Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus

Commissioner Luis A. Aguilar

"Cyber Risks and the Boardroom" Conference
New York Stock Exchange
New York, NY

June 10, 2014

Good afternoon. Thank you for that kind introduction. I am glad to be back at the New York Stock Exchange. In anticipating today's conference, I thought back to an earlier trip to the NYSE where in April 2009, I had the opportunity to ring the closing bell. Before I begin my remarks, let me issue the standard disclaimer that the views I express today are my own, and do not necessarily reflect the views of the U.S. Securities and Exchange Commission ("SEC" or "Commission"), my fellow Commissioners, or members of the staff.

I am pleased 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 not too long 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, according to one survey, U.S. companies experienced a 42% increase between 2011 and 2012 in the number of successful cyber-attacks they experienced per week.[4] As I am sure you have heard, recently there have also been a series of well-publicized cyber-attacks that have generated considerable media attention and raised public awareness of this issue. A few of the more well-known examples include:

- The October 2013 cyber-attack on the software company Adobe Systems, Inc., in which data from more than 38 million customer accounts was obtained improperly;[5]
- The December 2013 cyber-attack on Target Corporation, in which the payment card data of approximately 40 million Target customers and the personal data of up to 70 million Target customers was accessed without authorization;[6]
- The January 2014 cyber-attack on Snapchat, a mobile messaging service, in which a reported 4.6 million user names and phone numbers were exposed;[7]
- The sustained and repeated cyber-attacks against several large U.S. banks, in which their public websites have been knocked offline for hours at a time;[8] and

- The numerous cyber-attacks on the infrastructure underlying the capital markets, including quite a few on securities exchanges.[9]

In addition to becoming more frequent, there are reports indicating that 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.[10] In addition, the aftermath of the 2013 Target data breach demonstrates that the impact of cyber-attacks may extend far beyond the direct costs associated with the immediate response to an attack.[11] Beyond the unacceptable damage to consumers, these secondary effects include reputational harm that significantly affects a company's bottom line. 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.[12]

As an SEC Commissioner, the threats are a particular concern because of the widespread and severe impact that cyber-attacks could have on the integrity of the capital markets infrastructure and on public companies and investors.[13] The concern is not new. For example, in 2011, staff in the SEC's Division of Corporation Finance issued guidance to public companies regarding their disclosure obligations with respect to cybersecurity risks and cyber-incidents.[14] More recently, because of the escalation of cyber-attacks, 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.[15]

Today, I would like to focus my remarks on what boards of directors can, and should, do to ensure that their organizations are appropriately considering and addressing cyber-risks. Effective 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.

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

Background on the Role of Boards of Directors

When considering the board's role in addressing cybersecurity issues, 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 and around the world, that corporations are managed under the direction of their boards of directors.[16] 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 would be 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. Clearly, effective full-time management is essential for public companies to function. But management without accountability can lead to self-interested decision-making that may not benefit the company or its shareholders. 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.[17]

Corporate Boards and Risk Management Generally

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.[18] Indeed, many have 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.[19] Although primary responsibility for risk management has historically belonged to management, the boards are responsible for overseeing that the corporation has established appropriate risk management programs and for overseeing how management implements those programs.[20]

The importance of this oversight was highlighted when, in 2009, the Commission amended its rules to require 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.[21] The Commission 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."[22]

The evidence suggests that boards of directors have begun to assume greater responsibility for overseeing the risk management efforts of their companies.[23] For example, according to a recent survey of 2013 proxy filings by companies comprising the S&P 200, the full boards of these companies are increasingly, and nearly universally, taking responsibility for the risk oversight of the company.[24]

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[25] — and there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight. The recent announcement that a prominent proxy advisory firm is urging the ouster of most of the Target Corporation directors because of the perceived "failure…to ensure appropriate management of [the] risks" as to Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks.[26]

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

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. [27]

In addition to the threat of significant business disruptions, substantial response costs, negative publicity, and lasting reputational harm, there is also the threat of litigation and potential liability for failing to implement adequate steps to protect the company from cyber-threats.[28] Perhaps unsurprisingly, there has recently been a series of derivative lawsuits brought against companies and their officers and directors relating to data breaches resulting from cyber-attacks.[29] Thus, boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril.

