The Role of Boards of Directors and CISOs in Overseeing Cyber-Risks

Commissioner Luis A. Aguilar

Security Adviser Alliance Conference
Dallas, TX

September 22, 2016

Thank you for that kind introduction. I am glad to be here and to have the opportunity to speak about cyber-risks and the boardroom, a topic that is both timely and extremely important. Over just a relatively short period of time, cybersecurity has become a top concern of American companies, financial institutions, law enforcement, and many regulators.[1] I suspect that just a handful of years ago, we would have been hard-pressed to find many individuals who had even heard of cybersecurity, let alone known what it meant. Yet, in the past few years, there can be no doubt that the focus on this issue has dramatically increased.[2]

Cybersecurity has become an important topic in both the private and public sectors, and for good reason. Law enforcement and financial regulators have stated publicly that cyber-attacks are becoming both more frequent and more sophisticated.[3] Indeed, hardly a week seems to go by without hearing about a cyber-attack on a government agency or on one of our major corporations.

In addition to becoming more frequent, cyber-attacks have become increasingly costly to companies that are attacked. 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.[4] In addition, the impact of cyber-attacks may extend far beyond the direct costs associated with the immediate response to an attack.[5] Beyond the damage to individuals whose private information is stolen, organizations can experience significant business disruptions, substantial response costs, negative publicity, and lasting reputational harm. In sum, 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.[6]

When I was an SEC Commissioner, I became very concerned about the risks of cyber-attacks, and, as a result, I helped organize the Commission's March 26, 2014 roundtable to discuss the cyber-risks facing public companies and critical market participants like exchanges, broker-dealers, and transfer agents.[7]

I've remained vocal on the issues of cybersecurity. I've spoken at conferences targeted at directors of publicly-traded companies about what boards of directors can, and should, do to ensure that their organizations are appropriately considering and addressing cyber-risks. I've addressed the need for a joint effort by the public and private sectors and I've also focused on the unique challenges facing small and mid-sized businesses and on my own former agency's

responsibilities to implement effective cybersecurity protocols to protect the information the SEC obtains from the entities it oversees, much of it private and confidential.

Today, in speaking at an event sponsored by an organization founded by – and for – chief information security officers (CISO), I would like to focus my remarks on how CISOs and boards can work together to prepare for, respond to and mitigate the impact of a cyberattack.

Board oversight of cybersecurity issues invariably requires that directors rely on management to help them understand the company's cyber-profile – its strengths and weaknesses, and its infrastructure, cultural and technology needs. In particular, boards will need to rely on those on you in this room – their CISOs.

The Role of the Boards of Directors in Overseeing Cyber-Risk Management

Background on the Role of Boards of Directors

The question then is "how can you help the board understand the issues the organization faces in a way that enables the board to ensure that management is developing the right policies and processes?"

When a CISO considers the board's role in addressing cybersecurity issues and how you can help the board, it is useful to keep in mind the broad duties that the board owes to the corporation and, more specifically, the board's role in corporate governance and overseeing risk management. It has long been the accepted model, both here in the U.S. and around the world, that corporations are managed under the direction of their boards of directors.[8] This model arises from a central tenet of the modern corporation — the separation of ownership and control of the corporation. Under this structure, those who manage a corporation must answer to the true owners of the company — the shareholders.

It is neither possible nor desirable, however, for the many, widely-dispersed shareholders of any public company to come together and manage, or direct the management of, that company's business and affairs. As a result, shareholders elect a board of directors to represent their interests, and, in turn, the board of directors, through effective corporate governance, makes sure that management effectively serves the corporation and its shareholders.[9]

Directors - particularly directors of public companies - have very difficult jobs. They have significant oversight responsibilities with respect to executive management and for the overall direction of the company. Directors play a critical role in guarding a company's assets and working to improve its bottom line. Moreover, they are responsible for setting the appropriate tone at the top, shepherding a company's strategic planning, overseeing management's decision-making, setting executive compensation, and countless other responsibilities depending on the company and its industry.

In addition, as part of their overall director responsibilities, they typically sit on at least one board committee with enumerated responsibilities – whether it's the audit committee, the

compensation committee or the nominating and governance committee. And, increasingly, many boards are creating risk committees.

Clearly directors are busy lot. The many specific duties and responsibilities they have are too many to mention today, but as fiduciaries, all of them are clearly aimed at one overarching obligation—and that is to faithfully represent the interests of shareholders.

Moreover, directors are expected to carry out all of their duties and responsibilities with a keen focus and attention to detail — and all on a part-time basis, with directors typically meeting on a quarterly basis for just one, two or three days.

