Director Notes

THE CONFERENCE BOARD GOVERNANCE CENTER®

The Board's Role in Cybersecurity

by Richard Clarke and Jacob Olcott

The costs of a cyber attack can be significant. To protect finances, liability, reputation, and future growth, corporate boards must ensure that their companies have appropriate processes in place to manage cyber risk in the context of their business. This article looks at cybersecurity from a governance perspective and offers suggestions for directors on how to carry out their oversight role.

For many companies, 2013 marked the year that responsibility for oversight of cybersecurity moved from the IT department to the boardroom. Publicity surrounding China's growing cyber army, massive theft of information by trusted insiders like Edward Snowden, and large data breaches, such as the one experienced by Target Corporation in December 2013, all helped to elevate cyber risk to the forefront for business executives. With so much at stake for a business—financial loss, operational disruption, competitive disadvantage, legal liability, and harm to corporate reputation—the question for corporate directors and officers is not whether to become involved in cyber risk management, but how to appropriately oversee their company's initiatives.

The Rewards and Risks of Information Technology

Virtually every essential business function performed today uses information technology, making IT both a key business enabler and a critical business risk. The task of balancing business and employee demands for greater connectivity and access to information with the security concerns that may arise from granting those requests is complex and challenging. Each device or software application used can help facilitate new business opportunities, but those technologies also have the potential to be used to infiltrate or harm the business. Balancing the rewards and risks associated with the use of smart phones and other mobile devices by employees and/or board members is

No. DN-V6N6
MARCH 2014
Subscribe for free at www.conference-board.org/directornotes

THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

just one example of the growing challenges that corporate cybersecurity professionals face. Mobile devices facilitate working remotely, but the microphones and cameras in those devices that enable business functionality can also be activated remotely to record and monitor communications in real time, creating a potential risk that important financial and strategic data could be compromised.

Malicious actors can leverage information technology in countless ways that can negatively impact a business. Ironically, the very information technology originally developed to enable businesses may now be used as a weapon against the enterprise. For example, Iranian attackers harnessed the power of cloud computing to launch massive denial of service attacks against the US financial services industry, including JPMorgan Chase, Bank of America, Citigroup, and others, resulting in disabled corporate websites, lost revenues, high customer dissatisfaction, and new security technology expenditures.[1] In another example, reports have shown that software programs like Metasploit, originally developed to help defenders identify security holes in their own systems, have been used by outside actors to exploit those same vulnerabilities.[2]

The most damaging attacks may not even come from external threats, but from knowledgeable, trusted insiders with access to sensitive information. In 2013, former National Security Agency (NSA) contractor Edward Snowden demonstrated that even the most secure organizations are vulnerable to the insider threat. Enabled by advances in data storage that allow a nearly unlimited amount of information to be placed on a device small enough to fit in one's pocket, Snowden was able to bypass the NSA's digital and physical access management security and steal hundreds of thousands of classified documents.[3] Insider threats pose challenges for companies in the private sector as well. Last year, the US government obtained an indictment of Sinovel Corp., a China-based manufacturer and exporter of wind turbines that used an insider to steal proprietary source code and confidential business information from American Superconductor (AMSC).[4] The theft led to lost customers, which in turn caused a massive drop in the company's stock price, from which it has not recovered.[5]

Cyber attacks can also destroy data and assets, with the potential to inflict severe economic loss to a business. An August 2012 attack against oil company Saudi Aramco completely erased the hard drives and contents of approximately 30,000 corporate computers, all of which had to be replaced.[6] A similar attack was used in March 2013 against banks in South Korea.[7] The Stuxnet virus, launched several years ago against an Iranian nuclear facility, demonstrated that cyberweapons could be used to physically destroy infrastructure.[8] Remarkably, the virus destroyed nuclear centrifuges even though the facility was physically isolated and disconnected from the Internet. While cyber attacks resulting in this type of destruction, fortunately, remain rare, the ability to inflict this type of damage clearly exists.

