New York Law Journal An ALM Website

Cybersecurity Risks and the Board of Directors

By David A. Katz and Laura A. McIntosh

New York Law Journal
November 29, 2012


Wachtell Lipton's David A. Katz


Wachtell Lipton's Laura McIntosh

As boards of directors examine the risks that their companies face, corporate cybersecurity issues loom large.[1] Forty-eight percent of directors (and 55 percent of general counsel) cited data security as their top concern in a recent study by Corporate Board Member/FTI Consulting.[2] These numbers have roughly doubled since 2008, when only a quarter of directors and general counsel cited data security as a major concern.[3] With revenues, intellectual property, business relationships and customer confidence potentially at stake, directors should consider whether their companies and management teams are adequately addressing the growing threat of cybersecurity in the new high-tech landscape.

Cybersecurity risk is a difficult and intimidating topic for corporate boards to consider. However, it is important to keep in mind that cybersecurity risk is only one of many areas of risk that are overseen by boards of directors and that, in most cases, the usual strategies and procedures for evaluating and managing risk can apply. Directors are not expected to be experts in this area and are entitled to rely upon management and outside experts for information and advice. Nonetheless, directors should request that management reports to the board on the steps the company is taking to mitigate cyber threats, and directors should consider whether the company is appropriately assessing its risks and devoting adequate resources to the issue. The business judgment rule remains the standard for evaluating decisions taken by a board in this area.

Significance of Cyber Crime

With high-profile cyberattacks against large commercial banks and other household-name companies and organizations making headlines in recent months, directors have good reason to be concerned.[4] As noted in the Corporate Board Member/FTI Consulting study, cyber risk is "invisible, ever-changing, and pervasive—making it very difficult for boards to manage."[5] The reputational and economic downsides for companies can be very significant. Preet Bharara, U.S. Attorney for the Southern District of New York, has observed:

If they are not aware and not prepared, companies can go from having a great reputation and all the value associated with it, to having that reputation trashed completely overnight.[6]

As to the financial stakes, the median annualized cost of cyber crime has been estimated at an average $5.9 million per company,[7] based on data from a 2011 study by the Ponemon Institute that found that the cost of a cybersecurity breach ranged from $1.5 million to $36.5 million among the study's respondents.[8] There is also some evidence that public companies that have been the target of cyber crime have suffered a resulting drop in stock price.[9] The Securities and Exchange Commission has outlined a list of costs and consequences of cyber crime that includes remediation costs, increased cybersecurity protection costs, lost revenues, litigation, and reputational damage.[10]

Most boards of directors recognize the importance of effectively managing cybersecurity risks, but there may be room to improve the process. The Corporate Board Member/FTI Consulting study found that one-third of the general counsel surveyed believe that their board is not effective at managing cyber risk.[11] Only 42 percent of directors in that study said that their company has a formal, written crisis management plan for dealing with a cyber attack, and yet 77 percent of directors and general counsel believe that their company is prepared to detect a cyber breach—statistics that reveal a "disconnect between having written plans and the perception of preparedness."[12] Indeed, a 2012 governance survey by Carnegie Mellon CyLab concluded that "boards are not actively addressing cyber risk management."[13] Only 25 percent of the study's respondents (drawn from Forbes Global 2000 companies) review and approve top-level policies on privacy and information technology risks on a regular basis, while 41 percent rarely or never do so.[14] These figures indicate a need for boards to be more proactive when it comes to overseeing cybersecurity risk management.

Risk Management

The board of directors always sets the "tone at the top." The board should clearly communicate to senior management its sense of the need to address cybersecurity issues and create a culture that views cybersecurity as "a corporate social responsibility."[15] As Howard A. Schmidt, the nation's first Cyber Security Coordinator (appointed by President Obama in 2009), stated recently:

[W]hile there is a cost to doing more to improve cybersecurity, there is a bigger cost if we do not and that cost is measured not only in dollars, but in national security and public safety.[16]

With this in mind, boards should foster an environment that respects the importance of cybersecurity, including heightening awareness of security risks and encouraging the reporting of security incidents.

A recent panel discussion sponsored by the National Association of Corporate Directors cited the "IT confidence gap" as a reason that directors may be intimidated by cybersecurity issues.[17] The panel pointed to several factors: the fact that most directors are in their sixties, meaning that they have spent the majority of their careers in the pre-digital era; the highly technical jargon used by experts in the field; and the complexity and fluidity of the technology itself. Though the technical nature of cybersecurity risks may indeed be daunting to directors, they themselves are not expected to become experts in this area. The former chief of the SEC's Office of Internet Enforcement remarked last year:

I do not believe it's realistic to expect board members to have anything but a high-level understanding of the nature of cyber threats and how they impact the business of the corporation. Just as you need a good accounting firm to give you financial expertise, from the board's perspective this field…requires you to tap into… the necessary expertise and make sure your company is doing all it can to protect itself.[18]