Corporate Boards and Risk Management Generally

And it's not getting easier.

Although boards have long been responsible for overseeing multiple aspects of management's activities, since the financial crisis, there has been an increased focus on what boards of directors are doing to address risk management.[10] Indeed, it's been noted that, leading up to the financial crisis, boards of directors may not have been doing enough to oversee risk management within their companies, and that this failure contributed to the unreasonably risky behavior that resulted in the destruction of untold billions in shareholder value and plunged the country and the global economy into recession.[11] Although primary responsibility for risk management has historically belonged to management, it is increasingly clear that the boards are responsible for overseeing that the corporation has established appropriate risk management programs and for overseeing how management implements those programs.[12]

The importance of board oversight was highlighted when, in 2009, the SEC amended its rules to require public disclosure about, among other things, the board's role in risk oversight, including a description of whether and how the board administers its oversight function, such as through the whole board, a separate risk committee, or the audit committee.[13] The SEC did not mandate any particular structure, but noted that "risk oversight is a key competence of the board" and that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company."[14]

The evidence suggests that boards of directors have begun to assume greater responsibility for overseeing the risk management efforts of their companies.[15] Surveys have shown that many boards are increasingly taking responsibility for the risk oversight of their companies.[16]

Clearly, boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk[17] — and there is little doubt that cyber-risk also must be considered as part of board's overall risk oversight. One catalyst for this is the pressure being asserted by shareholders. For example, after the December 2013 cyber-attack on Target Corporation, a

prominent proxy advisory firm urged the ouster of most of the Target directors because of the perceived "failure…to ensure appropriate management of [the] risks". This type of pressure is another driver that puts directors on notice that they have to proactively address the risks associated with cyber-attacks.[18]

What Boards of Directors Can and Should Be Doing to Oversee Cyber-Risk

In addition to the threat to a director's tenure, there is also the threat of litigation and potential liability for failing to implement adequate steps to protect the company from cyber-threats.[19] Perhaps unsurprisingly, there have been various derivative lawsuits brought against companies and their officers and directors relating to data breaches resulting from cyber-attacks.[20] Thus, boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril.

Moreover, it is also noteworthy that the importance of a board having an understanding of cybersecurity has caught the attention of our lawmakers. In fact, last year, the U. S. Senate introduced the bipartisan Cybersecurity Disclosure Act.[21] This legislation seeks to strengthen and prioritize cybersecurity at publicly-traded companies by requiring them to disclose the extent, if any, of the cybersecurity expertise possessed by their boards of directors.

While it is doubtful that this legislation will be passed in a Presidential-election year, I suspect the idea will not go away. Too many legislators and other observers believe that shining a spotlight on whether a company's board has this critical expertize may encourage companies to be more proactive in understanding their cyber-attack profile and, hopefully, be better prepared for the inevitable attack.

While the Cybersecurity Disclosure Act did not become law, late last year the Congress did pass the "Cybersecurity Information Sharing Act", or CISA.[22] CISA is a complex piece of legislation and there isn't time today for an in-depth discussion of all of its requirements. At its essence, however, CISA encourages and promotes information sharing by broadly defining what is "cybersecurity" and by exempting information about cyber threats and defensive measures that a company shares with the government or other companies from standard disclosure laws, and by providing entities involved in cybersecurity threat analysis, monitoring, defense and information sharing with immunity from liability – if those actions are done in accordance with CISA. CISA can be both a shield and a sword. A sword to help you work with the government and other companies to proactively address cyber-threats and a shield that can prevent lawsuits. I urge CISOs to become familiar with CISA and to work with your legal advisers to know how to avail yourself of its benefits.

Given the known risks posed by cyber-attacks, one would expect that corporate boards and senior management universally would be proactively taking steps to confront these cyber-risks. While a few years ago, boards may have struggled to find guidance, that's no longer the case. Cybersecurity is now a frequent topic discussed at many conferences and there's a growing library of books and articles on the topic.

For those unsure where to start, I would urge them to look at the Framework for Improving Critical Infrastructure Cybersecurity, released by the National Institute of Standards and Technology ("NIST") in February 2014. The NIST Cybersecurity Framework is intended to provide companies with a set of industry standards and best practices for managing their cybersecurity risks.[23] In essence, the Framework encourages companies to be proactive and to think about these difficult issues in advance of the occurrence of a possibly devastating cyber-event. 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, including in assessing legal or regulatory exposure to these issues or for insurance purposes.[24] At a minimum, boards should work with management and, in particular, CISOs to assess their corporate policies to ensure how they match-up to the Framework's guidelines — and whether more may be needed.