Potential Enforcement and Liability

If new attack vectors and threat actors aren't enough cause for concern, corporate leaders face significant and growing legal liability for failing to protect their businesses. In the United States, cybersecurity regulations in the financial, energy, and defense sectors continue to expand. President Obama issued an executive order in 2013 creating new cybersecurity standards for critical infrastructure companies.[9] The Federal Trade Commission has been actively enforcing consumer protection laws against companies that have suffered breaches, most notably the ongoing case against Wyndham Worldwide Corporation.[10] Private regulatory organizations such as the credit industry-sponsored Payment Card Industry Council are developing stricter security guidelines for retailers that process credit card transactions, and banks and credit card institutions continue to enforce noncompliance with those guidelines through fines.[11] Nearly every US state has a data breach notification law that allows state attorneys general to pursue actions against organizations that fail to appropriately disclose incidents involving their constituents' information.[12] Federal agencies have announced increased oversight of new security requirements for companies that maintain personal health information.[13] The Securities and Exchange Commission, which issued guidance to publicly traded companies in 2011 about their obligations to disclose cyber attacks to shareholders, is now poised to enforce nondisclosure of material cyber incidents.[14] In addition, the commission will hold a public roundtable in March 2014 to discuss the issues and challenges cybersecurity raises for market participants and public companies, and how organizations are addressing those concerns. Following a massive data breach involving customer information in December of 2013, Target Corporation faces nearly 70 lawsuits, including at least two shareholder derivative lawsuits that allege that the company's board of directors breached their fiduciary duties by failing to take sufficient steps to protect the company from a breach and its consequences. [15]

Beyond the United States, countries around the globe continue to adopt new, tough laws requiring various levels of protection of business and customer information.

The European Union, for instance, has already adopted stringent data privacy standards, and is poised to require companies to implement greater cybersecurity controls to protect their businesses,[16] and Asian countries like Singapore assess financial institutions against a robust set of internal and vendor-focused security controls.[17] Lack of standardization for security poses a huge challenge for businesses and the people charged with meeting those standards. For companies seeking to expand operations, data security and privacy are critical components needed to compete in virtually every market and, for some companies, differentiate service offerings from less-secure competitors.

The Board's Role

With so much at stake for a business, it should be clear that cyber risk management is not merely the IT staff's responsibility. Cyber risk management should be an enterprise-wide effort with participation from senior executives, corporate officers, and directors to ensure that the appropriate strategies, risk management policies, and budget for the company are in place. Many corporate directors recognize that cyber risk management is an integral component of their fiduciary duty to the company, requiring them to act with care and diligence. Still, many boards struggle with how to effectively execute their duties to the company in the area of cyber risk management. The following steps may serve as a good starting point.

Common Cybersecurity Terms Defined

Advance Persistent Threat A type of threat actor that conducts multistage campaign against specific persons or organizations to breach their computer network in order to conduct surveillance, steal, or destroy specific information.

Event Anomalous code or data flow that real-time continuous monitoring technology flags as abnormal.

Breach The compromise of a network by a threat actor that provides an unauthorized person access to corporate network.

Perimeter-based Cybersecurity technology such as firewalls, antivirus, and antimalware scanners placed at the edge of a network that typically offers protection against malicious code that is already known.

Crown jewels Data or assets within an organization that is crucial to its business functions and/or future viability as a successful organization.

Understand cyber risk

To begin, though awareness continues to improve, many board members simply may not have a strong understanding of cyber risks and their actual or potential impact to the company. Reasons for this lack of awareness typically include the board's general discomfort or disinterest in information technology, the technology staff's difficulty in communicating risks to the business leaders, or the incorrect assumption by leadership that the company is impervious to a consequential cyber incident. If this is the board's first time engaging on cybersecurity issues, a briefing by a trusted internal, external, or even government advisor can help educate board members about important issues related to cyber threats, vulnerabilities, and consequences, and can help put those risks into the context of the business. Directors may also consider asking directors of other boards with more experience overseeing cybersecurity issues within their organizations to help supplement their information. Boards may also want to consider the framework or recommendations of widely recognized groups (see "Cybersecurity Guidance for Boards to Consider" below).

