investment decisions. The court reiterated its well-established principle that "the mere fact that a company takes on business risk and suffers losses—even catastrophic losses—does not evidence misconduct and without more, is not a basis for personal director liability." Following similar reasoning to *Citigroup*, in *In re Goldman Sachs Group Shareholder Litigation*, C.A. No. 5215-VCG (Del. Ch. Oct. 12, 2011), the court dismissed the plaintiffs' *Caremark* claims that directors failed to satisfy their oversight responsibilities with regard to compensation practices that allegedly led to overly risky business decisions.

Two cases have recently been filed in which shareholders are seeking to recover damages from board members for alleged failure to adequately monitor cybersecurity risks that directly implicate the *Caremark* progeny as it relates to the duties of a board. Following Target's reported consumer data breach in December 2013, shareholders filed a derivative suit in the District of Minnesota alleging that Target's board breached its fiduciary duties to the company by failing to maintain proper controls relating to data security, in *Kulla v. Steinhafel*, No. 14-cv-00203 (D. Minn. July 18, 2014). The complaint alleges that the board's failure to institute effective monitoring systems for cybersecurity caused Target to be exposed to millions of dollars of potential liability in class action lawsuits. Similarly, board members of Wyndham Worldwide Corp. are defending against allegations that they breached their duty to monitor risk following a consumer data leak, in *Palkon v. Holmes*, No. 2:14-cv-01234 (D.N.J. Feb. 27, 2014). The complaint alleges that the board's failure "to ensure that the company and its subsidiaries implemented adequate information security policies" and use of an operating system that was so out of date that the vendor "stopped providing security updates for the operating system more than three years prior to the intrusions" is enough to show that the board breached its duty to monitor and manage the cybersecurity risk of the company.

In light of the emphasis that has been recently placed by regulators, including the SEC, on cybersecurity issues, the pending rise of litigation stemming from cybercrime, and the guidelines offered by *Caremark* and its progeny, it would be advisable for boards of directors to act proactively to incorporate cybersecurity issues into their risk oversight functions to ensure that their fiduciary duties are properly discharged. With that in mind, the following are selected recommendations for boards to help ensure that they properly comply with their risk management obligations:

• Cyberrisk education for directors, including potential retention of cybersecurity experts and consultants to provide periodic updates to the board on new developments.

• Have enterprise risk committee or entirety of the board assume responsibility to ensure oversight and understanding of cybersecurity controls.

• Invest time and resources into making sure that management has developed a well-constructed and deliberate response plan that is consistent with best practices for a company in the same industry.

• Develop a business culture that prioritizes cybersecurity.

• Maintain cybersecurity insurance policy.

In the words of Aguilar, "Boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."

Eduardo Gallardo *is a partner in Gibson, Dunn & Crutcher's New York office. He focuses his practice on mergers and acquisitions and has experience representing public and private acquirers and targets in connection with mergers, acquisitions and takeovers, both negotiated and contested.*

Andrew Kaplan *is a corporate associate in the firm's New York office.*

Reprinted with permission from the August 20 2014 edition of DELAWARE BUSINESS COURT INSIDER © 2014 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 203-08-14-01