Yet, even as to those companies that have cybersecurity risks on their radar screen, evidence suggests that there may be a gap that exists between the magnitude of the exposure presented by cyber-risks and the steps, or lack thereof, that many corporate boards have taken to address these risks. Some have noted that boards are not spending enough time or devoting sufficient corporate resources to addressing cybersecurity issues.[25] According to one survey, boards were not undertaking key oversight activities related to cyber-risks, such as reviewing annual budgets for privacy and IT security programs, assigning roles and responsibilities for privacy and security, and receiving regular reports on breaches and IT risks.[26] In light of these observations, directors should be asking themselves what they can, and should, be doing to effectively oversee cyber-risk management. At companies with CISOs, I suspect that these same questions are being asked of the CISOs.

Board Structural Changes to Focus on Appropriate Cyber-Risk Management

Focus on cybersecurity can be an exercise in futility if there is no one at the company who is able to translate its concepts into action plans. Frequently, the board's risk oversight function lies either with the full board or is delegated to the board's audit committee. Unfortunately, many boards lack the technical expertise necessary to be able to evaluate whether management is taking appropriate steps to address cybersecurity issues. Moreover, the board's audit committee may not have the expertise, support, or skills necessary to add oversight of a company's cyber-risk management to their already full agenda.[27] As a result, some have recommended mandatory cyber-risk education for directors.[28] Others have suggested that boards be at least adequately represented by members with a good understanding of information technology issues that pose risks to the company.[29]

Clearly, there are various mechanisms that boards can employ to close the gap in addressing cybersecurity concerns — but it is equally clear that boards need to be proactive in doing so. Put simply, boards that lack an adequate understanding of cyber-risks are unlikely to be able to effectively oversee cyber-risk management. I suspect that boards with CISOs can greatly benefit from the CISO's regular input as to what mechanism may work best for that particular company. The complexity of the issues makes a "one-size-all" approach ill-advised.

Internal Roles and Responsibilities Focused on Cyber-Risk

In addition to proactive boards, a company must also have the appropriate personnel to carry out effective cyber-risk management and to provide regular reports to the board. Organizations need cyber leaders who can understand the technical issues, while being able to speak the language of business to help the board and other senior management understand the cybersecurity ecosystem. This represents both a challenge and an opportunity for CISOs. Traditionally, CISOs have focused on the technical requirements - such as, the protection of data, networks and systems – but the changing needs now requires that CISOs also fully understand their organization's core business operations and how cyber-threats can impact those operations.

The mere fact that your companies have CISOs is a step forward. A 2012 survey reported that less than two-thirds of responding companies had full-time personnel in key roles responsible for privacy and security, in a manner that was consistent with internationally accepted best practices and standards.[30]

The benefits of having a CISO is illustrated by a 2013 survey that found that the companies that detected more security incidents and reported lower average financial losses per incident shared key attributes, including that they employed a full-time chief information security officer (or equivalent) who reported directly to senior management.[31]

Companies with CISOs need to make sure that their boards interact effectively with CISOs. At a minimum, boards should develop organizational processes to facilitate communication between and among CISOs, senior executives and the board – whether directly or through an appropriate board committee. Ultimately, the board needs to exercise its fiduciary obligation to shareholders by having a clear understanding of who at the company has primary responsibility for cybersecurity risk oversight and for ensuring the adequacy of the company's cyber-risk management practices and resources.[32] As the evidence shows, devoting full-time personnel to cybersecurity issues helps to prevent and mitigate the effects of cyber-attacks.

Company Preparedness

The need for boards to be involved in addressing cybersecurity is undeniable. While, ultimately, boards must rely on management to perform the day-to-day functions, the board should engage with management and, preferably, directly with the CISO, to understand, among other things, the company's vulnerabilities, strategy, devoted technological and human resources, and existing plans for responding to a cyber-event.

Although different companies may choose different paths, depending on their cyber-profile, the goal is the same: to prepare the company for the inevitable cyber-attack and the resulting fallout from such an event. To that end, some of the key questions the board needs to ask are: what are key threats facing the firm; what is being done to mitigate those threats; are there areas that need additional attention and, if so, what are they and what are the plans to address them; and is there sufficient budget and resources available?

Beyond these overarching concerns boards should also be prepared to ask specific questions. For example: Have there been any specific breaches? How many? What was learned? How will they be prevented in the future?

Moreover, in addition to answering any questions the board may have, CISOs need to be prepared to help the boards understand the questions they should be asking. CISOs need to appreciate that directors have a long list of duties to perform, do so on a part-time basis, and most directors may only have passing familiarity with cyber and technology issues. Yet no director wants to fail their shareholder or be sued for failing to do the right thing - and, for that and other reasons, will greatly appreciate any help they can get.