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. Yet, 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.[30] 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.[31] Even when boards do pay attention to these risks, some have questioned the extent to which boards rely too much on the very personnel who implement those measures.[32] In light of these observations, directors should be asking themselves what they can, and should, be doing to effectively oversee cyber-risk management.

NIST Cybersecurity Framework

In considering where to begin to assess a company's possible cybersecurity measures, one conceptual roadmap boards should consider is 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.[33] 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.[34] At 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.

Board Structural Changes to Focus on Appropriate Cyber-Risk Management

The NIST Cybersecurity Framework, however, is a bible without a preacher 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.[35] As a result, some have recommended mandatory cyber-risk education for directors.[36] 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.[37]

Another way that has been identified to help curtail the knowledge gap and focus director attention on known cyber-risks is to create a separate enterprise risk committee on the board. It is believed that such committees can foster a "big picture" approach to company-wide risk that not only may result in improved risk reporting and monitoring for both management and the board, but also can provide a greater focus — at the board level — on the adequacy of resources and overall support provided to company executives responsible for risk management.[38] The Dodd-Frank Act already requires large financial institutions to establish independent risk committees on their boards.[39] Beyond the financial institutions required to do so, some public companies have chosen to proactively create such risk committees on their boards.[40] Research suggests that 48% of corporations currently have board-level risk committees that are responsible for privacy and security risks, which represents a dramatic increase from the 8% that reported having such a committee in 2008.[41]

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 commend the boards that are proactively addressing these new risks of the 21st Century. However, while enhancing board knowledge and board involvement is a good business practice, it is not necessarily a panacea to comprehensive cybersecurity oversight.

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. One 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.[42] In addition, a 2013 survey 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.[43]

At a minimum, boards should have 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.[44] In addition, as the evidence shows, devoting full-time personnel to cybersecurity issues may help prevent and mitigate the effects of cyber-attacks.

Board Preparedness

Although different companies may choose different paths, ultimately, the goal is the same: to prepare the company for the inevitable cyber-attack and the resulting fallout from such an event. As it has been noted, the primary distinction between a cyber-attack and other crises that a company may face is the speed with which the company must respond to contain the rapid spread of damage.[45] Companies need to be prepared to respond within hours, if not minutes, of a cyber-event to detect the cyber-event, analyze the event, prevent further damage from being done, and prepare a response to the event.[46]

While there is no "one-size-fits-all" way to properly prepare for the various ways a cyber-attack can unfold, and what responses may be appropriate, it can be just as damaging to have a poorly-implemented response to a cyber-event. As others have observed, an "ill-thought-out response can be far more damaging than the attack itself."[47] Accordingly, boards should put time and resources into making sure that management has developed a well-constructed and deliberate response plan that is consistent with best practices for a company in the same industry.

These plans should include, among other things, whether, and how, the cyber-attack will need to be disclosed internally and externally (both to customers and to investors).[48] In deciding the nature and extent of the disclosures, I would encourage companies to go beyond the impact on the company and to also consider the impact on others. It is possible that a cyber-attack may not have a direct material adverse impact on the company itself, but that a loss of customers' personal and financial data could have devastating effects on the lives of the company's customers and many Americans. In such cases, the right thing to do is to give these victims a heads-up so that they can protect themselves.[49]

Conclusion

Let me conclude my remarks by reaffirming the significance of the role of good corporate governance. Corporate governance performed properly, results in the protection of shareholder assets. Fortunately, many boards take on this difficult and challenging role and perform it well. They do so by, among other things, being active, informed, independent, involved, and focused on the interests of shareholders.

Good boards also recognize the need to adapt to new circumstances — such as the increasing risks of cyber-attacks. To that end, board oversight of cyber-risk management is 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.

Those of you who have taken the time and effort to be here today clearly recognize the risks, and I commend you for being proactive in dealing with the issue.

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://www.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] *2012 Cost of Cyber Crime Study: United States*, Ponemon Institute LLC and HP Enterprise Security (Oct. 2012), *available at* http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

[5] *See, e.g.,* Jim Finkle, *Adobe says customer data, source code accessed in cyber attack*, Reuters (Oct. 3, 2013), *available at* http://www.reuters.com/article/2013/10/03/us-adobe-cyberattack-idUSBRE99212Y20131003; Jim Finkle, *Adobe data breach more extensive than previously disclosed*, Reuters (Oct. 29, 2013), *available at* http://www.reuters.com/article/2013/10/29/us-adobe-cyberattack-idUSBRE99S1DJ20131029; Danny Yadron, *Hacker Attack on Adobe Sends Ripples Across Web*, Wall Street Journal (Nov. 11, 2013), *available at* http://online.wsj.com/news/articles/SB10001424052702304644104579192393329283358.

