WACHTELL, LIPTON, ROSEN & KATZ

The attached article, Corporate Governance Update: The Risky Business of Cybersecurity, was published in the New York Law Journal on October 30, 2014

October 30, 2014

Corporate Governance Update: The Risky Business of Cybersecurity

David A. Katz
and
Laura A. McIntosh*

> *The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.*[1]

In today's technology driven environment, public companies must constantly confront the challenge of cybersecurity, in its complex, varied, and ever-adapting forms. Cybersecurity breaches regularly fill the headlines,[2] the costs of cybercrime are skyrocketing,[3] and the repercussions of corporate cyber-attacks are felt all the way from chief executives to retail customers. President Barack Obama has stated that "the private sector and the government can, and should, work together to meet this

---

* 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.

[1] National Institute for Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0," Feb. 12, 2014, available at www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[2] *See, e.g.*, "Cybersecurity: A Special Report," Wash. Post, Oct. 8, 2014, available at www.washingtonpost.com/sf/post-live/collection/cybersecurity-special-report/. Just this week, it was disclosed that the White House's unclassified network recently had been hacked, supposedly by Russian hackers. Ellen Nakashima, "Hackers breach some White House computers," Wash. Post, Oct. 28, 2014, available at www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html?hpid=z2.

[3] *See, e.g.*, Remarks by SEC Commissioner Luis A. Aguilar, "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," June 10, 2014 ("According to one 2013 survey, the average annualized cost of cyber-crime to a sample of U.S. companies was $11.6 million per year, representing a 78% increase since 2009." (citation omitted)) ("Aguilar Speech, June 10, 2014"), available at www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VEUaY_ldWvg.

shared challenge,"[4] while FBI Director Robert S. Mueller has described "the critical role the private sector must play in cyber security."[5] As companies become increasingly dependent on networked technology, and as an expanding number of people conduct transactions and other activities online, cybersecurity will continue to grow in importance for the business community, for the global economy, and for society at large.

Pressure for boards to establish and maintain high standards for the management of cyber-risk comes not only from government officials, regulators, and shareholders but also from plaintiffs' lawyers, as expanding class action litigation in this area is an unfortunate repercussion of increasing cybercrime. Recent regulatory initiatives and the adoption of the National Institute of Standards and Technology (NIST) Framework earlier this year[6] offer guidance for boards of directors as they work to understand and oversee the myriad aspects of corporate cybersecurity.

Recent Developments

Regulatory authorities in the United States have signaled their intention to protect the public interest in corporate cybersecurity and to take steps to encourage and enhance cyber preparedness in the business community.[7] Earlier this year, Commissioner Luis A. Aguilar of the Securities and Exchange Commission (SEC) emphasized the Commission's sense of urgency around cybersecurity issues: "The capital markets and their critical participants, including public companies, are under a continuous and serious threat of cyber-attack, and this threat cannot be ignored."[8]

The SEC's increased focus on cybersecurity efforts began in 2011, when the Commission released disclosure guidance related to cybersecurity issues.[9] Since

---

[4] Statement by the President on the Cybersecurity Framework, Feb. 12, 2014, available at www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework.

[5] Remarks by Robert S. Mueller, III, Director, Federal Bureau of Investigation, Aug. 8, 2013, available at www.fbi.gov/news/speeches/the-future-of-cyber-security-from-the-fbis-perspective.

[6] *See* National Institute for Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," *supra*.

[7] For a list of federal regulations related to cybersecurity, see Paul Ferrillo and David J. Schwartz, "Cyber Security and Cyber Governance: Federal Regulation and Oversight—Today and Tomorrow," Sept. 10, 2014, available at blogs.law.harvard.edu/corpgov/2014/09/10/cyber-security-and-cyber-governance-federal-regulation-and-oversight-today-and-tomorrow/.

[8] *See* Aguilar Speech, June 10, 2014; Public Statement by SEC Commissioner Luis A. Aguilar, "The Commission's Role in Addressing the Growing Cyber-Threat," March 26, 2014, ("Aguilar Public Statement, March 26, 2014") available at www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184#.VEUXBfldWvg.