Both boards and CISOs need to appreciate that, in almost all cases, the CISOs will have greater understanding of cyber-issues. A board may not know all the right questions to ask and a CISO that fails to guide them is not helping. CISOs need to be cognizant that boards will need a certain amount of hand holding. CISOs also need to be sensitive to how they deliver information. For example: what level of detail will benefit the board, or a particular board committee? How much to provide in narrative form and how many charts and graphs are useful? Too little information may keep the directors uninformed, while too much could drown them in a sea of minutia that ends up being meaningless. Clearly, a committee focused on cyber issues can benefit from greater detail but, even then, there's much to consider about the nature, breadth and specificity provided.

Ultimately, how information is provided can determine whether board oversight is effective, and CISOs can be instrumental in calibrating how to most effectively and efficiently inform the boards. As time passes, CISO's will likely be a fixture at all companies and at all board meetings – and, for my money, directors, companies, shareholders and the capital markets will be the better for it.

Conclusion

Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities. [33]

Board oversight of cyber-risk management will remain critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues. Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks. In this regard, CISOs will be an invaluable asset to boards.

I commend those companies that have been proactive in dealing with the issue by hiring CISOs. Those that do not have CISOs, are performing a "high wire act" without a net.

Thank you for inviting me to speak to you today.

[1] For example, the Director of the Federal Bureau of Investigation (FBI), James Comey, said last November that "resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats." *See,* Testimony of James B. Comey, Jr., Director, FBI, U.S. Department of Justice, before the Senate Committee on Homeland Security and Governmental Affairs (Nov. 14, 2013), *available at* http://www.hsgac.senate.gov/hearings/threats-to-the-homeland. *See also*, Testimony of Jeh C. Johnson, Secretary, U.S. Department of Homeland Security, before the House Committee on Homeland Security (Feb. 26, 2014) ("DHS must continue efforts to address the growing cyber threat to the private sector and the '.gov' networks, illustrated by the real, pervasive, and ongoing series of attacks on public and private infrastructure."), *available at* http://docs.house.gov/meetings/HM/HM00/20140226/101722/HHRG-113-HM00-Wstate-JohnsonJ-20140226.pdf; Testimony of Ari Baranoff, Assistant Special Agent in Charge, United States Secret Service Criminal Investigative Division, before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies (Apr. 16, 2014), *available at* http://docs.house.gov/meetings/HM/HM08/20140416/102141/HHRG-113-HM08-Wstate-BaranoffA-20140416.pdf ("Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created online marketplaces for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cybercrimes targeting private industry and critical infrastructure."); Remarks by Secretary of Defense Leon E. Panetta to the Business Executives for National Security (Oct. 11, 2012), *available at* http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136 ("As director of the CIA and now Secretary of Defense, I have understood that cyber attacks are every bit as real as the more well-known threats like terrorism, nuclear weapons proliferation and the turmoil that we see in the Middle East. And the cyber threats facing this country are growing.").

[2] *See, e.g.*, Martin Lipton, *et al.*, *Risk Management and the Board of Directors — An Update for 2014*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Apr. 22, 2014), *available at* http://blogs.law.harvard.edu/corpgov/2014/04/22/risk-management-and-the-board-of-directors-an-update-for-2014/ (noting that cybersecurity is a risk management issue that "merits special attention" from the board of directors in 2014); PwC 2012 Annual Corporate Directors Survey, *Insights from the Boardroom 2012: Board evolution: Progress made yet challenges persist*, *available at* http://www.pwc.com/en_US/us/corporate-governance/annual-corporate-directors-survey/assets/pdf/pwc-annual-corporate-directors-survey.pdf (finding that 72% of directors are engaged with overseeing and understanding data security issues and risks related to compromising customer data); Michael A. Gold, *Cyber Risk and the Board of Directors–Closing the Gap*, Bloomberg BNA (Oct. 18, 2013) *available at* http://www.bna.com/cyber-risk-and-the-board-of-directors-closing-the-gap// ("The responsibility of corporate directors to address cyber security is commanding more attention and is obviously a significant issue."); Deloitte Development LLC, *Hot Topics: Cybersecurity … Continued in the boardroom*, Corporate Governance Monthly (Aug. 2013), *available at* http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/USEng/Documents/Deloitte%20Periodicals/Hot%20Topics/Hot%20Topics%20-%20Cybersecurity%20%20%20Continued%20in%20the%20boardroom%20-

August%202013%20-Final.pdf ("Not long ago, the term 'cybersecurity' was not frequently heard or addressed in the boardroom. Cybersecurity was often referred to as an information technology risk, and management and oversight were the responsibility of the chief information or technology officer, not the board. With the rapid advancement of technology, cybersecurity has become an increasingly challenging risk that boards may need to address."); Holly J. Gregory, *Board Oversight of Cybersecurity Risks*, Thomson Reuters Practical Law (Mar. 1, 2014), *available at* http://us.practicallaw.com/5-558-2825 ("The risk of cybersecurity breaches (and the harm that these breaches pose) is one of increasing significance for most companies and therefore an area for heightened board focus.").