[6] *See,* Testimony of John Mulligan, Executive Vice President and Chief Financial Officer of Target, before the Senate Judiciary Committee (Feb. 4, 2014), *available at* http://www.judiciary.senate.gov/imo/media/doc/02-04-14MulliganTestimony.pdf; Target Press Release, "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores" (Dec. 19, 2013), *available at* http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores.

[7] *See, e.g.,* Andrea Chang and Salvador Rodriguez, *Snapchat becomes target of widespread cyberattack*, L.A. Times (Jan. 2, 2014), *available at* http://articles.latimes.com/2014/jan/02/business/la-fi-snapchat-hack-20140103; Brian Fung, *A Snapchat security breach affects 4.6 million users. Did Snapchat drag its feet on a fix?* Washington Post (Jan. 1, 2014), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix/.

[8] *See, e.g.,* Joseph Menn, *Cyber attacks against banks more severe than most realize*, Reuters (May 18, 2013), *available at* http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518; Bob Sullivan, *Bank Website Attacks Reach New Highs*, CNBC (Apr. 3, 2013), *available at* http://www.cnbc.com/id/100613270.

[9] For example, according to a 2012 global survey of securities exchanges, 53% reported experiencing a cyber-attack in the previous year. *See,* Rohini Tendulkar, *Cyber-crime, securities markets, and systemic risk*, Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges (July 16, 2013), *available at* http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf. Forty-six securities exchanges responded to the survey.

[10] *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.

[11] *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).

[12] I also want to note that at the Investment Company Institute's ("ICI") general membership meeting, held just last month, 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.

[13] *See,* Commissioner Luis A. Aguilar, *The Commission's Role in Addressing the Growing Cyber-Threat* (Mar. 26, 2014), *available at* http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184.

[14] On October 13, 2011, staff in the Commission's Division of Corporation Finance (Corp Fin) issued guidance on issuers' disclosure obligations relating to cyber security risks and cyber incidents. *See,* SEC's Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2—Cybersecurity* ("SEC Guidance") (Oct. 31, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. Among other things,

this guidance notes that securities laws are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision, and cybersecurity risks and events are not exempt from these requirements. The guidance identifies six areas where cybersecurity disclosures may be necessary under Regulation S-K: (1) Risk Factors; (2) Management's Discussion and Analysis of Financial Condition and Results of Operation (MD&A); (3) Description of Business; (4) Legal Proceedings; (5) Financial Statement Disclosures; and (6) Disclosure Controls and Procedures. The SEC Guidance further recommends that material cybersecurity risks should be disclosed and adequately described as Risk Factors. Where cybersecurity risks and incidents that represent a material event, trend or uncertainty reasonably likely to have a material impact on the organization's operations, liquidity, or financial condition — it should be addressed in the MD&A. If cybersecurity risks materially affect the organization's products, services, relationships with customers or suppliers, or competitive conditions, the organization should disclose such risks in its description of business. Data breaches or other incidents can result in regulatory investigations or private actions that are material and should be discussed in the Legal Proceedings section. Cybersecurity risks and incidents that represent substantial costs in prevention or response should be included in Financial Statement Disclosures where the financial impact is material. Finally, where a cybersecurity risk or incident impairs the organization's ability to record or report information that must be disclosed, Disclosure Controls and Procedures that fail to address cybersecurity concerns may be ineffective and subject to disclosure. Some have suggested that such disclosures fail to fully inform investors about the true costs and benefits of companies' cybersecurity practices, and argue that the Commission (and not the staff) should issue further guidance regarding issuers' disclosure obligations. *See,* Letter from U.S. Senator John D. Rockefeller IV to Chair White (Apr. 9, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51.