[9] *See* SEC Division of Corporation Finance, "CF Disclosure Guidance: Topic No. 2: Cybersecurity," Oct. 13, 2011, available at www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

then, the Commission and its staff have been proactive in their efforts to highlight the importance of cybersecurity to market participants and the integrity of the capital markets, even hosting a roundtable in March 2014 that was focused entirely on cybersecurity topics. In April 2014, the SEC's Office of Compliance, Inspections and Examinations (OCIE) announced a cybersecurity initiative in which it is reviewing the cybersecurity preparedness of dozens of registered broker-dealers and investment advisors.[10] These companies are required to respond to an extensive questionnaire regarding their cybersecurity risk management and any cyber breaches. The Financial Industry Regulatory Authority (FINRA) announced a similar initiative in January 2014 for companies under its authority.[11]

In his speech in June, Commissioner Aguilar urged boards of directors to focus on oversight of cybersecurity issues. He referred directors to the NIST Framework for Improving Critical Infrastructure Cybersecurity, generally known as the "NIST Framework," which was released in February 2014 to provide companies with standards and best practices for managing cyber-risks.[12] The NIST Framework establishes a common vocabulary for discussions between businesspeople and technical specialists, and it offers a tiered approach to developing and refining cybersecurity programs.[13] Aguilar opined that "[a]t a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines—and whether more may be needed."[14]

The questions asked and issues highlighted by the initiatives of the OCIE and FINRA are valuable resources for directors and senior management to use when considering the key issues in cybersecurity. Likewise, the NIST Framework may be very useful to companies and boards, and directors should consider carefully Aguilar's advice of using the NIST Framework as a benchmark. It would be a good practice for the management team to brief the board on the NIST Framework and, if appropriate, have a specific discussion as to whether the company should use it for benchmarking and document the reasons for management's recommendation and the board's decision.

---

[10] *See* SEC National Exam Program Risk Alert, "OCIE Cybersecurity Initiative," Apr. 15, 2014, available at http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

[11] *See* FINRA, "Targeted Examination Letters—Re: Cybersecurity," Jan. 2014, available at http://www.finra.org/industry/regulation/guidance/targetedexaminationletters/p443219.

[12] *See* Aguilar Speech, June 10, 2014.; National Institute for Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," *supra.*

[13] *See* Paul A. Ferrillo, "Understanding and Implementing the NIST Cybersecurity Framework," Aug. 25, 2014, available at http://blogs.law.harvard.edu/corpgov/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/; Holly J. Gregory, "White House Releases NIST Cybersecurity Framework," Feb. 23, 2014, available at http://blogs.law.harvard.edu/corpgov/2014/02/23/white-house-releases-nist-cybersecurity-framework/.

[14] Aguilar Speech, June 10, 2014.

Though intended to be voluntary and advisory, the NIST Framework could effectively become an informal baseline for industry standards and best practices that may be used by plaintiffs' lawyers, insurers, and regulators to assess the adequacy of corporate policies and risk management.[15] While it is highly unlikely that these standards would in any way diminish or complicate the business judgment rule as the legal standard for review of directors' decisions, the costs of (even non-meritorious) class action litigation attracted by cybersecurity lapses—particularly those that might have been prevented by adherence to the standards of the NIST Framework—should not be taken lightly.

Board Oversight Responsibility

Boards of directors are finding themselves not only faced with the mounting challenges of cybersecurity, but also—perhaps uncomfortably—in the spotlight. Commissioner Aguilar recently observed that "[e]ffective board oversight of management's efforts to address these issues is critical to preventing and effectively responding to successful cyber-attacks and, ultimately, to protecting companies and their consumers, as well as protecting investors and the integrity of the capital markets."[16] Fortunately for directors, in addition to the regulatory resources mentioned above, useful guidance in this area has proliferated as concern over cybersecurity has gained momentum.[17] For the most part, this guidance provides directors with an arsenal of questions to ask themselves, their advisors, and senior management, along with the assurance that there are no perfect answers for any situation.[18]

---

[15] *See id*.

