Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity for Directors

In the evolving world of cybersecurity risk, companies and their officers and directors should continue to monitor and take into account developments regarding plaintiff shareholder derivative lawsuits and board of director actions, as well as legal, regulatory and industry developments and cybersecurity events, the author writes.

Director Cybersecurity Risk Oversight and Actions

BY MELISSA J. KRASNOW

This article begins by providing an overview of the duty of directors to oversee risk, including cybersecurity risk, in the cyberattack context and then outlines actions that board of directors are taking as reported by surveys, noting commonalities between certain of these actions and recommendations from director institute publications.

Director Cybersecurity Risk Oversight

Under Delaware law, directors owe fiduciary duties to the corporation—the duty of care and the duty of loyalty. Delaware case law describes the director duty to monitor and oversee risks as derived from the duty of care and the duty of loyalty.[1]

In *Palkon v. Holmes*, a plaintiff shareholder filed a derivative lawsuit on behalf of Wyndham (which is a Delaware corporation) against Wyndham and its individual directors and officers regarding three cyberattacks against Wyndham involving the personal information of over 600,000 customers between 2008 and 2010.[2] To bring the lawsuit on behalf of Wyndham, the plaintiff needed to plead with particularity that the board's decision to refuse his demand to bring lawsuit regarding the cyberattacks was in bad faith or not based on a reasonable investigation. Under the business judgment rule, there is a presumption that the board refused the demand on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company. Defendants argued, among other things, that the board's decision to refuse the demand was a good faith exercise of business judgment, made after a reasonable investigation.

The court in *Palkon* dismissed the lawsuit with prejudice and described the failure to act in good faith (as part of the duty of loyalty) that is required to show director oversight liability in a footnote:

> *Caremark* requires that a corporation's ''directors utterly failed to implement any reporting or information system . . . [or] consciously failed to monitor or oversee its operations thus disabling themselves from being informed.''[3] Yet Plaintiff concedes that security measures existed when the first breach oc-

Melissa J. Krasnow is a partner with Dorsey & Whitney LLP, in Minneapolis. She is an advisory board member for the Bloomberg BNA Privacy & Security Law Report and the International Association of Privacy Professionals. She is a Certified Information Privacy Professional/U.S. and a National Association of Corporate Directors Fellow.

[1] *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).
[2] *Palkon v. Holmes*, No. 2:14-CV-01234 (D.N.J. Oct. 20, 2014) (13 PVLR 1866, 10/27/14).
[3] *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

curred, and admits the Board addressed such concerns numerous times. (Compl. ¶¶ 46, 62, 63). The Board was free to consider such potential weaknesses when assessing the lawsuit.[4]

According to the Delaware Supreme Court in *Stone v. Ritter*, ''The failure to act in good faith may result in liability because the requirement to act in good faith 'is a subsidiary element[,]' i.e., a condition, 'of the fundamental duty of loyalty.' It follows that because a showing of bad faith conduct, in the sense described in *Disney* and *Caremark*, is essential to establish director oversight liability, the fiduciary duty violated by that conduct is the duty of loyalty.''[5] It is important to note that Delaware law does not permit eliminating or limiting the personal liability of a director to a corporation or its stockholders for monetary damages for breach of fiduciary duty for any breach of the director's duty of loyalty to the corporation or its stockholders or for acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of law, among other things.[6] Companies should consider reviewing their organizational documents, indemnification agreements or policies and directors and officers liability insurance and cybersecurity liability insurance coverage.

The *Target*, *Home Depot* and *Wyndham* cases may provide further guidance about what is required to show liability regarding the duty of a director to oversee risk, including cybersecurity risk, and shape the actions that directors take in fulfilling their oversight duty.

Actions of Wyndham that were mentioned in *Palkon v. Holmes* included: (1) board discussion of the cyberattacks, Wyndham's security policies and proposed security enhancements at 14 meetings and audit committee discussion at 16 meetings between 2008 and 2012; (2) Wyndham's hiring of technology firms to investigate each cyberattack and to issue recommendations on enhancing Wyndham's security; (3) Wyndham beginning to implement those recommendations after the second and third data cyberattacks and (4) presentations of Wyndham's general counsel regarding the cyberattacks and/or Wyndham's data security generally at every quarterly board meeting.[7]

Other plaintiff shareholder derivative lawsuits that have been filed (including Target and Home Depot) and that will be filed regarding cyberattacks should be monitored for developments. Home Depot, like Wyndham, is a Delaware corporation. Since Target is a Minnesota corporation, Minnesota law is applicable. These cases may provide further guidance about what is required to show liability regarding the duty of a director to oversee risk, including cybersecurity risk, and shape the actions that directors take in fulfilling their oversight duty.[8]

Board of Director Actions Regarding Cybersecurity Risk

Two surveys shed light on actions that boards are taking regarding cybersecurity risk. According to the Georgia Tech Information Security Center 2015 Report on Governance of Cybersecurity: How Boards & Senior Executives Are Managing Cyber Risks (''Georgia Tech Report'') and The Global State of Information Security® Survey 2016 (''Security Survey''), boards are: (1) addressing information security, (2) receiving information about privacy and security risks, (3) reviewing incident response plans, (4) receiving information about breaches and incidents, (5) reviewing privacy and security policies, (6) reviewing budgets for privacy and security, (7) reviewing cybersecurity liability insurance and (8) having a director with cybersecurity expertise.[9]

