Mitigating your Business Risk

Board Responsibilities in Cybersecurity

BY WILLIAM R. DENNY, POTTER ANDERSON & CORROON LLP

HIGH-PROFILE CYBER BREACHES have affected millions of customers and employees, resulting in unprecedented losses to businesses through direct costs in responding to the breaches, regulatory penalties, lawsuits brought by customers and business partners, business disruption, reputational damage and loss of shareholder value. Officers and directors are increasingly facing the possibility of personal liability for these losses.

A Director's Fiduciary Duties

In the past, directors were generally free from personal liability for cybersecurity breaches, because directors' cybersecurity duties were unclear. Personal fiduciary liability claims against Wyndham, Target, and Home Depot directors were all dismissed because the directors' cybersecurity monitoring duties were not clear enough to be "known duties" that would give rise to personal liability. Courts also concluded that claims that directors should have known of threats or had access to information about threats did not create liability for fiduciaries.

However, current trends suggest that directors might be more likely to face personal liability for cybersecurity breaches in the future as directors' cybersecurity responsibilities become clearer. Just this year, a judge in Georgia declined to dismiss a claim against a director of Equifax, Inc., who had personal knowledge of cybersecurity vulnerabilities, yet misrepresented the strength of the organization's technology. Also, this year, a judge in California approved the first settlement against directors and officers of Yahoo! Inc. relating to a data breach. The complexity and frequency of cybersecurity breaches, the severe consequences of a breach to corporations, and the growth of the cybersecurity industry all appear to clarify directors' cybersecurity duties.

When directors fail to institute or monitor cybersecurity measures, or when they consciously disregard red flags that they have a known duty to address, shareholders may bring claims to hold directors personally liable. A recent decision by the Delaware Supreme Court in June of 2019 called *Marchand v. Barnhill,* illustrates the importance of boards exercising reasonable oversight.

Marchand involved an ice cream manufacturer, Blue Bell Creameries, which operated numerous manufacturing plants in the U.S. In 2015, Blue Bell suffered a listeria outbreak in several of its manufacturing plants, which spread and caused the deaths of three people. The company was forced to recall its products, shut down production at several of its plants and lay off a large part of its workforce. Blue Bell had a history of food safety violations, but there was little evidence that the board was addressing those concerns. Shareholders sued the officers and directors, alleging that they breached their fiduciary duties of loyalty by failing to make good faith efforts to ensure that the company's regulatory compliance programs were adequate. According to the complaint, the board had no committee overseeing food safety, no board-level process to address food safety issues and no process to be advised of food safety reports or developments. Although the Delaware Court of Chancery dismissed the case against the directors, the Delaware Supreme Court reinstated the case, ruling that the complaint adequately alleged that the directors violated their duty of loyalty by consciously failing to attempt to assure that reasonable information and reporting systems existed and by failing to conduct reasonable investigations.

The principles of *Marchand* apply directly to cybersecurity risk. If a company suffers significant losses due to data breach and it is revealed that the directors failed to design board-level systems to oversee and monitor organization risk, or consistently failed to monitor those systems for red flags or cyber threats or conduct reasonable investigations, they could face personal liability. In June of 2014, then-SEC Commissioner, Luis Aguilar, counseled boards of directors that they are "already responsible for overseeing the management of all types of risks … and there can be little doubt that cyber risk also must be considered as part of the board's overall risk oversight."

Practical Guidance for Directors and Officers

The following are practical steps that directors and officers should take to minimize cybersecurity risks for their organizations as well as to minimize risk to themselves of personal liability.

- Understand the laws, regulations and guidance relating to data security and privacy that are applicable to your organization by consulting with the appropriate experts. Be aware of which regulatory bodies have authority over the organization.
- Ensure that your organization has conducted a cyber risk assessment and understand your vulnerabilities. Be aware of what type of data your organization collects or maintains and how the data flows through the organization.

- For public companies, ensure that there are effective controls and procedures to address cybersecurity risks and incidents in required public filings and disclosures.
- Ensure that your organization has a written information security program and data privacy and security policies that are tailored to your risk profile. Make sure that employees receive regular and frequent security and privacy training, that policies are regularly updated, and that policies are properly implemented and enforced.
- Implement cybersecurity reporting systems and controls and monitor these systems to remain abreast of potential risks, red flags, and cybersecurity threats.
- Ask cybersecurity personnel about the security practices and policies of the organization and about any changes or red flags related to cybersecurity. Consider deficiencies revealed in audits and adopt a security plan that is tailored to the organization's specific risk profile.
- Be aware of which members or committees of the board have cybersecurity responsibilities. Make sure that at least one director is sufficiently technically educated to lead board discussions and questions on information security.
- Include cybersecurity as a regular topic at board meetings and make sure that, in both appearance and substance, the board is focused on the organization's security.
- Establish a culture of security by consistently updating and enforcing physical and technological security policies. A "tone at the top" is critical to achieving a culture of security.
- Oversee the prudent selection and monitoring of vendors and service providers to ensure that information of the organization remains free of unnecessary risk and that contracts with vendors contain appropriate security and privacy obligations, remedy for breach and audit rights.
- Be familiar with insurance policies that cover cyber risk and data breach response. Ask about their policy limits and exclusions, and whether they cover both first- and third-party data losses.

Conclusion

Directors and officers have a duty to oversee an organization's management of its cybersecurity risks. Instituting, updating, and monitoring system controls is key to avoiding personal fiduciary liability, and directors should give special attention to any red or yellow flags. As cybersecurity threats continue to proliferate, directors' good faith efforts to fulfill their oversight duties will not only protect them from potential personal liability, it will also protect the organization, its customers, employees, and shareholders. ■

William Denny is a Partner and Head of Cybersecurity, Data Privacy and Information Governance Practice Group at Potter Anderson & Corroon LLP.