Bloomberg BNA

BNA's Banking Report™

CYBERSECURITY

The Board of Directors and Cybersecurity: Setting up the Right Structure




BY ELIZABETH E. MCGINN, THOMAS A. SPORKIN, ALEXANDER D. LUTCH AND JAMES T. SHREVE

Security breaches have become a staple of the daily news. A national restaurant chain announced in August 2014, that a payment card processing system breach involved 33 restaurants in 18 states and that the incident lasted nearly six months.[1] In December 2013 and January 2014, three major retailers acknowledged cyber-attacks affecting over 70 million customers; in October 2013, a major software company acknowledged that hackers had accessed customer names and card information for up to 2.9 million customers;[2] and in May 2013, a daily-deal company announced that information about more than 50 million users may have been accessed in a cyber-attack.[3] Hackers brought down a major bank's website in March 2013,[4] and a month earlier, a social media platform announced that hackers had accessed the personal information of as many as 250,000 users.[5] These are just a few examples of recent cyber-attacks against major corporations. Se-

[1] Michael Calia, *P.F. Chang's Says Data Breach Affected 33 Locations*, Wall Street Journal (Aug. 4, 2014, 9:32 AM), (password protected) http://online.wsj.com/articles/p-f-changs-says-data-breach-affected-33-locations-1407159131; P.F. Chang's Security Compromise Update (Aug. 4, 2014), http://www.pfchangs.com/security/.

Elizabeth E. McGinn and Thomas A. Sporkin are Partners and James T. Shreve and Alexander D. Lutch are Associates at BuckleySandler LLP. They advise financial institutions on regulatory compliance and represent them in litigation and investigations involving privacy and cybersecurity, securities laws, fair lending, financial fraud, and False Claims Act, FIRREA, and white-collar criminal matters.

[2] Alex Konrad, *After Security Breach Exposes 2.9 Million Adobe Users, How Safe is Encrypted Credit Card Data*, Forbes (Oct. 9, 2013, 12:57 PM), http://www.forbes.com/sites/alexkonrad/2013/10/09/how-safe-is-encrypted-card-data-adobe.

[3] Katie W. Johnson, *Living Social Reveals Cyber-Attack, Notifies 50 Million, Says No Credit Data Breached*, Bloomberg BNA (May 6, 2013), http://www.bna.com/livingsocial-reveals-cyberattack-n17179873787/ .

[4] Brian Browdie, *JPMorgan Chase Suffers Online Banking Outage, Confirms Cyberattack*, American Banker (Mar. 12, 2013, 6:22 PM), http://www.americanbanker.com/issues/178_49/jpmorgan-chase-suffers-online-banking-outage-1057455-1.html.

[5] Nicole Pelroth, *Twitter Hacked: Data for 250,000 Users May be Stolen*, New York Times Bits Blog (Feb. 1, 2013, 7:49

 ISSN 0891-0634

curity experts now claim that data breaches and cyber-attacks are not a matter of ''whether,'' but of ''when.'' Such attacks cause major headaches for targeted companies, lead to declines in enterprise value, and create significant liability.

As security breaches proliferate, their consequences are becoming increasingly severe.[6] However, a 2012 report by the Carnegie Mellon CyLab, RSA, and Forbes exposes the generally hands-off approach of many corporate boards of directors where cyber threats are concerned.[7] That report found that ''boards still are not undertaking key oversight activities related to cyber risks.''[8] Cybersecurity is a highly technical area and not a revenue-generating expenditure, but rather a cost-saving one. Nevertheless, a successful cyber-attack can lead to a drop in share price, regulatory action, negative publicity, and possibly personal liability for board members. As Securities and Exchange (''SEC'') Commissioner Luis A. Aguilar explained in June 2014 remarks to the New York Stock Exchange (''NYSE''), ''ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities.''[9] However, only 31 percent of those surveyed for the CyLab report stated that their boards regularly reviewed reports of security breaches.[10]

However, a 2012 report by the Carnegie Mellon CyLab, RSA, and Forbes exposes the generally hands-off approach of many corporate boards of directors where cyber threats are concerned.