Respondents to the Georgia Tech Report were at the board or senior executive level at Forbes Global 2000 companies (38 percent from North America, 31 percent from Europe and 21 percent from Asia). 43 percent of the respondents were inside or outside directors and the remainder were outside non-voting attendees and senior executives. 73 percent of the respondents were from critical infrastructure companies. Respondents to the Security Survey were chief executive officers, chief financial officers, chief information officers, chief information security officers, chief security officers, vice presidents and directors of information technology and security practices (37 percent from North America, 30 percent from Europe, 16 percent from Asia Pacific, 14 percent from South America and 3 percent from the Middle East and Africa).

There are commonalities between certain of these actions and recommendations from two director institute publications, the National Association of Corporate Directors (NACD) Cyber-Risk Oversight Handbook (the Handbook) and the Global Network of Director Institutes (GNDI) ''Guiding Principles for Cybersecurity Oversight'' perspectives paper (the Paper).[10] The GNDI is comprised of 16 member director institutes, including NACD in the U.S. and the Institute of Corporate Directors in Canada, as well as the Australian Institute of Company Directors, the Brazilian Institute of Corporate Governance, the European Confederation of Director Associations, the Gulf States Gulf Cooperation Council Board Directors Institute, the Hong Kong Institute of Directors, the Malaysian Alliance of Corporate Direc-

[4] *Id.*

[5] *Id.*, at 369-70.

[6] Del. Gen. Corp. Law § 102(b)(7).

[7] *Palkon v. Holmes*, No. 2:14-CV-01234 (D.N.J. Oct. 20, 2014).

[8] *In re Target Corp. Shareholder Derivative Litig.*, No. 14-cv-00203-PAM-JJK (D. Minn. July 18, 2014); *Bennek v. Ackerman*, No. 1:15-cv-02999 (N.D. Ga. Aug. 25, 2015).

[9] Jody R. Westby, Adjunct Professor, Georgia Institute of Technology CEO, Global Cyber Risk LLC; research sponsors Forbes, Financial Services Roundtable and Palo Alto Networks, ''Georgia Tech Information Security Center 2015 Report on Governance of Cybersecurity: How Boards & Senior Executives Are Managing Cyber Risks'' (October 2015); PricewaterhouseCoopers LLP, CIO and CSO, ''The Global State of Information Security® Survey 2016'' (October 2015).

[10] Larry Clinton, Internet Security Alliance, NACD and AIG, ''Cyber-Risk Oversight'' (June 2014); GNDI, ''Guiding Principles for Cybersecurity Oversight'' (November 2015).

  PVLR ISSN 1538-3423

tors, the Mauritius Institute of Directors, New Zealand's Institute of Directors, the Pakistan Institute of Corporate Governance, the Singapore Institute of Directors, the Institute of Directors in Southern Africa, the Swiss Institute of Directors, the Thai Institute of Directors and the United Kingdom's Institute of Directors.

Addressing Information Security

According to the Georgia Tech Report, 63 percent of respondent boards are actively addressing and governing computer and information security and computer and information security, including reviewing security budgets, designating roles and responsibilities for the management of privacy and security, developing and reviewing top-level policies, receiving regular reports on security risks and incidents, reviewing annual risk assessments of the security program and reviewing cyber-incident response plans. Addressing information security was the fifth highest issue of importance to boards, following long term strategy and operational goals, risk management, compliance and mergers and acquisitions. The Security Survey found that 45 percent of boards participate in overall security strategy and 37 percent participate regarding security technologies.

Addressing information security involves asking questions to become informed. The Handbook provides examples of questions for directors to ask and NACD subsequently has provided additional examples of questions at https://www.nacdonline.org. In addition to NACD, other organizations have provided examples of questions for directors to ask.[11]

Receiving Information About Privacy and Security Risks

The Georgia Tech Report found that 82 percent of boards regularly or occasionally received reports from senior management regarding privacy and IT security risks. 93 percent of respondents said their boards reviewed risk assessment reports and 53 percent said their boards used outside experts to help with risk assessments and risk management. 63 percent of respondents said their board regularly or occasionally reviewed annual security program assessments. 47 percent of respondents said their board regularly or occasionally reviewed and approved roles and responsibilities of personnel responsible for privacy and security risks. According to the Security Survey, 32percent of boards review security and privacy risks and 35 percent of security leaders deliver information security risk updates to the board at least four times a year. According to two of the five principles in the Handbook, (1) directors should understand the legal implications of cybersecurity risks as they relate to their company's specific circumstances and (2) boards should have adequate access to cybersecurity expertise and discussions about cybersecurity risk management should be given regular and adequate time on the board meeting agenda.