[3] For example, on December 9, 2013, the Financial Stability Oversight Council held a meeting to discuss cybersecurity threats to the financial system. *See*, U.S. Department of the Treasury Press Release, "Financial Stability Oversight Council to Meet December 9," *available at* http://www.treasury.gov/press-center/press-releases/Pages/jl2228.aspx. During that meeting, Assistant Treasury Secretary Cyrus-Amir-Mokri said that "[o]ur experience over the last couple of years shows that cyber-threats to financial institutions and markets are growing in both frequency and sophistication." *See*, Remarks of Assistant Secretary Cyrus Amir-Mokri on Cybersecurity at a Meeting of the Financial Stability Oversight Council (Dec. 9, 2013), *available at* http://www.treasury.gov/press-center/press-releases/Pages/jl2234.aspx. In addition, in testimony before the House Financial Services Committee in 2011, the Assistant Director of the FBI's Cyber Division stated that the number and sophistication of malicious incidents involving financial institutions has increased dramatically over the past several years and offered numerous examples of such attacks, which included fraudulent monetary transfers, unauthorized financial transactions from compromised bank and brokerage accounts, denial of service attacks on U.S. stock exchanges, and hacking incidents in which confidential information was misappropriated. *See*, Testimony of Gordon M. Snow, Assistant Director, Cyber Division, FBI, U.S. Department of Justice, before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit (Sept. 14, 2011), *available at* http://financialservices.house.gov/uploadedfiles/091411snow.pdf.

[4] *See*, HP Press Release, *HP Reveals Cost of Cybercrime Escalates 70 Percent, Time to Resolve Attacks More Than Doubles* (Oct. 8, 2013), *available at* http://www8.hp.com/us/en/hp-news/press-release.html?id=1501128.

[5] *See*, Target Financial News Release, *Target Reports Fourth Quarter and Full-Year 2013 Earnings* (Feb. 26, 2014), *available at* http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1903678&highlight (including a statement from then-Chairman, President and CEO Gregg Steinhafel that Target's fourth quarter results "softened meaningfully following our December announcement of a data breach."); Elizabeth A. Harris, *Data Breach Hurts Profit at Target*, N.Y. Times (Feb. 26, 2014), *available at* http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html?_r=0 (noting that "[t]he widespread theft of Target customer data had a significant impact on the company's profit, which fell more than 40 percent in the fourth quarter" of 2013).

[6] I also want to note that at the 2014 Investment Company Institute's ("ICI") general membership meeting the issue of cybersecurity was front and center. Among the issues raised during the meeting was the "huge risk to brand" for a firm if they have a security failure in the event of a cyber-attack. A separate panel at the ICI conference devoted to cybersecurity also discussed the shift in focus from building "hard walls" to protect against risks from outside the company to cybersecurity focused on "inside" risks, such as ensuring that individuals with mobile applications or other types of flexible applications don't introduce, intentionally or unintentionally, malware or other kinds of security breaches that could lead to a cyber-attack on the company. *See, e.g.*, Jackie Noblett, *Cyber Breach a "Huge Risk to Brand,"* Ignites (May 29, 2014), *available at* http://ignites.com/c/897654/86334/cyber_breach_huge_risk_brand?referrer_module=emailMorningNews&module_order=7.

[7] *See* SEC Press Release, *SEC Announces Agenda, Panelists for Cybersecurity Roundtable* (Mar. 24, 2014), *available at* http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541253749; *Cybersecurity Roundtable Webcast* (Mar. 26, 2014), *available at* http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml. In addition, the SEC's National Exam Program included cybersecurity among its areas of focus in its National Examination Priorities for 2014. *See,* SEC's National Exam Priorities for 2014, *available at* http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf. In addition, it was announced that SEC examiners will review whether asset managers have policies to prevent and detect cyber-attacks and are properly safeguarding against security risks that could arise from vendors having access to their systems. *See*, Sarah N. Lynch, *SEC examiners to review how asset managers fend off cyber attacks*, Reuters (Jan. 30, 2014), *available at* http://www.reuters.com/article/2014/01/30/us-sec-cyber-assetmanagers-idUSBREA0T1PJ20140130. FINRA has also identified cybersecurity as one of its examination priorities for 2014. *See,* FINRA's 2014 Regulatory and Examination Priorities Letter (Jan. 2, 2014), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p419710.pdf.