Cybersecurity Guidance for Boards to Consider

ISO/IEC 27032 An international standard that contains baseline security practices for companies.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework A framework of best practices based on a variety of international cybersecurity standards that companies can use to assess their own cybersecurity maturity.

The SANS Institute Critical Security Controls These guidelines feature a list of 20 prioritized security controls that have been deemed to be effective to combat cyber attackers by a group of public and private security experts.

Sources: International Organization for Standardization (www.iso.org), NIST (www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf) and The SANS Institute (www.sans.org/critical-security-controls/).

Evaluate the organizational approach to cybersecurity

Prioritizing cyber risk management at the board level can help to increase awareness, establish management and oversight expectations, facilitate information exchange about strategic and technical cyber risk challenges between the board and employees, and help facilitate a company-wide culture of cybersecurity. Directors should focus on both creating a board-level governance structure and evaluating the corporation's approach to cyber governance.

A number of companies have designated or created a board-level committee to oversee cyber risk. Some companies delegate cyber risk management to the audit committee.[18] If a company determines that cyber risk oversight should be designated to a board-level committee, the cross-functional impact that cyber incidents can have on the business should be considered in determining where within the board's organizational structure oversight of such risk is best housed.

Recognizing that cyber risk management is more than just an IT component, directors should ensure that their companies have developed a cyber risk governance program that incorporates business and technology executives and functions across the company. This approach should consider the role of key executives (e.g., CEO, general counsel, chief financial officer, chief information officer (CIO), and chief information security officer), the way that risk management decisions are made, and whether a cybersecurity committee or management team exists or should be created. This committee or team can provide the board with information about a variety of cross-cutting cyber risk issues, including, for instance, existing and emerging legal requirements related to network and data security. As a result of rapidly expanding legal liability, general counsels are increasingly being tasked with leading or co-leading, along with the CIO, cyber risk governance programs. Fortune 500 companies that maintain enterprise risk management programs are incorporating cyber risk into this broader framework.

Request regular briefings on cyber risk/threats

In order to effectively carry out their oversight responsibility, board members should request strategic and technical information about the company's cyber risk and mitigation efforts from those responsible within the organization. However, a 2012 survey by Carnegie Melon University found that fewer than 40 percent of boards regularly receive reports on privacy and security risks, and 26 percent rarely or never receive such information.[19] In a study released in January by the Ponemon Institute, only 12 percent of boards stated that they received cyber threat briefings frequently.[20] Boards that do not have updated information regarding privacy and security risks are unable to adequately consider how to prioritize threats to their companies, and cannot effectively oversee or approve management priorities. Since cyber risks and threats can change quickly, directors with designated responsibility for overseeing cyber risk management should receive briefings or updates at least quarterly. Briefings to the full board should be provided semiannually or as situations warrant.

Prioritize material cyber risks to protect business value

Not all cyber risks are created equal, therefore companies must prioritize cybersecurity initiatives. Businesses should focus their resources on reducing material cyber risks by protecting their "crown jewels," which are the information and technology assets that could have the most significant financial impact on the business if compromised, destroyed, or disrupted. In other words, the company's "worst case scenarios" for a cyber attack should be the ones to which it devotes the most resources. In considering financial impact, a company must not only consider direct financial and economic loss, but the financial harm that can arise from defending lawsuits, operational disruption, reputational damage, and competitive loss.

Questions for Boards to Consider

- What are the company's "crown jewels"?
- Has the company effectively allocated resources based on risk appetite and strategic assets?
- What technical capabilities does the company have in place to identify malicious events in real-time?
- How frequently does the board receive cyber threat briefings from the company?
- What is the company's response plan in the event of a breach/attack? How often is the response plan tested?
- What relationships does the company have/need to develop with government and other third-party organizations to respond effectively to a breach?