As a general matter, common sense and business judgment must apply in this area as in any other. Many of the same types of questions and approaches used by boards to address other categories of risk apply here as well. For example, directors should be confident that they understand both the company's level of exposure to cybersecurity risks and the programs in place to manage that risk.[19] It is important for the company's management to prioritize risks, recognizing what is the most sensitive and critical information, where it is located, how it is protected, and the potential effects of a security breach.[20]

Directors should consider whether the company's exposure is being effectively managed, recognizing that, as with any risk, it cannot be completely eliminated. Although there are many approaches that can be utilized, directors may want to be briefed on the assignment of responsibilities for cybersecurity

management and receive reports from senior management regarding cybersecurity risks, cyber attacks and cyber risk management programs. The board may wish to consider with management whether cyber insurance policies are needed or, if they are already in place, if the existing coverage is adequate. The board also may wish to review the company's annual budget for security risk management, including funds needed to hire outside consultants, if appropriate. Finally, boards should understand management's approach to the disclosure of any material cybersecurity-related risks or incidents, particularly in light of the relevant SEC guidance discussed below.

One potential difference between cybersecurity crises and other corporate crises is that both internal and external aspects of crisis management with respect to a cyber incident must begin within hours rather than days, in order to be as effective as possible. Directors should expect management to be prepared to respond very quickly to any cyber attack. As part of a preparedness plan, management should consider in advance the circumstances under which it would be appropriate to notify law enforcement. U.S. Attorney Bharara has encouraged companies to report cyber attacks promptly, hoping to overcome traditional corporate reluctance to involve law enforcement:

People need to develop a culture of early disclosure and communication with law enforcement. The quickest way to save a company—and to save massive damage to other people in a particular industry and beyond—is for law enforcement to have the ability to get the bad guys. And that possibility will be maximized if companies notify law enforcement right away.[21]

It is becoming more common for boards to have a separate risk committee in addition to the audit committee, though this is often not necessary or appropriate. Board committee structure should be determined based on a company's individual circumstances and, of course, any applicable laws and regulations. Depending on the nature of the company, the size of its board and the expertise of the directors, it might make sense to have a dedicated cybersecurity/technology committee. Unless the full board performs both functions, it would be advisable to separate the task of developing cybersecurity management programs from that of reviewing the controls and effectiveness of these programs.[22] Depending on the needs of the company, it may be worthwhile for the nominating committee to consider seeking one or more director candidates with some expertise in the area of cybersecurity and information technology. Notwithstanding the delegation of oversight responsibilities to one or more board committees, it is important to emphasize that the full board is responsible for risk management oversight generally, regardless of the specific type of risk at issue.

Regulatory, Legislative Efforts

The SEC Division of Corporate Finance released guidance in October 2011 on the topic of cybersecurity disclosure.[23] Though the guidance is only general, it is the best available, as the SEC has yet to issue any applicable rules or regulations. In its release, the SEC urges companies to "review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents."[24] Public companies are expected in certain cases to disclose cyber risks in advance of breaches and to disclose any material cyber incidents. The guidance discourages boilerplate and reduces companies' discretion in determining which cyberattacks are material. The release states that "disclosure that itself would compromise a registrant's cybersecurity" need not be disclosed;[25] however, companies frequently are reluctant to disclose information about cyber incidents for other reasons as well. Disclosing a cyberattack can be embarrassing and damaging for companies; it also can be difficult to draft the disclosure when a company may not fully understand what has happened from a technical perspective. Moreover, after—and in certain cases, perhaps even before—a company does experience and disclose a material cyberattack, the company may need to add a risk factor to its Form 10-Q and Form 10-K on the topic.[26]

To date, the U.S. Congress has failed to pass legislation relating to cybersecurity. The Cybersecurity Act of 2012 (SB 2105) was introduced in February 2012 and passed the House of Representatives but then stalled in the Senate due to privacy concerns. Competing bills reportedly are moving through Congress.[27] In August, it was reported that the White House is working on an executive order relating to cybersecurity.[28]

Director Liability

The business judgment rule applies to the question of whether a board's failure to manage cybersecurity risks can amount to a breach of fiduciary duty. There has been some suggestion by commentators that boards could be held to a higher standard in this area because of the existence of widely accepted best practices and standards in terms of cybersecurity and the existence of international standards released by organizations such as the International Organization for Standardization (ISO)[29] and the National Institute of Standards and Technology (NIST),[30] but we view this as unlikely. There is currently no reason to believe that the protections of the business judgment rule will not continue to apply in the area of cybersecurity to directors who fulfill their duty to act in good faith, with the loyalty and due care that are always required.