To continue the discussion and to allow the public to weigh in on this important topic, the SEC set up a public comment file associated with the Cybersecurity Roundtable, *available at* http://www.sec.gov/comments/4-673/4-673.shtml.

[8] *See, e.g.*, Model Bus. Corp. Act § 8.01 (2002); Del. Gen. Corp. Law § 141(a).

[9] For additional thoughts on the importance of effective corporate governance, *see* Commissioner Luis A. Aguilar, *Looking at Corporate Governance from the Investor's Perspective*, *available at* http://www.sec.gov/News/Speech/Detail/Speech/1370541547078.

[10] *See, e.g.*, Committee of Sponsoring Organizations of the Treadway Commission, *Effective Enterprise Risk Oversight: The Role of the Board of Directors* (2009), *available at* http://www.coso.org/documents/COSOBoardsERM4pager-

FINALRELEASEVERSION82409_001.pdf ("Clearly, one result of the financial crisis is an increased focus on the effectiveness of board risk oversight practices."); Committee of Sponsoring Organizations of the Treadway Commission, *Board Risk Oversight: A Progress Report — Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities* (Dec. 2010), *available at* http://www.coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf ("Risk oversight is a high priority on the agenda of most boards of directors. Recently, the importance of this responsibility has become more evident in the wake of an historic global financial crisis, which disclosed perceived risk management weaknesses across financial services and other organizations worldwide. Based on numerous legislative and regulatory actions in the United States and other countries as well as initiatives in the private sector, it is clear that expectations for more effective risk oversight are being raised not just for financial services companies, but broadly across all types of businesses."); David A. Katz, *Boards Play A Leading Role in Risk Management Oversight*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Oct. 8, 2009), *available at* http://blogs.law.harvard.edu/corpgov/2009/10/08/boards-play-a-leading-role-in-risk-management-oversight/ ("Just as the Enron and other high-profile corporate scandals were seen as resulting from a lack of ethics and oversight, the credit market meltdown and resulting financial crisis have been blamed in large part on inadequate risk management by corporations and their boards of directors. As a result, along with the task of implementing corporate governance procedures and guidelines, a company's board of directors is expected to take a leading role in overseeing risk management structures and policies.").

[11] Nicola Faith Sharpe, *Informational Autonomy in the Boardroom*, 201 U. Ill. L. Rev. 1089 (2013) ("The financial crisis of 2007-2008 was one of the worst in U.S. history. In a single quarter, the blue chip company Lehman Brothers (who eventually went bankrupt) lost $2.8 billion. While commentators have identified multiple reasons why the crisis occurred, many posit that boards mismanaged risk and failed in their oversight duties, which directly contributed to their firms failing."); Lawrence J. Trautman and Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. Marshall J. Computer & Info. L. 313 (Spring 2011) ("With accusations that boards of directors of financial institutions were asleep at the wheel while their companies engaged in risky behavior that erased millions of dollars of shareholder value and plunged the country into recession, increasing pressure is now being placed on public company boards to shoulder the burden of risk oversight for the companies they serve."); William B. Asher, Jr., Michael T. Gass, Erik Skramstad, and Michele Edwards, *The Role of Board of Directors in Risk Oversight in a Post-Crisis Economy*, Bloomberg Law Reports-Corporate Law Vol. 4, No. 13, *available at* http://www.choate.com/uploads/113/doc/Asher,%20Gass%20-The%20Role%20of%20Board%20of%20Directors%20in%20Risk%20Oversight%20in%20a%20Post-Crisis%20Economy.pdf ("Senior management and corporate directors face renewed criticism surrounding risk management practices and apparent failures in oversight that are considered, at least in part, to be at the root of the recent crisis.").

[12] *See, e.g.*, Stephen M. Bainbridge, *Caremark and Enterprise Risk Management*, 34 Iowa J. Corp. L. 967 (2009) ("Although primary responsibility for risk management rests with the corporation's top management team, the board of directors is responsible for ensuring that the

corporation has established appropriate risk management programs and for overseeing management's implementation of such programs."); Martin Lipton, *Risk Management and the Board of Directors–An Update for 2014*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Apr. 22, 2014), *available at* http://blogs.law.harvard.edu/corpgov/2014/04/22/risk-management-and-the-board-of-directors-an-update-for-2014/ (". . . the board cannot and should not be involved in actual day-to day risk *management*. Directors should instead, through their risk oversight role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite, that these policies and procedures are functioning as directed, and that necessary steps are taken to foster a culture of risk-aware and risk-adjusted decision making throughout the organization. The board should establish that the CEO and the senior executives are fully engaged in risk management and should also be aware of the type and magnitude of the company's principal risks that underlie its risk oversight. Through its oversight role, the board can send a message to management and employees that comprehensive risk management is neither an impediment to the conduct of business nor a mere supplement to a firm's overall compliance program, but is instead an integral component of strategy, culture and business operations.").