[15] *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 has 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 recently 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. To date, we have received ten comment letters from academics, software companies, and other interested parties, *available at* http://www.sec.gov/comments/4-673/4-673.shtml. *See, e.g.*, Jodie Kelly, Senior Vice President and General Counsel, BSA| The Software Alliance comment letter (Apr. 30, 2014) (highlighting the importance of strong internal controls related to software assets as a first line of defense against cyber-attacks, and noting that verifying legal use of software is a critical first step in deterring cyber-attacks because the "existence and availability of pirated and counterfeit software exposes corporate information technology networks to significant risks in many ways."); Tom C.W. Lin, Associate Professor of Law, Temple University Beasley School of Law comment letter (Apr. 29, 2014) (expressing support for the roundtable and the Commission's attention to cybersecurity and highlighting four broad issues for the Commission's consideration: (1) cybersecurity threats to the high-speed, electronically connected modern capital markets can create systemic risks; (2) due to technological advances, financial choices are made by both people and machines, which does not comport congruently with many traditional modes of securities regulation; (3) incentives, in addition to penalties, should be designed to encourage firms to upgrade their cybersecurity capabilities; and (4) private regulation of cybersecurity should be vigorously enhanced and leveraged to better complement government regulation); Dave Parsonage, CEO, MitoSystems, Inc. comment letter (Apr. 3, 2014); Gail P. Ricketts, Senior IT Compliance and Risk Analyst, ON Semiconductor comment letter (Mar. 26, 2014) (suggesting future roundtables include speakers from outside the financial services industry, such as manufacturing); Michael Utzig, IT Director, Hefren Tillotson, Inc. comment letter (Mar. 26, 2014) (noting that readily available technologies that can protect email communications are not widely used despite universal understanding that cybersecurity is a high-priority); Cathy Santoro comment letter (Mar. 26, 2014) (raising questions about the interactions between banks and service providers and the measures being undertaken regarding mobile payment cybersecurity risks); Duane Kuroda, Senior Threat Researcher, NetCitadel comment letter (Mar. 25, 2014) (noting that the panel discussion should focus on the process and people involved in responding to breaches and not just their detection); William Pfister, Jr. comment letter (Mar. 25, 2014) (requesting that one of the panels address the potential conflicts between national security and required disclosure). Many of these letters are generally supportive of the Commission's efforts and focus in this area, and some identify issues and concerns that were not discussed in detail during the roundtable and warrant further attention. For example, one commenter highlighted the need for companies to adopt sound internal controls over the legal use of software, noting that pirated and counterfeit software can expose companies to heightened risk of cyber-attacks and recommending that registrants report on the status of such internal controls.[15] *See, e.g.*, Jodie Kelly, Senior Vice President and General Counsel, BSA| The Software Alliance comment letter (Apr. 30, 2014) (noting, among other things, that unlicensed software eliminates the opportunity for security updates and patches from legitimate vendors when security breaches are identified, and that malware and viruses may be contained within pirated software itself or reside on the networks from which it is downloaded. BSA recommends that registrants report on the status of their internal controls in the area of licensing and legal use of software, and that such controls should, at a minimum, ensure that software is only purchased from authorized vendors and that companies should have procedures to conduct periodic software

inventories and limit exposure to malware and viruses brought into their systems by linkage of employees' personal devices to corporate systems). I encourage others to comment and provide valuable input on this critical issue.

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

[17] 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.

[18] *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.").

[19] 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.").

[20] *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.").

[21] *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.

[22] *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.

[23] *Supra* note 19, 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.").

[24] *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.").

[25] See, *Proxy Disclosure Enhancements*, *supra* note 21.

[26] Paul Ziobro, *Target Shareholders Should Oust Directors, ISS Says*, Wall St. Journal (May 28, 2014), *available at* http://online.wsj.com/article/BT-CO-20140528-709863.html; 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.

[27] *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.").

[28] 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.").

[29] *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.).

[30] 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.").

[31] 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.").

[32] *Supra note 30,* Steven P. Blonder, *How Closely is the Board Paying Attention to Cyber Risks?* (stating that "[f]urther, even if a board has evaluated these risks, to what extent is such an evaluation dependent on a company's IT department — the same group implementing the existing technology protocols?").

[33] 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.

[34] *Supra note* 2*,* Holly J. Gregory, *Board Oversight of Cybersecurity Risks; supra note* 33, 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.").

[35] 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?").

[36] *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.

[37] *Supra* note 19, Lawrence J. Trautman and Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*.

