The Board's Cybersecurity Responsibility

by James M. Westerlind[1] | May 2, 2016 at 6:05 am

[2]

[3]

It is beyond question at this point that cybersecurity is a key obligation of the board of directors with respect to its enterprise

risk management function. Luis A. Aguilar, the commissioner of the SEC, made this clear in a speech at the New York Stock Exchange in 2014, saying, "there can be little doubt that cyber-risk also must be considered as part of a board's overall risk oversight." Hence, a company's board members each have a fiduciary duty to shareholders and investors to actively oversee the measures in effect to protect the company's sensitive data and that of its customers.

But what is a board member's legal duty in this regard? Under Delaware law, for example, the threshold for director oversight liability is very high and may arise: "a) where 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," according to Stone ex rel. AmSouth Bancorporation v. Ritter. Thus, it is critical that a board exercise good faith judgment that the company's information and reporting system is adequate in concept and design to assure the board that appropriate information will come to its attention in a timely manner in the ordinary course of its operations.

More recently, in October 2014's *Palkon v. Holmes*, the court dismissed a shareholder derivative lawsuit against the board members of Wyndham Worldwide

Corporation that had resulted from numerous data breaches

sustained by the global hotel and resort operator. The court concluded that Wyndham's board of directors had sufficient familiarity with the underlying facts when it denied the shareholder's demand that the company hold its board members personally liable for the losses the company sustained, as the board had previously discussed the cyberattacks at 14 meetings over the prior four years; the company's general counsel had given a presentation regarding the breaches (and Wyndham's data security generally) at every quarterly meeting; and Wyndham's audit committee had discussed these same issues in at least 16 committee meetings during the same period.

The lesson to be learned from *Palkon* is that a board should regularly address cybersecurity at its meetings—more than annually—and that an even better idea is to create a subcommittee for the subject. Some commentators also suggest retaining an outside board member with cybersecurity expertise to further inform the board. The amount of effort and money that a board spends on cybersecurity, however, is premised on a cost-benefit analysis based on what type of sensitive data the company maintains and how important it is to protect. If the board makes an informed decision in this regard, it should satisfy its fiduciary obligations with respect to the duty of care to the company.

The Federal Trade Commission had also initiated a separate lawsuit against Wyndham contending that its conduct in connection with the same data breaches that were the subject of the *Palkon* lawsuit violated federal law prohibiting unfair or deceptive trade practices affecting commerce. Wyndham eventually settled. The terms of the settlement are interesting as

the FTC did not require Wyndham to pay any fines, but rather that the corporation comply with annual audits of its information security program to conform to the Payment Card Industry Data Security Standard for certification of a company's security program. In addition, Wyndham's annual audits will require certification of: 1) the "untrusted" status of franchisee networks, to prevent future hackers from using the same method used in the company's prior breaches; 2) the extent of compliance with a formal risk assessment process that will analyze the possible data security risks faced by the company; and 3) the auditor is qualified, independent and free from conflicts of interest.

The terms of this settlement should be of particular interest to boards of directors and their general counsel as they may provide insight into what protocols the FTC believes are important to prevent data breaches and resulting liability.

In Executive Order 13636, titled "Improving Critical Infrastructure Technology," President Obama required the National Institute of Standards and Technology (NIST) to develop a voluntary cybersecurity framework that provides a "prioritized, flexible, repeatable, performance-based and cost-effective approach" to manage cybersecurity risk for those processes, information and systems directly involved in the delivery of critical infrastructure services. Nearly every expert in the field has recommended that companies seeking to devise protocols for cybersecurity should follow the guidelines set forth in the resulting framework, the NIST Framework for Improving Critical Infrastructure, published in February 2014.

Considering the case law, including the parameters of Wyndham's settlement with the FTC, and recommendations from experts in the field, it appears that a board of directors would likely protect its company from losses and liability—and its members from personal liability for breach of their fiduciary duty of care in connection with cybersecurity—by following the guidelines set forth in the framework.

More articles by James M. Westerlind[4] »

About the Author

James M. Westerlind is counsel at Arent Fox LLP.

1. http://www.rmmagazine.com/author/james-m-westerlind/
2. http://www.rmmagazine.com/wp-content/uploads/2016/04/RM05.16_ff_boardcybersecurity.jpg
3. http://www.rmmagazine.com/wp-content/uploads/2016/04/RM05.16_ff_boardcybersecurity.jpg
4. http://www.rmmagazine.com/author/james-m-westerlind/