[13] *Proxy Disclosure Enhancements*, SEC Rel. No. 33-9089 (Dec. 16, 2009), 74 Fed. Reg. 68334, *available at* http://www.sec.gov/rules/final/2009/33-9089.pdf.

[14] *Id.* That amendment also required disclosure of a company's compensation policies and practices as they relate to a company's risk management in order to help investors identify whether the company has established a system of incentives that could lead to excessive or inappropriate risk taking by its employees.

[15] *Supra* note 11, William B. Asher, Jr. *et al.*, *The Role of Board of Directors in Risk Oversight in a Post-Crisis Economy* ("We know today, however, that risk management has indeed forced its way into the boardroom and that there has been a substantial change in the relationship between the overseers of public companies and their shareholders.").

[16] *Risk Intelligent Proxy Disclosures — 2013: Trending upward*, Deloitte (2013), *available at* http://deloitte.wsj.com/riskandcompliance/files/2014/01/Risk_Intelligent_Proxy_Disclosures_2013.pdf (noting that 91% of the issuers of proxy disclosures noted that "the full board is responsible for risk.").

[17] See, *Proxy Disclosure Enhancements*, *supra* note 13.

[18] Paul Ziobro, *Target Shareholders Should Oust Directors, ISS Says*, Wall St. Journal (May 28, 2014); Bruce Carton, *ISS Recommends Ouster of Seven Target Directors for Data Breach Failures*, ComplianceWeek (May 29, 2014), *available at* http://www.complianceweek.com/iss-recommends-ouster-of-seven-target-directors-for-data-breach-failures/article/348954/?DCMP=EMC-CW-WeekendEdition.

[19] Charles R. Ragan, *Information Governance: It's a Duty and It's Smart Business*, 19 Rich. J.L. & Tech. 12 (2013), *available at* http://jolt.richmond.edu/v19i4/article12.pdf (indicating that "[t]he principles thus enunciated raise the specter of potential liability if officers and directors utterly fail to ensure the adequacy of information systems."); J. Wylie Donald and Jennifer Black Strutt, *Cybersecurity: Moving Toward a Standard of Care for the Board*, Bloomberg BNA (Nov. 4, 2013), *available at* http://www.bna.com/cybersecurity-moving-toward-a-standard-of-care-for-the-board/ (quoting from a Delaware Chancery Court decision stating that directors may be liable if "(a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.").

[20] *See, e.g., Collier v. Steinhafel et al.* (D.C. Minn. Jan. 2014), case number 0:14-cv-00266 (alleging that Target's board and top executives harmed the company financially by failing to take adequate steps to prevent the cyber-attack then by subsequently providing customers with misleading information about the extent of the data theft.); *Dennis Palkon et al. v. Stephen P. Holmes et al*. (D.C.N.J. May 2014), case number 2:14-cv-01234 (alleging that Wyndham's board and top executives harmed the company financially by failing to take adequate steps to safeguard customers' personal and financial information.).

[21] S.B. 2410 (114th Congress (2015-2016)), *available at* https://www.congress.gov/bill/114th-congress/senate-bill/2410/text.

[22] Cybersecurity Information Sharing Act, 6 U.S.C.A. § 1501 – 1510 (West 2015).

[23] The National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014) (the "NIST Cybersecurity Framework"), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, was released in response to President Obama's issued Executive Order 13636, titled "Improving Critical Infrastructure Cybersecuity," dated February 12, 2013. The NIST Cybersecurity Framework sets out five core functions and categories of activities for companies to implement that relate generally to cyber-risk management and oversight, which the NIST helpfully boiled down to five terms: Identify, Protect, Detect, Respond and Recover. This core fundamentally means the following: companies should (i) *identify* known cybersecurity risks to their infrastructure; (ii) develop safeguards to *protect* the delivery and maintenance of infrastructure services; (iii) implement methods to *detect* the occurrence of a cybersecurity event; (iv) develop methods to *respond* to a detected cybersecurity event; and (v) develop plans to *recover* and restore the companies' capabilities that were impaired as a result of a cybersecurity event. *See also,* Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom*, The Metropolitan Corporate Counsel (Mar. 17, 2014), *available at* http://www.sheppardmullin.com/media/article/1280_MCC-Cybersecurity-Breaching%20The%20Boardroom.pdf.