A 2013 study of American data breach incidents by the Ponemon Institute and Symantec found that the average data breach cost an organization $5.4 million, or $188 per record compromised.[11] That study also found that if an organization implemented a formal incident response plan prior to an incident, the average cost of a data breach decreased by as much as $42 per compromised record. Moreover, the appointment of a Chief Information Security Officer (''CISO'') saved $23 per record.[12] Another Ponemon Institute study, with HP Enterprise Security Products, released in October 2013 states that the average annualized cyberattack cost to surveyed U.S. companies was $11.56 million, a 78 percent increase over four years, but that ''[d]eployment of enterprise security governance practices including investing in adequate resources, appointing a high-level security leader, and employing certified or expert staff can reduce cybercrime costs and enable organizations to save an estimated average of $1.5 million per year.''[13]

This article presents several action items for boards seeking to prepare themselves and their companies for the increasing external scrutiny on cybersecurity and hoping to minimize the costs of security breaches.

I. Stay Informed and Prepared

Because investments in cybersecurity do not generate revenue, they can be a hard sell. At the same time, such investments generally lead to significant cost savings and can help a company avoid the reputational damage associated with a successful attack. In addition to devoting attention to reports on security efforts and any breaches that occur, there are concrete steps the board can take to promote an effective corporate cybersecurity structure.

a. Hire a Knowledgeable Cybersecurity Expert With Good Communication Skills

The board needs someone in management who is both knowledgeable about cybersecurity and able to explain highly technical concepts in straightforward terms. The board should take an active role in hiring for management positions that impact cybersecurity efforts. When hiring a CISO or Chief Technology Officer (''CTO''), the board should evaluate candidates not only on their ability to deal with technical issues, but also on their ability to communicate effectively. The board should also consider cybersecurity experience when evaluating candidates for positions such as Chief Risk Officer (''CRO''). The CISO or CTO should understand cybersecurity threats generally, and also those particular to the company's industry and to the company itself.

b. Allocate Adequate Resources

One key to successful preparedness is allocating sufficient resources. According to the October 2013 Ponemon study, the two most significant barriers identified by IT and risk professionals to ''achieving effective risk-based security management activities'' within their organizations were (1) lack of skilled or expert personnel and (2) insufficient resources or budget.[14] Without sufficient resources—both financial and human capital—a company cannot keep up with threats and

PM), http://bits.blogs.nytimes.com/2013/02/01/twitter-hacked-data-for-250000-users-stolen/.

[6] Brian Browdie, *Cyberattacks Could Disable Banking System, Hagel Says*, American Banker (May 31, 2013, 5:06 PM) http://www.americanbanker.com/issues/178_105/cyberattacks-could-disable-banking-system-hagel-says-1059532-1.html (''You know, [cyber] attacks can paralyze an electric grid, a banking system, knock out computers on ships or weapons systems, and you never fire a shot,' [Defense Secretary Chuck] Hagel told troops in Honolulu.'').

[7] Jody R. Westby, *Governance of Enterprise Security: CyLab 2012 Report* (May 16, 2012), http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf.

[8] *Id.* at 5.

[9] Luis A. Aguilar, Commissioner, Sec. and Exch. Comm., Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014), http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

[10] *Id at 16.*

[11] *2013 Cost of Data Breach Study: United States*, Ponemon Institute, 1 (May 2013), https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf.

[12] *Id.* at 2.

[13] Press Release, Hewlett Packard, HP Reveals Cost of Cybercrime Escalates 78 percent, Time to Resolve Attacks More Than Doubles (Oct. 8, 2013), http://www8.hp.com/us/en/hp-news/press-release.html?id=1501128#.UlRYqj-OM40.

[14] *The State of Risk-Based Security Management2013*, Ponemon Institute LLC, 45 (released Sept. 5, 2013), *http://www.tripwire.com/linkservid/C46831EC-06FB-78EA-2605C857D1AF201A/showMeta/0/?dl=C4FEDC6D-CA1F-B5BC-8816561E822ACABE*.

