



Governance of Cybersecurity: 2015 Report

How Boards & Senior Executives Are Managing Cyber Risks


**Author: Jody R. Westby
Adjunct Professor, Georgia Institute of Technology
CEO, Global Cyber Risk LLC**

October 2, 2015

Research Sponsors:

The logo for Forbes, featuring the word "Forbes" in a large, bold, black serif font.





© 2015 by Jody R. Westby and Georgia Tech Information Security Center
All rights reserved. No part of the contents hereof may be reproduced in any form without the
prior written consent of the copyright owners.

Georgia Tech Information Security Center

Georgia Institute of Technology
Klaus Advanced Computing Building
266 Ferst Drive
Atlanta, GA 30332-0765 USA
(404) 385-2879 • (404) 894-1155 (Fax)
Wenke Lee, Ph.D., Director

Jody R. Westby, Esq.

Adjunct Professor, Georgia Institute of Technology, School of Computer Science,
CEO, Global Cyber Risk LLC
5125 MacArthur Blvd., NW
Third Floor
Washington, DC 20016
(202) 255-2700 • (202) 537-5073 (Fax)

Table of Contents

Table of Contents	iii
Abbreviations	iv
About Georgia Tech and GTISC	1
About Jody R. Westby	2
About Financial Services Roundtable	3
About Forbes	3
About Palo Alto Networks	4
Executive Summary	5
About the Survey	11
I. Introduction	12
Purpose of the Governance Survey	12
Background: Duty of Boards & Directors	12
II. Findings & Conclusion	15
Who We Asked	15
Findings	17
Conclusions	33
III. Recommendations	37
Endnotes	39

Abbreviations

ABA	American Bar Association
ASIS	American Society for Industrial Security
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CMU	Carnegie Mellon University
CoE	Council of Europe
COO	Chief Operating Officer
CPO	Chief Privacy Officer
CRO	Chief Risk Officer
CSO	Chief Security Officer
CyLab	Carnegie Mellon CyLab
D&Os	Directors & Officers
EU	European Union
FFIEC	Federal Financial Institutions Examination Council
FTC	Federal Trade Commission
FSR	Financial Services Roundtable
GLBA	Gramm-Leach-Bliley Act
GTISC	Georgia Tech Information Security Center
GTRI	Georgia Tech Research Institute
HITECH Act	Health Information Technology for Economic and Clinical Health Act
HIPAA	Health Insurance Portability and Accountability Act
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISS	Institutional Shareholder Services
IEC	International Electrotechnical Commission
IT	Information Technology
ITU	International Telecommunication Union
ITGI	Information Technology Governance Institute
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards & Technology
OIT	Office of Information Technology (Georgia Tech)
PII	Personally Identifiable Information
PwC	PricewaterhouseCoopers
R&D	Research & Development
SEC	Securities and Exchange Commission
SOD	Segregation of Duties
U.S.	United States

About Georgia Tech and GTISC

Located in Atlanta, Georgia, the Georgia Institute of Technology is a leading research university committed to improving the human condition through advanced science and technology. Ranked as the #7 best public university, Georgia Tech provides a focused, technologically based education to more than 21,500 undergraduate and graduate students.

Georgia Tech has many nationally recognized programs, all top-ranked by peers and publications alike, and is ranked in the nation's top 10 public universities by U.S. News and World Report. It is ranked:

#3, Software Engineering Institution (2007)

#6, Artificial Intelligence Program (2014)

#6, Systems Program (2014)

#8, Computer Theory Program (2014)

#9, Graduate Computer Science Program (2014)

#13, Programming Languages (2014)

The School of Computer Science is defining the foundations and advancing the frontiers of computing. Its mission is to invent the intellectual and architectural basis for computing; to educate students in the foundations and future of the field; to understand and realize the potential of computation in algorithms, systems, software, architecture, and networks; to invent and enable networks, computers, and platforms that advance our knowledge and benefit society; to educate practitioners and future leaders of computer science; and to be at the forefront of research, education, and service based on computer science.

As a leading technological university, Georgia Tech has more than 100 centers focused on interdisciplinary research that consistently contribute vital research and innovation to American government, industry, and business.

Comprised of faculty, staff, and students from multiple units across campus, the Georgia Tech Information Security Center (GTISC) is a catalyst for initiating a wide range of activities in both research and education. Members come from the College of Computing, College of Engineering, College of Business, College of Liberal Arts, the Georgia Tech Office of Information Technology (OIT) and the Georgia Tech Research Institute (GTRI).

