New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 263—NO. 40

MONDAY, MARCH 2, 2020

Cyber Preparedness in the Boardroom

Directors in 2020 should approach cyber risk from a governance and duty of oversight perspective.

BY NICK GOLDIN AND KAREN HSU KELLEY

SHUTTERSTOCK

As cyber risk facing companies of all sizes continues to grow, more corporate directors than ever appear to appreciate that their role as fiduciaries requires them to maintain sustained focus on data privacy and cybersecurity just as much as they oversee more traditional elements of enterprise risk management. But even as boards increasingly expand their oversight of cybersecurity programs, there is a growing likelihood that their oversight will be challenged in the courts and second-guessed by regulators. The continued growth in the scope and number of cyber incidents will lead to more scrutiny of a board's oversight of a company's preparedness, mitigation, response and resiliency programs. After describing the governing standards, this article proposes 10 questions that directors might ask to help meet these standards while minimizing potential liability for perceived shortcomings in corporate cybersecurity programs.

Duties of Directors

It is well established under corporate law in Delaware and elsewhere that part of a director's duty of care to become and remain reasonably informed in making decisions and overseeing the company's business is a duty to oversee corporate risk. Under the familiar *Caremark* standard set out in *In re Caremark International Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996), directors will be liable for a breach of the duty of oversight only if there was a "sustained or systemic failure of the board to exercise over-

NICK GOLDIN *and* KAREN HSU KELLEY *are partners at Simpson Thacher & Bartlett. Associate* JONATHAN KAPLAN *contributed to the preparation of this article.*

sight – such as an utter failure to assure a reasonable information and reporting system exists." As further addressed in *Stone v. Ritter*, this standard requires proof that directors either "utterly failed to implement any reporting or information system or controls," or "consciously failed" to monitor or oversee the operations of the system or controls in order to be held liable. 911 A.2d 362 (Del. 2006).

Claims Against Directors

Perhaps unsurprisingly, then, claims against directors for failing to adequately oversee cyber risk almost universally have failed. The litigation against the directors of Wyndham hotels nonetheless provides a useful roadmap for how directors might approach cyber risk. In dismissing claims against the directors, the court in *Palkon v. Holmes*, 2014 WL 5341880 (D.N.J. Oct. 20, 2014), observed that the board had discussed the company's cybersecurity efforts at 14 meetings over four years, the audit committee had discussed cyber issues at 16 meetings at a minimum during this same period, and the company had hired technology experts to investigate each data breach and to make recommendations on enhancing the company's security, which the company implemented. On the other hand, in a closely watched securities fraud litigation relating to the Equifax incident, claims against the former CEO survived a motion to dismiss, where the former CEO is alleged to have had specific information about cybersecurity deficiencies. Lessons for directors could emerge from that litigation as well.

While outside the cyber context, the Delaware Supreme Court's more recent decision in *Marchand v. Barnhill,* 212 A.3d 805 (Del. Sup. Ct. 2019) is also instructive in understanding the duty of oversight. In *Marchand*, the plaintiffs alleged a breach of the duty of loyalty against the directors of Blue Bell, an ice cream manufacturer, for failing to implement an adequate reporting system and failing to inform themselves about food-safety compliance matters despite "red and yellow flags about growing food safety issues." There, the court unanimously held that a plaintiff stockholder alleged facts sufficient to show bad faith by the board by failing to make a good faith effort to oversee a company's material risks. Of particular relevance, the court held that in order to demonstrate a good faith effort to implement and monitor risk, boards need to ensure their companies have systems reasonably designed to identify, monitor and mitigate material risks. The court noted that Blue Bell's central compliance risk was food safety but that the board had no committee charged with monitoring food safety, no process in place to discuss food safety and no specific discussion of food safety was reflected in board minutes. Holding that Blue Bell did not have a protocol requiring that management update the board about food safety compliance, the court also observed that boards cannot ignore information that comes to their attention and should document their oversight efforts in board minutes and other meeting materials.