  BBR ISSN 0891-0634

stay prepared. The CyLab Report found that 53% of respondents stated that their boards rarely or never reviewed and approved budgets for privacy and IT security programs.[15] Effective cybersecurity can be expensive, given the constantly evolving nature of cyber threats. A recent study suggested that to repel 95% of cyber-attacks, organizations would have to increase spending from a current combined level of $5.3 billion to $46.6 billion, and that even to stop 84 percent of attacks would require around $10 billion.[16]

c. Stay Informed

Boards should receive updates from the CISO or CTO on the steps being taken to protect against cyber threats, risks to which the company is exposed, and serious incidents that occur. These updates should be meaningful and based on established guidelines for determining whether a risk or incident requires an update to the board. To take an example from the data security context, employees may occasionally send emails to the wrong address inadvertently, posing a risk that sensitive information may be comprised. This type of incident happens frequently enough, and the response to such an incident is standardized enough, that there is no need, absent additional risk factors, to update the board each time such an incident occurs. At the same time, the board should be updated about a data breach that potentially involves thousands of customers' sensitive information and should be aware of the steps the company is taking to address such a breach.

d. Consider Hiring Outside Resources as Necessary

There may be situations where it is helpful to have an outside party involved to help with the communication between the board and the CISO or CTO. Someone with significant experience in addressing cyber risks and incidents and the requirements on companies and their boards, such as outside counsel or a consulting firm, can serve as a translator and help bridge the gap between the board and those in charge of protecting the company against cyber-attacks and resolving issues that arise. The outside counsel or consultant can also review policies and procedures, training and other materials in place in order to make recommendations based on the company's risk profile to meet industry best practices and regulatory expectations. In addition to the value as a proactive step, such a review can also help to protect the company and its board in the finger pointing that often occurs in the aftermath of a security breach.

e. Understand Your Company's Risk Factors

The board should ask the right questions. Companies in different industries have different risk profiles depending on the types of information they maintain. The board must understand the company's particular risk profile and be aware of which corporate assets are vulnerable to a cyber-attack. A recent report found that 22 percent of Chief Information Officers (''CIOs'') and CTOs did not know how monetary losses from cybersecurity events within their companies had changed in the past twelve months.[17] The board should ask for this kind of information in part to ensure that this type of information is tracked and readily available. Additionally, the board should review case studies to understand potential outcomes in the event of a successful attack and ways that the damage caused by such an attack can be minimized before the attack occurs.

In particular, individual liability for cyber-attacks can arise through regulatory enforcement actions or shareholder derivative suits.

Once the risk factors are identified and a monitoring and reporting process is in place, the board may consider the necessity and wisdom of recommending cybersecurity liability insurance coverage, or of reserving assets for damages resulting from cyber-attacks. A 2013 Ponemon study reported that with cyber-attacks on the increase, companies are looking to other corporate leaders, including insurers, to help them manage their risk exposure.[18]

II. Cybersecurity Is Serious

Failing to adequately prepare for attacks and address cybersecurity can lead to liability for the company and potentially for individual board members. In particular, individual liability for cyber-attacks can arise through regulatory enforcement actions or shareholder derivative suits.

a. Liability Under Federal Law

The Gramm-Leach-Bliley Act (''GLBA'') requires financial institutions to safeguard consumers' personal information. GLBA defines ''financial institutions'' to include businesses that are ''significantly engaged'' in providing financial products or services. The Federal Trade Commission's (''FTC'') Safeguards Rule applies to financial institutions subject to FTC jurisdiction.

The Safeguards Rule requires financial institutions to ''develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards that are appropriate to [the institution's] size and complexity, the nature and scope of [the institution's] activities, and the sensitivity of any customer information at issue.''[19] The Rule applies not only to financial institutions, but also

[15] Jody R. Westby, *How Board & Senior Executives are Managing Cyber Risks*, Governance of Enterprise Security: Cylab 2012 Report, (released May 16, 2012), http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf.