[16] *Id.*

[17] *See, e.g.*, "Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition," 2014, by the National Association of Corporate Directors, in collaboration with AIG and Internet Security Alliance, available at www.directorscenter.com/cyber-risk-oversight-nacd-directors-handbook-series/; "Cyber Security: What the Board of Directors Needs To Ask," 2014, by The IIA Research Foundation, in partnership with ISACA, available at www.theiia.org/bookstore/product/cyber-security-what-the-board-of-directors-needs-to-ask-download-pdf-1852.cfm; Dana Post, "Cybersecurity in the Boardroom: The New Reality for Directors," Privacy Advisor, May 27, 2014, available at privacyassociation.org/news/a/cybersecurity-in-the-boardroom-the-new-reality-for-directors/; Deloitte Insights, "The Board's Role in Overseeing Cybersecurity Risk," WSJ Risk & Compliance J., Oct. 10, 2013, available at deloitte.wsj.com/riskandcompliance/2013/10/10/the-boards-role-in-overseeing-cybersecurity-risk/; *see also* David A. Katz and Laura A. McIntosh, "Cybersecurity Risks and the Board of Directors," NYLJ, Nov. 29, 2012.

[18] *See, e.g.*, Paul A. Ferrillo et al., "Cloud Cyber Security: What Every Director Needs To Know," Aug. 6, 2014, available at blogs.law.harvard.edu/corpgov/2014/08/06/cloud-cyber-security-what-every-director-needs-to-know/; *see also* Ellen Messmer, "Homeland Security wants corporate board of directors more involved in cyber-security," networkworld.com, July 29,2014, available at www.networkworld.com/article/2458975/security0/homeland-security-wants-corporate-board-of-directors-more-involved-in-cyber-security.html.

The board's oversight of cybersecurity has two critical components: risk management and crisis management. In the risk management category, boards should view cyber-risk not as a technology issue, but as a component of enterprise risk generally. Though cyber-risk has some unique features, boards need not be intimidated by the technical aspects of cybersecurity but instead should address cybersecurity issues in the context of their broad oversight responsibility. A key component of risk management in this area is ensuring that the company has high-level personnel fully engaged and tasked with cybersecurity who report to senior management and, if appropriate, to the board.[19] Another issue that should be considered by management and boards is whether the company should purchase stand-alone cyber insurance to cover or mitigate the costs of a cyber-attack and its consequences.[20]

Whether or not a specific board committee is tasked with the responsibility for cyber risk oversight, it is important that the entire board remain informed and engaged on cyber-risk issues. A recent survey found that 58 percent of board members surveyed felt they should be actively involved in cybersecurity preparedness. Surveying the same directors, only 14 percent said they were actively involved in cybersecurity preparedness, although 65 percent said that the perception of the risk their companies faced had increased in the last year or two.[21]

Directors should be up-to-date not only with respect to cybersecurity generally, but specifically as to trends in the company's own cyber incidents. Director education is one of the central challenges for boards in this area. For various reasons, directors often feel that they lack the expertise necessary to fully grasp the challenges of cybersecurity; education thus is a key component of effective oversight.[22] One increasingly popular option is for boards to bring in technical consultants on an annual or as-needed basis to apprise directors of current developments in cybersecurity and to engage with the management team as to how the entity measures up. While by no means essential, an outside consultant can provide a valuable perspective that may enhance directors' ability to evaluate the sufficiency of their internal personnel and processes in anticipating, preventing, detecting, and responding to cyber-attacks. Outside consultants are also available to audit a company's cybersecurity practices. Whether or not they hire

---

[19] *See* Aguilar Speech, June 10, 2014.

[20] For a detailed discussion of cyber insurance, see Paul A. Ferrillo, "Cyber Governance: What Every Public Company Director Needs To Know," June 5, 2014, available at blogs.law.harvard.edu/corpgov/2014/06/05/cyber-governance-what-every-director-needs-to-know/.