The issue of cybersecurity risk is likely to grow in prominence as our society and economy become ever more dependent on technology. Likewise, effective corporate management of cybersecurity is increasingly important not only for a company's employees, customers, and business partners, but also for society at large. As U.S. Cyber Security Coordinator Schmidt noted:

Until such time as cybersecurity becomes a regular board of directors' agenda item and measurable progress [is] made consistent with International Information Security standards…, the potential for disruption is real and serious and we all pay the price.[31]

David A. Katz *is a partner at Wachtell, Lipton, Rosen & Katz.* **Laura A. McIntosh** *is a consulting attorney for the firm. The views expressed are the authors' and do not necessarily represent the views of the partners of Wachtell, Lipton, Rosen & Katz or the firm as a whole.*

Endnotes:

1. "Cybersecurity" is defined in the relevant SEC guidance as "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access." SEC 2011 CF Disclosure Guidance: Topic No. 2, Cybersecurity, Oct. 13, 2011 (Cybersecurity Release).

2. Corporate Board Member, "Legal Risks on the Radar," 2012 Law and the Boardroom Study, Aug 13, 2012, at 2.

3. Id.

4. See, e.g., Charles Keenan, "The Invisible Threat," Corporate Board Member, May 10, 2012.

5. Corporate Board Member, "Legal Risks on the Radar," 2012 Law and the Boardroom Study, Aug. 13, 2012, at 2.

6. Keenan, supra note 4.

7. Corporate Board Member, "Legal Risks on the Radar," 2012 Law and the Boardroom Study, Aug. 13, 2012, at 2.

8. See Keenan, supra note 4. The Ponemon Institute is a "Michigan-based consulting firm that conducts research on privacy, data protection, and information security." Id.

9. See John Jorgensen, "The Statistics," InfraGard Tampa Bay, Nov. 2, 2012; Jody R. Westby, "How Boards and Senior Executives Are Managing Cyber Risks," Governance of Enterprise Security: CyLab 2012 Report, Carnegie Mellon University CyLab, May 16, 2012, at 11.

10. Cybersecurity Release.

11. Corporate Board Member, "Legal Risks on the Radar," 2012 Law and the Boardroom Study, Aug 13, 2012, at 3.

12. Id.

13. See Westby, supra note 9, at 5.

14. Id. at 16.

15. Id. at 8.

16. Howard A. Schmidt, "Price of Inaction Will Be Onerous," www.nytimes.com/roomfordebate, Oct. 17, 2012 (updated Oct. 18, 2012).

17. "Cybersecurity and the Board," NACD Board Leadership Conference, Oct. 15, 2012, Slide 5.

18. Jamie Reeves, Interview with John Reed Stark, former chief of the SEC's Office of Internet Enforcement, BoardMember.com, Nov. 7, 2011.

19. See "Risk Intelligent Governance in the Age of Cyber Threats," Risk Intelligence Series, No. 23, Deloitte & Touche, 2012, at 3.

20. Some companies are highly vulnerable to damage from cybersecurity breaches because privacy and security may be key elements of their products or services. The recent hacking of Stratfor, a private intelligence firm, has been particularly embarrassing and devastating: WikiLeaks has begun to publish large numbers of emails relating to sensitive projects being undertaken by Stratfor on behalf of its private clients. Companies whose very business model depends upon cyber integrity should prioritize cybersecurity accordingly.

21. See Keenan, supra note 4.

22. See Westby, supra, at 6.

23. Cybersecurity Release.

24. Id.

25. Id.

26. Amazon.com Inc. and Google Inc., for example, were asked by the SEC in 2012 to disclose recent cyberattacks in their upcoming reports. Amazon.com asserted that the cyberattack experienced by its subsidiary Zappos.com was not material and therefore not covered by the Cybersecurity Release; nonetheless, Amazon.com agreed to revise the risk factors disclosure in its 2011 Form 10-K to contain a reference to the security breach at Zappos.com. See Letter to William H. Thompson, Accounting Branch Chief, Div. Corp. Fin., U.S. SEC, from Shelley Reynolds, VP, Worldwide Controller and Principal Accounting Officer, Amazon.com Inc., May 3, 2012. Similarly, Google Inc. was asked by the SEC in May to revise its risk factors disclosure in its next Form 10-Q to include a statement that it had, in the past, experienced cyber attacks. The SEC noted that in 2010, Google Inc. had filed a Current Report on Form 8-K to disclose that it had been the subject of a cyber attack. See Letter to Barbara C. Jacobs and Maryse Mills-Apenteng, Div. Corp. Fin., U.S. SEC, from David J. Segre, Wilson Sonsini Goodrich & Rosati, on behalf of Google Inc., May 4, 2012.

27. "Corporate Attorneys, Directors Call Cybersecurity Top Issue for Business," FloridaTechOnline.com, Oct. 16, 2012.

28. See Jennifer Martinez, "Rockefeller Calls on Obama To Issue Cybersecurity Executive Order," TheHill.com, Aug. 13, 2012.

29. See ISO 38500, described as "the international standard for corporate governance of information technology." Westby, supra, at 12.

30. See Westby, supra note 9, at 11-12. With respect to corporate liability, the United States has ratified the Council of Europe Convention on Cybercrime, which "holds companies civilly, administratively, or criminally liable for cybercrimes that benefit the company and were made possible due to the lack of supervision or control by someone in a senior management position, such as an officer or director." Id. at 12.

31. Schmidt, supra note 16.