[16] Valentina Pasquali, *The Untold Cost of Cybersecurity*, Global Finance (May 2, 2013) (citing a 2012 Ponemon Institute study), http://www.gfmag.com/archives/175-may-2013/12482-cover-growing-threat-the-untold-costs-of-cybersecurity.html#axzz2Ypqa99Ad.

[17] *Key Findings from the 2013 U.S. State of Cybercrime Survey*, PricewaterhouseCoopers LLP, 4 (June 2013), http://www.pwc.com/cybersecurity.

[18] *2013 Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*, Ponemon Institute, (August 2013), http://assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf.

[19] Federal Trade Commission, *Standards for Safeguarding Customer Information*; *Final Rule*, FTC, 16 CFR Part 314.3(a) (2002), http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/standards-safeguarding-customer.

to their vendors, since financial institutions must monitor vendors' efforts at safeguarding information.

Failure to comply with the Safeguards Rule can lead to an FTC enforcement action with significant financial and reputational consequences—the FTC lists 26 cases that it has brought under GLBA's privacy and data security provisions.[20] The federal banking regulators have also issued guidance pursuant to GLBA that requires annual reports to the board on a bank's information security program and compliance with the guidance.[21]

b. Liability Under State Law

In addition to federal data security regulation, nearly all states have adopted security breach notification requirements and some states have enacted specific requirements for the safeguarding of personal information. State attorneys general can use these requirements bring enforcement actions against companies that do not adequately protect against cyber-attacks or give required consumer or regulatory notices. Massachusetts, for example, has data security regulations that apply to *anyone* who owns or licenses personal information about a state resident,[22] not just financial institutions. Recent Massachusetts enforcement actions have involved penalties of up to $750,000.[23] Companies must be aware of various (and changing) state laws that impact their cybersecurity efforts and state requirements for board involvement in addressing cybersecurity.

Consideration also must be paid to costs from litigation under the state security breach notice laws. These laws, in effect in all but three states, generally permit the state attorney general, and/or private litigants, to sue an entity failing to meet the requirements of the law and causing damages to state residents. Although lawsuits under breach notice laws have not advanced because of plaintiff inability to demonstrate actual damages, such suits may progress in the future. A ballot initiative filed with the California Secretary of State in 2013 would have significantly increased potential liability for data breaches and amended the California constitution to (1) create a presumption that personally identifying information is confidential when disclosed to a person who collects such information for a commercial or governmental purpose, requiring that person to use ''all reasonably available means to protect it from unauthorized disclosure''; and (2) create a presumption of harm whenever confidential personally identifying information is disclosed without authorization.[24] The ballot initiative was withdrawn, but other legislative attempts to ease proof of damages requirements in lawsuits under security breach laws are likely.

c. Reputational Risk

A cyber-incident can dramatically impact a company's public image. Many companies, including those in the financial services and healthcare industries, obtain sensitive information from customers. A cyber-attack that compromises the security of this information may impair customer confidence and cause customers to change providers. Additionally, a cyber-attack that causes outage of a critical service—e.g., an attack that shuts down access to a bank's online services—may leave customers wary of relying on that service provider in the future. A 2014 study commissioned by Semafone revealed that consumers will avoid doing business with companies that have experienced data breaches, particularly those involving credit cards, email addresses, home addresses and telephone numbers.[25]

Although lawsuits under breach notice laws have not advanced because of plaintiff inability to demonstrate actual damages, such suits may progress in the future.

Reputational damage has real dollar consequences. One study found that brand value declined in the wake of a breach by at least twelve percent, and up to twenty-five percent, ranging in dollar amounts from $184 million to more than $330 million.[26] This kind of reputational damage can have a ripple effect, causing a drop in stock price and eventually even leading to shareholder suits. Estimates of the stock price drop of Target's stock following its security breach announcement ranged from nine to eleven percent in the days following the company's announcement, with estimates of the total cost to Target of about $450 million. The incident also brought about the resignation of the company's CEO and CIO and led Institutional Shareholder Services, to recommend against retaining seven of Target's ten directors.[27] While shareholders voted to retain the Target directors, the results could be different in shareholder votes in the wake of future incidents.