[24] *Supra note* 2, Holly J. Gregory, *Board Oversight of Cybersecurity Risks; supra note* 23, Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom* (stating that "[w]hile

adoption of the Cybersecurity Framework is voluntary, it will likely become a key reference for regulators, insurance companies and the plaintiffs' bar in assessing whether a company took steps reasonably designed to reduce and manage cybersecurity risks.").

[25] Steven P. Blonder, *How closely is the board paying attention to cyber risks?*, Inside Counsel (formerly Corporate Legal Times) (Apr. 9, 2014), *available at* http://www.insidecounsel.com/2014/04/09/how-closely-is-the-board-paying-attention-to-cyber. (Indicating that "[i]n all likelihood, absent an incident, it is likely that board members are not spending sufficient time evaluating or analyzing the risks inherent in new technologies, as well as their related cybersecurity risks.").

[26] Jody R. Westby, *Governance of Enterprise Security: CyLab 2012 Report — How Boards & Senior Executives Are Managing Cyber Risks*, Carnegie Mellon University CyLab (May 16, 2012), at 5. (Hereinafter "CyLab 2012 Report.").

[27] Matteo Tonello, *Should Your Board Have a Separate Risk Committee?*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Feb. 12, 2012), *available at* https://blogs.law.harvard.edu/corpgov/2012/02/12/should-your-board-have-a-separate-risk-committee/ (asking "[d]oes the audit committee have the time, the skills, and the support to do the job, given everything else it is required to do?").

[28] *See, e.g.*, Katie W. Johnson, *Publicly Traded Companies Should Prepare To Disclose Cybersecurity Risks, Incidents*, Bloomberg BNA (Mar. 17, 2014), *available at* http://www.bna.com/publicly-traded-companies-n17179885721/ (citing Mary Ellen Callahan, Chair of the Privacy and Information Governance Practice at Jenner & Block, LLP at the International Association of Privacy Professionals Global Privacy Summit, held in March 2014); Michael A. Gold, *Cyber Risk and the Board of Directors — Closing the Gap*, Bloomberg BNA (Oct. 18, 2013), *available at* http://www.bna.com/cyber-risk-and-the-board-of-directors-closing-the-gap// (suggesting that companies would do well to have "[m]andatory cyber risk education for directors," among other things.); *see also, The Comprehensive National Cybersecurity Initiative*, initially launched by then-President George W. Bush in 2008, referencing "Initiative #8. Expand cyber education," and *available at* http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[29] *Supra* note 11, Lawrence J. Trautman and Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*.

[30] *See, supra* note 26, CyLab 2012 Report, at 27.

[31] PricewaterhouseCoopers LLP, *The Global State of Information Security Survey 2014*, at 4, *available at* http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.html (the "PwC IS Survey"). The PwC IS Survey also noted other shared attributes, such as having (i) an overall information security strategy; (ii) measured and reviewed the effectiveness of their security measures within the past year; and (iii) an understanding as to

exactly what type of security events have occurred in the past year. *See also*, *supra* note 2, Holly Gregory, *Board Oversight of Cybersecurity Risks*.

[32] Alice Hsu, Tracy Crum, Francine E. Friedman, and Karol A. Kepchar, *Cybersecurity Update: Are Data Breach Disclosure Requirements On Target?*, The Metropolitan Corporate Counsel (Jan. 24, 2014), *available at* http://www.metrocorpcounsel.com/articles/27148/cybersecurity-update-are-data-breach-disclosure-requirements-target

[33] *See, e.g.*, *Risk Management and the Board of Directors–An Update for* 2014, *supra* note 2 (noting that cybersecurity is a risk management issue that "merits special attention" from the board of directors in 2014); Alice Hsu, Tracy Crum, Francine E. Friedman, and Karol A. Kepchar, *Cybersecurity Update: Are Data Breach Disclosure Requirements On Target?*, The Metropolitan Corporate Counsel (Jan. 24, 2014), *available at* http://www.metrocorpcounsel.com/articles/27148/cybersecurity-update-are-data-breach-disclosure-requirements-target ("As part of a board's risk management oversight function, directors should assess the adequacy of their company's data security measures. Among other things, boards should have a clear understanding of the company's cybersecurity risk profile and who has primary responsibility for cybersecurity risk oversight and should ensure the adequacy of the company's cyber risk management practices, as well as the company's insurance coverage for losses and costs associate with data breaches.").