Akin®

Top 10 Topics for Directors in 2016: Cybersecurity

Dec 30, 2015

Reading Time : **5 min**

By: Kerry E. Berchem, Rick L. Burdick, Garrett A. DeVries, Dan Fisher, Natasha G. Kohne, Christine B. LaFollette, Zachary N. Wittenberg, Iain Wood

Risk management. One of the biggest concerns facing boards is how to provide effective oversight of cybersecurity. The following are questions that boards should be asking:

- *Governance*. Has the board established a cybersecurity review committee and determined clear lines of reporting and responsibility for cyber issues? Does the board have directors with the necessary expertise to understand cybersecurity and related issues?
- *Critical asset review*. Has the company identified what its highest cyber risks assets are (e.g., intellectual property, personal information and trade secrets)? Are sufficient resources allocated to protect these assets?
- *Threat assessment*. What is the daily/weekly/monthly threat report for the company? What are the current gaps, and how are they being resolved?
- *Incident response preparedness*. Does the company have an incident response plan, and has it been tested in the past six months? Has the company established contracts via outside counsel with forensic investigators in the event of a breach to facilitate quick response and privilege protection?
- *Employee training*. What training is provided to employees to help them identify common risk areas for cyber threat?
- *Third-party management*. What are the company's practices with respect to third parties? What are the procedures for issuing credentials? Are access rights limited and backdoors to key data entry points restricted? Has the company conducted cyber due

diligence for any acquired companies? Do the third-party contracts contain proper data breach notification, audit rights, indemnification and other provisions?

- *Insurance*. Does the company have specific cyber insurance, and does it have sufficient limits and coverage?
- *Risk disclosure*. Has the company updated its cyber risk disclosures in SEC filings or other investor disclosures to reflect key incidents and specific risks?

The SEC and other government agencies have made it clear that it is their expectation that boards actively manage cyber risk at an enterprise level. Given the complexity of the cybersecurity inquiry, boards should seriously consider conducting an annual third-party risk assessment to review current practices and risks.

Increased regulation. Directors should anticipate increased regulation for companies in the area of cybersecurity. The 3rd Circuit Court of Appeal's decision in the Federal Trade Commission's (FTC) suit against Wyndham Worldwide for a series of three data breaches—acknowledging the FTC's jurisdiction to regulate data security practices under its authority to regulate unfair and deceptive trade practices—will likely embolden the FTC in its role as de facto chief cybersecurity regulator.[3] Fortunately for defendants, such authority will not go unchecked, as evidenced by the dismissal of the FTC's action against LabMD.[4]

The SEC appears similarly emboldened in the area of cybersecurity, as 2015 was the SEC's most active year to date in setting out expectations regarding cybersecurity. The SEC Office of Compliance Inspections and Examinations (OCIE) issued multiple risk alerts and announced a new cybersecurity audit, and the Investment Management Division issued additional cybersecurity guidance. To make sure everyone was listening, the SEC announced an enforcement action against RT Jones, an investment advisor, pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 under Rule 30 of Regulation S-P for its "failure to adopt policies reasonably designed to protect customer records and information." Although there was no evidence that any client suffered financial harm, the investment advisor settled for $75,000.

Increased litigation exposure. Responsibility, accountability and liability in connection with data breaches are not always clear. Indeed, as evidenced by Target's recent $39 million settlement with certain major credit card brands, companies are fighting over who should be liable for exposure in a data breach. In October 2015, Visa/Mastercard/American Express and

others shifted liability to the bank of merchants who failed to implement "smart chip" (EMV) technology to credit cards.

Class action liability to consumers is also broadening. In *Remijas v. Neiman Marcus Gp*., the 7th Circuit reversed the district court's decision, ruling that Neiman Marcus customers whose credit card information was compromised had standing to bring a class action suit against the retailer.[5] With dozens of lawsuits being filed within days of a major data breach, most major data breach class actions are now being transferred to the multidistrict litigation panel in federal court. All of these issues signal that the risks of getting cybersecurity wrong will likely cost companies millions (and potentially hundreds of millions) in losses.

Director liability. Directors of companies that experience major data breaches are often faced with derivative actions following an event. However, provided that boards have been actively engaged in monitoring their companies' efforts to avoid and mitigate such a breach, the risk of personal liability appears to be slim. In assessing whether directors have met their duty of due care, the court will "look for evidence of whether a board has acted in a deliberate and knowledgeable way, identifying and exploring alternatives."[6] In the most notable case to date, the derivative lawsuit against Wyndham Worldwide's board of directors was dismissed. The court held that the directors were not grossly negligent in conducting the investigation, noting key metrics for directors: Wyndham's board had discussed the cyberattacks at 14 meetings during the relevant time frame, and the company's general counsel gave a presentation regarding the data breaches or data security at each meeting. The court also noted that the board's audit committee discussed these issues during at least 16 meetings over the same time period. Noting that the company had retained third-party technology firms to investigate each breach and recommend enhancements to Wyndham's systems, the court reasoned that the board had conducted a reasonable investigation.

International data transfers. Directors should also be aware of, and focus on, international data protection compliance. In late 2015, the European Court of Justice issued a landmark decision in *Schrems v. Data Protection Commissioner*, which invalidated the Safe Harbor that allowed for transfer of data between Europe and the United States.[7] Multinational companies faced a chaotic regulatory environment, with the U.S. Department of Commerce saying that it would still enforce the Safe Harbor and with some European Data Protection Authorities saying that they would prosecute companies transferring data from Europe to the United States in reliance on the now-invalidated Safe Harbor. European Union Justice Commissioner

Vera Jourova has since announced that the European Union has "agreed in principle" with the United States on a new trans-Atlantic data transfer agreement. Directors should be aware of their companies' international data protection practices and the ever-changing regulatory landscape internationally.

The National Association of Corporate Directors' (NACD) five principles of cybersecurity are instructive to keep directors on top of mitigating cyber risk:

1. Directors need to understand and approach cybersecurity as an enterprisewide risk management issue, not just an IT issue.

2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.

4. Directors should set the expectation that management will establish an enterprisewide risk management framework with adequate staffing and budget.

5. Board management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate or transfer through insurance, as well as specific plans associated with each approach.

This post was excerpted from our annual Top 10 Topic for Directors in 2016 alert. To read the full alert, please click here.

---

[1] PwC's 18th Annual Global CEO Survey 2015.

[2] Ponemon Institute's 2015 Global Megatrends in Cybersecurity (February 2015).

[3] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[4] *In re LabMD Inc.*, F.T.C. ALJ (Nov. 13, 2015).

[5] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015).

[6] *Palkon v. Holmes* ¸ No. 2:14-cv-01234 (D. N.J.).

[7] *Schrems v. Data Protection Commissioner* (Case C-362/14) (October 6, 2015).

Categories

Corporate Governance

Cybersecurity, Privacy & Data Protection

Compliance