[20] *Legal Resources: BCP Business Center*, Bureau of Consumer Protection Business Center, http://business.ftc.gov/legal-resources/46/35 (last accessed July 9, 2013).

[21] Federal Reserve Board, 12 C.F.R. pt. 225, App. F(III)(F) (2013); Federal Deposit Insurance Corporation,12 C.F.R. pt. 364, App. B(III)(F) (2013); Office of the Comptroller of the Currency 12 C.F.R. pt. 30, App. B(III)(F) (2013).

[22] *Standards for the Protection of Personal Information of Residents of the Commonwealth*, 201 CMR 17.03(1): M.G.L. c. 93H, http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

[23] Press Release, Attorney General Martha Coakley, *South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations* (May 24, 2012), http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breach-settlement.html.

[24] Office of the Attorney General, Ballot Initiative Request – California Personal Privacy Initiative, (August 2, 2013), https://oag.ca.gov/system/files/initiatives/pdfs/13-0008%20%2813-0008A1S%20%28Privacy%29%29.pdf.

[25] Press Release, Semaphone, *86% of customers would shun brands following a data breach* (March 27, 2014), http://op.bna.com/UTILS/lk.nsf/r/wsts9mznv9?opendocument.

[26] Kelly Jackson Higgins, *Study: How Data Breaches Damage Brand Reputation*, Dark Reading, (Oct. 27, 2011, 8:47 PM), http://www.darkreading.com/attacks-breaches/study-how-data-breaches-damage-brand-rep/231901835.

[27] *Target Corporation*, Institutional Shareholder Services, Inc., (May 27, 2014), http://op.bna.com/bar.nsf/r?Open=jtin-9mysp6.

  BBR ISSN 0891-0634

d. Board Member Liability

Board members may also be subject to personal liability for cybersecurity failures. The SEC recently settled an enforcement proceeding against directors of mutual funds for failing to satisfy pricing responsibilities under federal laws.[28] The SEC sought to hold the directors liable for delegating responsibilities to a committee without providing sufficient guidance on how decisions should be made.[29]

Board members also have fiduciary duties to shareholders that often give rise to shareholder derivative suits if a company's stock price falls. While courts typically give deference to board decisions under the ''business judgment rule,'' they are more willing to question the process through which a board makes decisions. Importantly, Delaware courts have suggested that board members can be liable for breaching their fiduciary duties as a result of a failure to implement compliance systems.[30] This is significant given state and federal data security regulations as well as the recent proliferation of standards and guidelines for protecting a company's data and assets from cyber-attacks, all of which provide a means for measuring board actions to prevent cyber-attacks. A successful cyber-attack that causes a drop in a public company's share price may prove an easy basis for a shareholder suit if the attack's success can be attributed to a failure to take generally agreed-upon steps to prevent such attacks, and a board that is not involved in and regularly briefed regarding cybersecurity efforts, will become an easy target for such shareholder suits.

III. Recent Developments Underscore the Importance of Cybersecurity Awareness

The need for board involvement in cybersecurity efforts is also increasing because of recent legislative developments. On April 18, 2013, the House of Representatives passed the Cyber Intelligence Sharing and Protection Act (''CISPA'') to facilitate sharing of information about cyber threats between businesses and the government. Although tabled in the Senate, it provides insight into potential future legislation that may affect how companies share information with the government and each other about cyber security risks.

While courts typically give deference to board decisions under the ''business judgment rule,'' they are more willing to question the process through which a board makes decisions.

Among other provisions, CISPA directs the Director of National Intelligence to establish procedures for the sharing of ''cyber threat intelligence'' by the government with private sector businesses[31] and provides a framework for businesses to share information relating to cyber threats with others, including the federal government.[32] CISPA also provides a broad exemption from liability for businesses that share information pursuant to the Act.[33] If CISPA or a similar law is enacted, boards would need to be involved in determining the extent to which companies share information about cyber threats, both with the federal government and with other companies. While companies generally protect information from competitors, cybersecurity may be an arena with significant benefits to sharing information, and minimal costs. Further, CISPA, or a similar law, may help alleviate concerns that companies' sharing of information will attract antitrust scrutiny to the extent that these laws encourage cyber-threat information sharing.