Regardless of the industry, ensuring that the company's cyber risk management strategy is built around protecting the information and assets that are important to the business is a key role of the board. Board members are well suited to help their companies with this important discovery process. They have knowledge of the company's business information, trade secrets, customer records, and essential technology. Prioritizing a cyber risk management program without considering the business consequences to the company can waste valuable resources protecting the wrong things. Unfortunately, according to a 2013 study conducted by Tripwire, over 30 percent of companies say they do not have a "risk-based" security management program.[21] Moreover, a 2010 Forrester report revealed that organizations allocate the same amount of resources to protect their company secrets and customer data, even though they consider company secrets twice as valuable as the data.[22] Sensitive business data that provides the most value to business operations and future success should be prioritized and guarded with appropriate resources. Board members can promote the concept of protecting business value within their organizations by participating in these information identification initiatives.

A cyber risk management program that is focused on material risks and consequences to the company will also help public companies satisfy their fiduciary duty and legal obligations to investors. The SEC stated in 2011 that public companies must report material cyber risks and incidents to their shareholders. Identifying and mitigating the cyber risks that would have the most significant economic impact to the business can help reduce the likelihood that a company will have to disclose incidents to its shareholders, thereby protecting business value and reducing liability exposure.

Boards should keep in mind that information vital to the long-term success of the organization resides not only within the walls of the corporate castle, but also on the networks of the company's external advisors (its law firms, consulting firms, etc.). Ensuring that the company has a vendor risk management plan is an essential step to managing material cyber risk.

Request a security technology "roadmap" and budget estimates to implement the strategy

Technology is an important component to help reduce cyber risk. Directors should review the company's cybersecurity expenditures to ensure that they are aligned with reducing the company's most significant business risks.

Though cyber threats have evolved significantly in recent decades, many companies still use traditional perimeter-based technical approaches to defend their networks and data. According to a 2013 ISACA study, more than 80 percent of companies reported that they use traditional perimeter security, including firewalls, routers, and anti-virus/anti-malware programs, to defend themselves against advanced persistent threats (APTs).[23] Modern cybersecurity requires visibility inside the network and at endpoints that traditional firewalls and antivirus technologies cannot provide solely at the perimeter. Boards play an important role in ensuring that their companies acquire the appropriate technology to protect the most critical elements of the business. Directors should request a security technology "road map," a strategy with accompanying budget that incorporates the company's business risks into a technology acquisition strategy.

In considering the role of technology, it is becoming clear to most organizations that they must maintain a "real-time" view of the security of the company's networks and data in order to identify and mitigate incidents when they occur. It appears that few companies are doing this successfully. Companies rarely discover data breach incidents on their own, as reported by Verizon, which found that almost 70 percent of companies penetrated did not know until told by a third party.[24] Moreover, that same report found that it took "weeks or months" for most companies to discover they had been breached.[25] Having real-time security and event monitoring can help companies develop metrics to measure progress and maturity over time. Ironically, though they would clearly benefit from receiving real-time information about the company's security posture, board members are among the least likely members of an organization to request such a capability.[26]

While the amount spent on security is not directly relevant to a company's security posture, it can provide indications of how the company treats the issue. A 2013 PWC survey found that companies typically invest only 3.8 percent of their total information technology investment in security.[27] Though there is no "right" or "wrong" percentage of investment in cybersecurity, corporate directors should inquire about whether budgets are adequate for all information technology operations, including security.

Having a security technology roadmap and corresponding budget to implement it can lead to a more efficient allocation of resources that reduces the company's most significant risks. After a breach event, for instance, companies often rush to buy technology without fully appreciating the problem that they are trying to solve. Board members addressing a breach event should ensure that any technologies purchased are aligned with the company's short-, medium-, and long-term requirements, and should review this alignment iteratively.