Apart from obligations under applicable corporate law, regulators are increasingly conveying their expectations of boards in the cyber risk context.

Regulatory Expectations of Boards

Apart from obligations under applicable corporate law, regulators are increasingly conveying their expectations of boards in the cyber risk context. Most recently, on Jan. 27, 2020, the SEC's Office of Compliance and Inspections and Examinations reiterated that SEC registrants should devote "appropriate board and senior leadership attention to setting the strategy of and overseeing the organization's cybersecurity and resiliency programs" and involve "board and senior leadership" in "updating policies and procedures to address any gaps or perceived weaknesses." Even though this particular guidance was directed at broker-dealers, investment advisors, clearing agencies, national securities exchanges and other SEC registrants, it serves as a useful reminder on a broader scale of the importance from a regulatory perspective of board engagement on cyber risk. This guidance followed the SEC's "Statement and Guidance on Public Company Cybersecurity Disclosures," issued in February 2018, that reminded public companies about the obligation to disclose "how the board of

directors engages with management on cybersecurity issues." Likewise, the cyber regulations issued by the New York Department of Financial Services require DFS-regulated entities to ensure that boards are kept up to date about cyber risks and that boards or senior officers certify compliance with comprehensive cyber regulations.

Key Cyber Issues for Directors

As others have noted, there is no "one size fits all" approach when it comes to cybersecurity, given that different sectors present different cyber risk profiles. Drawing on the governing standards, case law, and regulatory guidance, however, set forth below are 10 universal questions that directors might ask as part of their oversight of a company's cybersecurity program. In essence, these questions are geared at evaluating whether management has developed sufficient systems to identify and mitigate the particular cyber risks facing a company and has operational resiliency plans to insure a comprehensive and prompt response to a cyber incident.

(1) Who is responsible for organization-wide security preparedness? Companies should identify a senior person with clear responsibility for organization-wide security preparedness and ensure that the board regularly receives updates from this individual. This person is often a Chief Information Security Officer, but it does not need to be.

(2) What resources have been allocated to address cyber risk? Management should evaluate the budget, staffing, and expertise needed to maintain a proper cyber risk program. This will depend on a variety of factors, including the industry in which the company operates.

(3) Does our company have a sufficient written cybersecurity program? It is essential for companies to formulate a comprehensive, written data privacy and cybersecurity plan. This is one of the key aspects of any cybersecurity program. The plan should then be reviewed by, and distributed to, all individuals who may be involved in its execution and kept current as cyber risks evolve.

(4) Are our employees sufficiently trained? Companies need to institute effective training programs that instruct employees on the appropriate handling and protection of sensitive data.

(5) Have cyber systems at third-party vendors been closely scrutinized? Companies should take steps to mitigate the cybersecurity risks associated with outsourcing business functions to third parties. A company can have robust data privacy and security policies and practices, but if its vendors, who have access to the company's data, do not have a similarly robust cybersecurity program, the company is leaving itself vulnerable.

(6) What regulatory and statutory schemes apply to data our company handles? Companies need to be aware of whether they are subject to federal, state and international laws that require them to take measures to secure sensitive data.

(7) Does our company have, or need, cyber liability insurance? Companies need to consider whether cyber liability insurance is available and appropriate to purchase.

(8) Does our company have sufficient threat detection capabilities? Companies need to ensure that they have state-of-the-art technology for preventing the downloading of malicious software and detecting and alerting the company to attempted breaches.

(9) Does our company have a comprehensive, written breach response plan? It is critical that companies be prepared to respond to a breach quickly, efficiently and calmly. To that end, companies should have a comprehensive, written breach response plan in place, and they must be clear on what will trigger the response plan. As part of this plan, companies should form a breach response team composed of individuals from key departments and external advisors, if necessary, and identify individual functions and responsibilities in case of a breach.

(10) Does our company secure non-digital information and physical devices? Sensitive non-digital information must be safeguarded as well. To the extent possible, companies should minimize the locations in which sensitive non-digital information is stored and should ensure the safe and secure storage of this data.