[38] *Supra* note 35, Matteo Tonello, *Should Your Board Have a Separate Risk Committee?*; *supra* note 33, Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom*.

[39] Dodd-Frank Act Section 165(h).

[40] *Supra* note 19, Lawrence J. Trautman and Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*.

[41] Deloitte Audit Committee Brief, *Cybersecurity and the audit committee* (Aug. 2013), at 2, *available at* http://deloitte.wsj.com/cfo/files/2013/08/ACBrief_August2013.pdf.

[42] *See*, *supra* note 31, CyLab 2012 Report, at 27.

[43] 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.jhtml (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*.

[44] *Supra* note 27, Alice Hsu, *et al.*, *Cybersecurity Update: Are Data Breach Disclosure Requirements on Target?*.

[45] *See, e.g.,* Roland L. Trope and Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid,* 40 Wm. Mitchell L. Rev. 647 (2014), at 656 (stating that "unlike other corporate crises, boards and management must be ready to address severe cyber incidents with response and recovery plans that activate upon discovery of an intrusion and with little or no time for deliberation.") Some observers have even suggested that companies conduct "cyberwar games" organized around hypothetical business scenarios in order to reenact how a company might respond in a real cybersecurity situation in order to fix what vulnerabilities are teased out from the simulated scenario. Tucker Bailey, James Kaplan, and Allen Weinberg, *Playing war games to prepare for a cyberattack*, McKinsey & Company Insights & Publications (July 2012). Other observers have suggested that companies implement a response plan that takes into consideration a number of factors, such as (i) how much risk the company can accept if systems or services have to shut down; (ii) for how long the company can sustain operations using limited or backup technology; and (iii) how quickly the company can restore full operations. *See, Former FBI Agent Mary Galligan on Preparing for a Cyber Attack,* CIO Journal, Deloitte Insights (Mar. 3, 2104), *available at* http://deloitte.wsj.com/cio/2014/03/03/former-fbi-agent-mary-galligan-on-preparing-for-a-cyber-attack/.

[46] *See, e.g., id*., Roland L. Trope and Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid*, at 656.

[47] *Supra* note 45, Tucker Bailey, James Kaplan, and Allen Weinberg, *Playing War Games to Prepare for a Cyberattack*.

[48] *Supra* note 33, Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom*, Metropolitan Corporate Counsel (stating that "Boards should prepare for worst-case scenario cybersecurity breaches and help management develop immediate response plans, including public disclosure procedures and economic recovery strategies, to mitigate potential damages." In addition, "[b]oards should consider disclosing cybersecurity risks and protective measures on relevant SEC filings, as such disclosures can generate confidence in investors rather than fear.") The U.S. Department of Commerce also has suggested that a company's cybersecurity preparedness could include cybersecurity insurance, which is specifically designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. *Cybersecurity Insurance*, U.S. Department of Homeland Security, *available at* http://www.dhs.gov/publication/cybersecurity-insurance. Despite the increased threats of cyber-attacks, the cybersecurity insurance market has been slow to develop, and many companies have chosen to forego available policies, citing their perceived high cost, a lack of awareness about what they cover, and their confidence (or ignorance) about their actual risk of a cyber-attack. *Id.* Moreover, despite the fact that cyber incidents are not covered by general liability policies, one survey noted that 57% of respondents indicated that their boards are not reviewing their existing policies for cyber-related risks. *See*, *supra* note 31, CyLab 2012 Report, at 15.

[49] The Department of Justice recently unsealed indictments against five Chinese military officials who allegedly conspired to steal information from U.S. companies across different industries. In connection with this indictment, it was recently reported that three U.S. public companies identified as victims of this conspiracy failed to report the theft of trade secrets and other data to their investors, despite the Commission's disclosure guidance on this topic. Two of the companies, Alcoa Inc. and Allegheny Technologies Inc., said that the thefts were not "material," and therefore did not have to be disclosed to investors. *See,* Chris Strohm, Dave Michaels and Sonja Elmquist, *U.S. Companies Hacked by Chinese Didn't Tell Investors*, Bloomberg (May 21, 2014), *available at* http://www.bloomberg.com/news/2014-05-21/u-s-companies-hacked-by-chinese-didn-t-tell-investors.html*; See also, supra note 14.*

Last modified: June 10, 2014