Testing your company's response plan with a cyber exercise

Even with a robust strategy and cutting-edge technology, a company may still suffer a breach. Advanced preparation and effective crisis management are therefore key elements of a company's cyber risk management strategy. Knowing when to bring in technical and legal support and how to engage with law enforcement, customers, shareholders, the media, and other affected parties is critical to reducing the damage that could result from a cyber incident.

Unfortunately, many companies do not adequately account for a cyber-related incident in their business continuity and disaster recovery plans, and few companies test their plans before a cyber crisis occurs.

Simulations that include the participation of important executive and operational personnel across the organization can strengthen awareness and improve the ability of teams from across the organization to work together and to communicate quickly and effectively in a real crisis. Scenarios should test a variety of different cyber incidents, from the loss of critical data to significant operational disruption. Board members should initiate and participate in such exercises to help them understand their role and responsibility during a crisis. After-action reports that summarize the simulation findings and contain actionable recommendations for board members and business leaders to improve cyber risk management can help drive important changes in the business that may help reduce the risk of future events or, at the very least, any damage that may result from such an attack.

Conclusion

Cybersecurity is a rapidly changing risk that every business must address. Corporate directors play an important role in ensuring their companies have sufficient policies and resources in place to address that risk and to respond in the event that the company does suffer a cyber attack. Boards should ensure that they are requesting and receiving appropriate and timely information to help them fulfill their oversight role in managing cyber risk.

ENDNOTES

[1] Nicole Perlroth and Quentin Hardy "Bank Hacking Was the Work of Iranians, Officials Say," *New York Times*, January 8, 2013. See also Tracy Kitten, "Top Banks Offer New DDoS Details," *BankInfoSecurity.com*, April 9, 2013 (www.bankinfosecurity.com/top-banks-offer-new-ddos-details-a-5667/op-1).

[2] Tom Brewster, "How the NSA, GCHQ and Crooks Can Hack Mobile Apps," *Wired*, January 30, 2014 (www.wired.co.uk/news/archive/2014-01/30/how-the-nsa-gchq-and-crooks-can-hack-mobile-apps).

[3] Ken Dilanian, "Officials: Edward Snowden Took NSA Secrets on Thumb Drive," *Los Angeles Times*, June 13, 2013 (http://articles.latimes.com/2013/jun/13/news/la-pn-snowden-nsa-secrets-thumb-drive-20130613).

[4] "Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of Amsc Trade Secrets," US Department of Justice press release, June 27, 2013 (www.justice.gov/opa/pr/2013/June/13-crm-730.html).

[5] Michael A. Riley and Ashlee Vance, "China Corporate Espionage Boom Knocks Wind Out of US Companies," *Bloomberg*, March 15, 2012 (www.businessweek.com/news/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-dot-s-dot-companies).

[6] "Saudi Arabia Says Cyber Attack Aimed to Disrupt Oil, Gas Flow," *Reuters*, December 9, 2012 (www.reuters.com/article/2012/12/09/saudi-attack-idUSL5E8N91UE20121209).

[7] Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *New York Times*, March 20, 2013 (www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html).

[8] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012 (www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all).

[9] See "Executive Order—Improving Critical Infrastructure Cybersecurity," The White House, February 12, 2013 (www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity) and *Framework for Improving Critical Infrastructure Cybersecurity,* The National Institute of Standards and Technology (NIST) (www.nist.gov/cyberframework/).

[10] "FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information," Federal Trade Commission press release, June 26, 2102 (www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect) and FTC complaint, filed August 9, 2012 (www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf).

[11] "Payment Card Industry (PCI) Data Security Standard," PCI, November 2013 (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf).

[12] "State Security Breach Notification Laws," National Conference of State Legislatures, last updated January 21, 2014 (www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

[13] "New Rule Protects Patient Privacy, Secures Health Information," US Department of Health and Human Services press release, January 17, 2013 (www.hhs.gov/news/press/2013pres/01/20130117b.html).