[21] David F. Carr, "Cybersecurity: How Involved Should Boards Of Directors Be?" Information Week available at www.informationweek.com/government/cybersecurity/cybersecurity-how-involved-should-boards-of-directors-be/d/d-id/1298127.

[22] *See* PWC, "Directors and IT—What Works Best: Abridged Version," Oct. 2012, available at www.pwc.com/us/en/corporate-governance/publications/directors-and-it/directors-and-it-abridged-report.jhtml.

a consultant, directors should be wary of relying too heavily for information and a technical education on the corporate employees whose overall effectiveness they are evaluating.[23]

On the crisis management side, directors should educate themselves as to the potential consequences of various types of cybersecurity breaches. Each company is likely to have its own specific set of vulnerabilities. Directors may not fully understand the range of possible repercussions without a comprehensive review of the company's vulnerabilities and the ways that their exploitation can damage the enterprise and its participants. For example, many enterprises now use cloud technology, which can be highly valuable to a business and, without the proper safeguards, also extremely risky from a cybersecurity perspective. In a recent survey, over a third of companies that have moved to cloud technology said that they had not done anything to mitigate the legal, regulatory, and compliance risks of doing so.[24] Companies thus need to consider their vulnerability not only to cyber-attacks on their own systems but also the impact of cybersecurity breaches on third party vendors on whom the company relies for specific parts of its business.

The board should seek to ensure that the company has a comprehensive and stress-tested plan in place to respond to cyber-attacks of varying kind and degree. Time is always of the essence in dealing with cyber-crime, and advance preparation therefore is crucial to an effective response. Once an incident is identified and understood, the board's priorities must be to minimize disruption of business and damage to reputation, mitigate potential harm to customers and employees, and eliminate any additional vulnerabilities created or exposed by the attack. While these efforts will be led by the company's management on a day-to-day basis, it is important that management keep the board fully apprised and for the board to oversee the communication of a clear and forthright public message about the attack and the company's response.

In addition to litigation, directors may face scrutiny from the proxy advisory services if the company suffers a cyber-attack. Earlier this year, Institutional Shareholder Services (ISS) recommended that Target shareholders vote against all seven of the directors that were on the board at the time of a significant data breach near the end of 2013.[25] ISS asserted that the board's "failure … to ensure appropriate management of these risks set the stage for the data breach, which has resulted in significant losses to the

---

[23] *See* Aguilar Speech, June 10, 2014.

[24] *See* E&Y, "Cybersecurity: Considerations for the Audit Committee," 2013, available at www.ey.com/US/en/Issues/Governance-and-reporting/Audit-Committee/Cybersecurity---Considerations-for-the-audit-committee.

[25] *See* Paul Ziobro and Joann S. Lublin, "ISS's View on Target Directors Is a Signal on Cybersecurity," WSJ.com, May 28, 2014, available at online.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278.

company and its shareholders."[26] Notably, proxy advisor Glass, Lewis & Co. recommended in favor of the Target board and the shareholders evidently agreed with Glass, Lewis; all seven of the directors pinpointed by ISS were reelected to the board.

High Stakes of Cyber-Attacks

Cybersecurity is a dynamic challenge, and proactive behavior is likely to serve boards and management teams well. Companies must constantly update their security protocols to meet the new challenges that are continuing to evolve. Likewise, boards should be updated on a regular basis so that they understand how the cyber-risks the company faces are changing as well as the mitigation plan being pursued by management to combat these developments. A top government official, an expert in the field of cybersecurity, recently commented:

> I do not ascribe to a school of pessimism, and by that, I don't mean to belittle the magnitude of the threat, both in terms of its gravity and its frequency of occurrence. I think everyone understands that cybersecurity is a field of growth. With respect to the security of the government, and with respect to the security of the private sector, I would take the alarm not as necessarily a cause for concern, but rather as a call to action. While attackers are, in fact, becoming more and more sophisticated, our prevention capabilities are growing in sophistication, our detection capabilities are growing in sophistication, our response and remediation capabilities are escalating as well.[27]