Even in the absence of a comprehensive federal cybersecurity law, companies must consider the utility and risks of cyber-threat information sharing. Entities such as the U.S. Computer Emergency Response Team or the industry Information Sharing and Analysis Centers permit entities to share and receive information on cybersecurity threats and ways that the threats may be addressed. Such threat sharing may provide valuable information for an organization in discovering and addressing threats, but cybersecurity professionals should inform the board about information provided for threat sharing and the board should consider guidelines for how such cybersecurity threat sharing groups will be used.

Additionally, On February 12, 2013, President Obama issued an Executive Order that directs the Director for the National Institute of Standards and Technology (''NIST'') to develop a framework to reduce cyber risks, particularly to critical infrastructure.[34] Draft versions of the NIST framework were released for comment in August and October and the final version was released in February 2014. The existence of the framework will provide a model for identifying negligence in protecting against cyber threats. Boards of companies designated as ''critical infrastructure'' providers will need to be familiar with the framework in order to avoid regulatory actions. Failure to comply with the framework may result in liability in the event of a successful cyber-attack to the extent that the framework sets forth clear standards for cybersecurity efforts. As SEC Commissioner Aguilar noted, ''while the Framework is voluntary guidance for any company, some commentators have already suggested that it will likely become a baseline for best practices by companies'' and thus boards should assess their companies' compliance with the Framework's guidelines even if they are not legally required to comply with them.[35]

IV. Leveraging Existing Compliance Frameworks

Cybersecurity is but one of a number of issues regarding which the board must remain informed. Bank boards have a leg up in dealing with cybersecurity given their heavily regulated operational environment. For example, most financial institution boards have over-

[28] Press Release, Securities and Exchange Commission, *Former Mutual Fund Directors Agree to Settle Claims That They Failed to Properly Oversee Asset Valuation* (June 13, 2013), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171574878#.UgE29cXgfos.

[29] *Id.*

[30] *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).

[31] H.R. 3523 § 2(a), 112th Cong. (2d Sess. 2013).

[32] *Id.* at § 2(b).

[33] *Id.* at § 2(b)(4).

[34] *Id.* at § 7(a).

[35] Aguilar, *supra* note 8.

sight responsibilities for issues such as Anti-Money Laundering (''AML'') compliance. In the AML context, the board of directors of a bank is responsible for ensuring that the bank ''has a comprehensive and effective BSA/AML compliance program and oversight framework that is reasonably designed to ensure compliance with BSA/AML regulation.''[36] This includes ''ensur[ing] that senior management is fully capable, qualified, and properly motivated to manage the BSA/AML compliance risks arising from the organization's business activities in a manner that is consistent with the board's expectations.''[37] Boards can leverage their experience overseeing AML compliance when preparing for a more involved role in cybersecurity efforts.

The potential costs to an enterprise from cybersecurity threats are significant, and, in the words of SEC Commissioner Aguilar, ''boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril.''[38] However as we have discussed, the potential costs can be mitigated by a well-educated and informed board. By taking steps, including those outlined in this article, boards can ensure the company has an effective structure for addressing cybersecurity risks. While we have attempted to provide general guidelines for approaching cybersecurity, directors should consider engaging outside consultants and ''translators'' who can help them understand the issues and implement appropriate policies and procedures and assist the board in communicating its needs to security professionals. In the current cybersecurity risk climate, the time to take these actions is now.

[36] *FFIEC Bank Secrecy Act Anti-Money Laundering Examination Manual*, Federal Financial Institutions Examination Council, 163 (Apr. 29, 2010), http://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2010.pdf.

[37] *Id.*

[38] Aguilar, *supra* note 8.

  BBR ISSN 0891-0634