[14] "CF Disclosure Guidance : Topic No. 2 Cybersecurity," US Securities and Exchange Commission Division of Corporation Finance, October 13, 2011 (www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm) and Sara N. Lynch, "SEC Examiners to Review How Asset Managers Fend Off Cyber Attacks," *Reuters*, January 30, 2014 (www.reuters.com/article/2014/01/30/us-sec-cyber-assetmanagers-idUSBREA0T1PJ20140130).

[15] See Joel Schechtman, "Target Faces Nearly 70 Lawsuits Over Breach," *Wall Street Journal*, January 15, 2014; and Kevin LaCroix, "Target Directors and Officers Hit with Derivative Suits Based on Data Breach," *The D&O Diary,* February 3, 2014 (www.dandodiary.com/2014/02/articles/cyber-liability/target-directors-and-officers-hit-with-derivative-suits-based-on-data-breach/).

[16] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on The Free Movement of Such Data" (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT).

[17] "Technology Risk Management Guidelines," Monetary Authority of Singapore, June 2013 (www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf).

[18] "Global Audit Committee Survey," KPMG Audit Committee Institute, January 2013, p. 10 (https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/documents/global-audit-committee-survey-2013.pdf).

[19] Jody Westby "Governance of Enterprise Security: CyLab 2012 Report," Carnegie Mellon University, 2012, p. 16 (http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf).

[20] *Cyber Security Incident Response: Are We as Prepared As We Think?* Ponemon Institute Research Report, January 2014, p. 25 (www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf/).

[21] "The State of Risk-based Security Management," Tripwire and Ponemon Institute, 2013, p. 10 (www.tripwire.com/ponemon/2013/).

[22] "The Value of Corporate Secrets: How Compliance and Collaboration Affect Enterprise Perceptions of Risk," Forrester, March 2010, p. 2 (www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf).

[23] "Advanced Persistent Threat Awareness Study Results," ISACA, February 2013, p. 14 (www.isaca.org/Knowledge-Center/Research/Documents/APT-Survey-Report_whp_Eng_0213.pdf?id=b109a417-5a2f-44f1-88eb-7b5d2f5f1362).

[24] "2013 Data Breach Investigations Report," Verizon, 2013, p. 53 (www.verizonenterprise.com/DBIR/2013/).

[25] "2013 Data Breach Investigations Report," Verizon, 2013, p. 51 (www.verizonenterprise.com/DBIR/2013/). For example, Target Corp. discovered it was breached through an investigation by credit card issuers into a spike in fraudulent charges when they discovered that all the cards had recently been used at Target. Target was notified in mid-December 2013 that some credit cards used at their stores were used to run fraudulent charges, but it wasn't until January 1, 2014 that the company discovered evidence of a breach. See Danny Yadron, "Target Hackers Wrote Partly in Russian, Displayed High Skill, Report Finds," *Wall Street Journal*, January 16, 2014 (http://online.wsj.com/news/articles/SB10001424052702304419104579324902602426862).

[26] "Continuous Auditing and Continuous Monitoring: The Current Status and the Road Ahead," KPMG, 2012, p. 12 (http://www.kpmg.com/AE/en/IssuesAndInsights/ArticlesPublications/Press_releases/Documents/CA_CM_survey.PDF).

[27] "Defending Yesterday: Key Findings from The Global State of Information Security Survey 2014," PWC, October 2013, p. 4 (www.pwc.com/en_GX/gx/consulting-services/information-security-survey/pwc-gsiss-2014-key-findings-report.pdf).

About the Authors

Richard Clarke is chairman and CEO of Good Harbor Security Risk Management, a boutique firm providing cyber risk management advice to corporate leaders. He served the last three presidents as a senior White House Advisor, including as Special Advisor to the President for Cybersecurity and National Coordinator for Security and Counterterrorism. He recently served on President Obama's Review Group on Intelligence and Communications Technology. More at www.goodharbor.net.