The repercussions of a cyber-attack and significant data breach may include, in addition to controversy over director elections, a decline in profits and transactions, significant response costs, negative press, pressure on management, and a proliferation of shareholder suits against the company. Other negative consequences of a corporate cyber-attack can include loss of trade secrets, prototypes, or proprietary processes, disruption of business, theft of funds, widespread consumer identity theft, invasion of employee or customer privacy, and permanent damage to or destruction of corporate databases or IT systems. Each company is likely to have unique vulnerabilities, and each cyber-attacker may have different goals.

---

[26] *Id*.

[27] Washington Post Live, "What Top Government and Business Officials Are Saying About Cybersecurity," Wash. Post, Oct. 7, 2014 (quoting Alejandro Mayorkas, Deputy Secretary, Department of Homeland Security), available at www.washingtonpost.com/postlive/what-top-government-and-business-officials-are-saying-about-cybersecurity/2014/10/07/a6e5142e-4e70-11e4-8c24-487e92bc997b_story.html?asdfsdafsa.

The bottom line is that the costs of cybersecurity will continue to rise. According to a 2013 analysis, cybercrime may already be costing the U.S. economy as much as $100 billion annually.[28] Earlier this month, Jamie Dimon of J.P Morgan Chase & Co. estimated that the bank would double its spending on cybersecurity—an estimated $250 million in 2014—over the next four to five years.[29] Dimon's comments reflected last summer's cyber-attack on J.P Morgan Chase, which resulted in a data breach affecting 76 million households and seven million small businesses. Recent reports trace the sophisticated J.P. Morgan Chase cyber-attack back to Russia. It is clear that both Russia and China are using very sophisticated technology to infiltrate both businesses and government computers, although it is difficult to pinpoint whether these are criminal enterprises or state-sponsored.[30]

The United Nations estimates that, by the end of 2014, three billion people will be online.[31] There can be no doubt that, as Commissioner Aguilar observed in March, "the constant threat of cyber-attack is real, lasting, and cannot be ignored."[32] Corporate vulnerability is significant, and boards of directors face the daunting task of overseeing the management of corporate cyber-risk. It bears emphasis that cybersecurity is, in the final analysis, no different from a liability perspective than any other topic on a board of directors' agenda. The business judgment rule continues to apply, and directors who proactively address cybersecurity issues in good faith and with diligence and care can be confident that their decisions will receive the traditional protection in Delaware. Armed with sound advice, fortified by an education on the issues, and guided by their own good judgment, directors can and should be well-equipped to manage cyber-risk, just as they manage the other business risks inherent in a successful enterprise.

---

[28] *See* Center for Strategic and International Studies, "The Economic Impact of Cyber Crime and Cyber Espionage," July 2013, at 7, available at csis.org/publication/economic-impact-cybercrime-and-cyber-espionage.

[29] Emily Glazer, "J.P Morgan CEO: Cybersecurity Spending To Double," WSJ.com, Oct. 10, 2014, available at online.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976.

[30] Danny Yadron and Siobhan Gorman, "Hacking Trail Leads to Russia, Experts Say," WSJ.com, Oct. 28, 2014 ("China, the object of recent U.S. allegations of cyberspying, may hack more often, U.S. officials and researchers say. But Russia hacks better."), available at online.wsj.com/articles/hacking-trail-leads-to-russia-experts-say-1414468869?KEYWORDS=russian+hackers.

[31] *See, e.g.*, Mary Jordan, "Cyber Attackers Have the Upper Hand," Wash. Post, Oct. 8, 2014, available at washingtonpost.com/postlive/cyber-attackers-have-upper-hand/2014/10/07/c6482ece-4e29-11e4-babe-e91da079cb8a_story.html.

[32] Aguilar Public Statement, March 26, 2014.