Reviewing Incident Response Plans

While 74percent of the respondents in the Georgia Tech Report said they had reviewed their company's incident response plan, 46percent said they had participated in a test scenario against the plan. Examples of questions that directors could ask regarding incident response plans and testing include: (1) what the date of the plan is and what was the most recent date of testing the plan, (2) how frequently is the plan tested or updated, (3) what was the situation that was the subject of the testing, (4) what are the results of and insights from the testing or updating of the plan, (5) who are the members of the incident response team, (6) who are the external team members (including service providers), (7) what are team member responsibilities, (8) what are the lines of communication, (9) what communications, disclosures and notifications are being considered and (10) what is the nature of and how frequently is employee security training and awareness provided.[12]

Receiving Information About Breaches and Incidents

69% of respondents in the Georgia Tech Report said their board regularly or occasionally reviewed reports of security breaches or incidents involving the disclosure of personally identifiable information or theft of corporate data. Issues relating to such reporting to the board include: (1) how a company becomes aware of such breaches, incidents and thefts, (2) what are the criteria for reporting such breaches, incidents or thefts to the board, (3) what are the channels of communications and the content of the communications to the board, (4) whether external service providers are involved and (5) timing and other considerations regarding providing communications, disclosures and notifications regarding such breaches, incidents and thefts, internally as well as externally. As of 2016, 47 states (all U.S. states except Alabama, New Mexico and South Dakota), plus the District of Columbia, Guam, Puerto Rico and Virgin Islands have enacted breach notification laws. The Health Insurance Portability and Accountability Act[13] provides for breach notification. Other countries have breach notification laws. The U.S. Securities and Exchange Commission provides guidance regarding disclosure of cybersecurity risks and cyber-incidents.[14]

Reviewing Privacy and Security Policies

64 percent of respondents in the Georgia Tech Report said their board regularly or occasionally reviewed and approved top-level policies regarding privacy and security risks. The Security Survey found that 41 percent of boards participated regarding security policies.

Reviewing Budgets for Privacy and Security

50 percent of respondents in the Georgia Tech Report said their board regularly or occasionally reviewed and

[11] *See, e.g.*, The Institute of Internal Auditors Research Foundation and Information Systems Audit and Control Associations Inc., ''What the Board of Directors Needs to Ask'' (Aug. 18, 2014); ISACA, ''The Cyberresilient Enterprise: What the Board of Directors Needs to Ask'' (Aug. 20, 2015).

[12] For additional information about incident response plans, *see* Melissa Krasnow, ''Guidance for Guidance for Incident Response Plans,'' International Risk Management Institute (May 2015).

[13] Pub. L. No. 104-191, *as amended by* the Health Information Technology for Economic and Clinical Health Act (enacted under Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5).

[14] *See* Division of Corporation Finance, U.S. Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011); Melissa Krasnow, The Securities and Exchange Commission's Guidance on Cybersecurity and Cyber Incident Disclosure, BNA Privacy & Security Law Report (Oct. 31, 2011) (10 PVLR 1575, 10/31/11).

approved annual budgets for privacy and IT security programs. In the Security Survey, 46 percent of boards participated regarding security budgets and respondents boosted their information security budgets by 24 percent in 2015. According to one of five principles in the Handbook, directors should set the expectation that management will establish an enterprise-wide cybersecurity risk management framework with adequate staffing and budget.[15]

Reviewing Cybersecurity Liability Insurance

48 percent of the respondent boards reviewed their company's insurance for cyber-related risks per the Georgia Tech Report. 50 percent of respondents said their company had quantified the business interruption or loss exposure from a cyber-incident. According to one of the five principles in the Handbook, board-management discussion of cybersecurity risk should include identification of which risks to avoid, accept, mitigate or transfer through insurance, as well as specific plans associated with each approach.

Having a Director With Cybersecurity Expertise

23 percent of respondents in the Georgia Tech Report said their board had a director with cybersecurity expertise. The GNDI recommended in the Paper that boards consider adding a member with some knowledge of information technology (including digitalization and cybersecurity). It is interesting to note that legislation was introduced in the U.S. that would require a public company to disclose to the Securities and Exchange Commission (SEC) whether any director has cybersecurity expertise or experience; if no director has cybersecurity expertise or experience, such legislation would require the public company to describe the other cybersecurity steps taken by the public company that were taken into account by persons responsible for identifying and evaluating director nominees. The SEC, in coordination with the National Institute of Standards and Technology, would define what constitutes cybersecurity expertise or experience, such as professional qualifications to administer information security program functions or experience detecting, preventing, mitigating or addressing cybersecurity threats.″ See S. 2410: Cybersecurity Disclosure Act of 2015 at[16].

Conclusion

In the evolving world of cybersecurity risk, companies and their officers and directors should continue to be monitor and take into account developments regarding plaintiff shareholder derivative lawsuits and board of director actions, as well as legal, regulatory and industry developments and cyber events.

---

[15] *See, e.g.*, National Institute of Standards and Technology, ''Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0'' (Feb. 12, 2014).

[16] https://www.govtrack.us/congress/bills/114/s2410.

  PVLR ISSN 1538-3423