Jacob Olcott is a principal at Good Harbor Security Risk Management. Previously, he served as legal advisor on cybersecurity to members of the US Senate Commerce Committee and House of Representatives Homeland Security Committee.

About Director Notes

Director Notes is a series of online publications in which The Conference Board engages experts from several disciplines of business leadership, including corporate governance, risk oversight, and sustainability, in an open dialogue about topical issues of concern to member companies. The opinions expressed in this report are those of the author(s) only and do not necessarily reflect the views of The Conference Board. The Conference Board makes no representation as to the accuracy and completeness of the content. This report is not intended to provide legal advice with respect to any particular situation, and no legal or business decision should be based solely on its content.

About the Series Director

Matteo Tonello is managing director of corporate leadership at The Conference Board in New York. In his role, Tonello advises members of The Conference Board on issues of corporate governance, regulatory compliance, and risk management. He regularly participates as a speaker and moderator in educational programs on governance best practices and conducts analyses and research in collaboration with leading corporations, institutional investors and professional firms. He is the author of several publications, including *Corporate Governance Handbook: Legal Standards and Board Practices,* the annual *U.S. Directors' Compensation and Board Practices* and *Institutional Investment reports,* and *Sustainability in the Boardrooom*. Recently, he served as the co-chair of The Conference Board Expert Committee on Shareholder Activism and on the Technical Advisory Board to The Conference Board Task Force on Executive Compensation. He is a member of the Network for Sustainable Financial Markets. Prior to joining The Conference Board, he practiced corporate law at Davis Polk & Wardwell. Tonello is a graduate of Harvard Law School and the University of Bologna.

About the Executive Editor

Melissa Aguilar is a researcher in the corporate leadership department at The Conference Board in New York. Her research focuses on corporate governance and risk issues, including succession planning, enterprise risk management, and shareholder activism. Aguilar serves as executive editor of *Director Notes,* a bimonthly online publication published by The Conference Board for corporate board members and business executives that covers issues such as governance, risk, and sustainability. She is also the author of The Conference Board *Proxy Voting Fact Sheet* and co-author of *CEO Succession Practices*. Prior to joining The Conference Board, she reported on compliance and corporate governance issues as a contributor to *Compliance Week* and *Bloomberg Brief Financial Regulation*. Aguilar previously held a number of editorial positions at SourceMedia Inc.

About The Conference Board

The Conference Board is a global, independent business membership and research association working in the public interest. Our mission is unique: to provide the world's leading organizations with the practical knowledge they need to improve their performance and better serve society. The Conference Board is a nonadvocacy, not-for-profit entity, holding 501(c)(3) tax-exempt status in the USA.

About The Conference Board Governance Center®

The Conference Board Governance Center brings together a distinguished group of senior corporate executives from leading world-class companies and influential institutional investors in a collaborative setting. As a member of the Governance Center, you will participate in a thought-leading forum to engage with other corporate executives and institutional investors in a confidential, collaborative setting; hear from outside experts about emerging issues; discuss and get counsel on your most pressing governance, ethics, and enterprise risk challenges; examine issues from an interdisciplinary perspective; and drive landmark research that contributes to advancing best practices. For more information, please visit www.conference-board.org/governance.

For more information on this report, please contact:
Melissa Aguilar, researcher, corporate leadership at 212 339 0303 or melissa.aguilar@conferenceboard.org

THE CONFERENCE BOARD, INC. | WWW.CONFERENCEBOARD.ORG
AMERICAS | +1 212 759 0900 | CUSTOMER.SERVICE@CONFERENCEBOARD.ORG
ASIA | +65 6325 3121 | SERVICE.AP@CONFERENCEBOARD.ORG
EUROPE, MIDDLE EAST, AFRICA | +32 2 675 54 05 | BRUSSELS@CONFERENCEBOARD.ORG

THE CONFERENCE BOARD OF CANADA | +1 613 526 3280 | WWW.CONFERENCEBOARD.CA

To learn more about The Conference Board corporate membership, please email us at membership@conferenceboard.org