GTISC was established in 1998, when Georgia Tech hosted the Sam Nunn Policy Forum. Developed from Senator Nunn's concept of educating citizens about important issues, the focus of the forum was the critical and strategic role of information security to the business community, to private citizens, and to all levels of government. As the program for this forum was developed, it became increasingly clear that Georgia Tech's strengths in technology and policy, coupled with the pressing need for education and research in information security, meant that the Institute had a responsibility to lead in this area.

About Jody R. Westby

Drawing upon a unique combination of more than 20 years of technical, legal, policy, and business experience, Ms. Westby provides consulting and legal services to public and private sector clients in the areas of privacy, cybersecurity, breach management and incident response, and cyber governance. Her services include trusted advisory services to boards and senior management, security risk assessments, global compliance reviews, incident response planning, data mapping, and digital asset management. Her company, Global Cyber Risk LLC, is a strategic partner of Aon Global Risk Consulting and a preferred provider of privacy and security consulting services to Reed Smith.

Ms. Westby serves as Adjunct Professor to the Georgia Institute of Technology, School of Computer Science. She authored Carnegie Mellon CyLab's 2008, 2010, and 2012 *Governance of Enterprise Security Survey* reports and was lead author of CMU's *Governing for Enterprise Security Implementation Guide*.¹ Ms. Westby's work on the governance responsibilities of boards and senior executives has been showcased by the CISO Executive Network and Bloomberg BNA's *Privacy & Security Law Report*.

Prior to founding Global Cyber Risk, Ms. Westby served as senior managing director for PricewaterhouseCoopers (PwC) where she was responsible for information security, privacy, information sharing, and critical infrastructure protection issues across the federal government. She also was co-lead in launching their outsourcing practice. Before joining PwC, Ms. Westby founded the Work-IT Group, and specialized in serving government and private sector clients on legal and regulatory issues associated with information technology and online business. Ms. Westby has advised government officials and industry in countries around the world on the development of their legal frameworks for e-commerce and information security.

Previously, Ms. Westby launched In-Q-Tel, an IT solutions/venture capital company founded by the CIA, was Senior Fellow & Director of IT Studies for the Progress & Freedom Foundation, and was Director of Domestic Policy for the U.S. Chamber of Commerce. She also practiced law with the New York firms of Shearman & Sterling and Paul, Weiss, Rifkind, Wharton & Garrison.

Ms. Westby is a professional blogger for *Forbes* on cybersecurity, cybercrime, and privacy issues. She is co-chair of the American Bar Association's (ABA) Privacy and Computer Crime Committee and was chair, co-author and editor of its *International Guide to Combating Cybercrime*, *International Guide to Cyber Security*, *International Guide to Privacy*, and *Roadmap to an Enterprise Security Program* (endorsed by the Global CSO Council). She is author of the *Legal Guide to Cybersecurity Research* and the *Legal Guide to Botnet Research*, both published by the ABA. She was editor and co-author of the 2010 UN publication, *The Quest for Cyber Peace*. Ms. Westby is co-chair of the ABA Cybercrime Committee (Criminal Justice Section) and just completed three terms on the ABA President's Cybersecurity Task Force. She served as co-chair of the World Federation of Scientists' Permanent Monitoring Panel on Information Security and was appointed to the United Nations' ITU High Level Experts Group on Cyber Security.

Ms. Westby is a member of the bars of the District of Columbia, Colorado, and Pennsylvania, and of the ABA. She received her B.A., *summa cum laude*, from the University of Tulsa and her J.D., *magna cum laude*, from Georgetown University Law Center. She is a member of the Order of the Coif, the American Bar Foundation, and the Cosmos Club.

About Financial Services Roundtable

Financial Services Roundtable (FSR) is the leading advocacy organization for America's financial services industry. With a 100-year tradition of service and accomplishment, FSR is a dynamic, forward-looking association advocating for the top financial services companies, keeping them informed on the vital policy and regulatory matters that impact their business.

FSR members include the leading banking, insurance, asset management, finance, and credit card companies in America. FSR's members are financing the American economy - creating jobs, expanding businesses, securing homes, businesses and retirement, insuring growth and building consumer confidence.

With expanding Washington involvement in the financial sector, forming relationships and engaging with public officials and policymakers is critical to helping our members see around the curve, understand policies and regulations, and provide input to help shape them.

FSR is driven at the CEO level, giving us a unique and influential voice in Washington. At every level of the government, FSR is working to ensure that our members' interests are well represented.

www.FSRoundtable.org

About Forbes

Forbes Media encompasses Forbes and Forbes.com (www.forbes.com), the leading business site on the Web that reaches on average 65 million people monthly. The company publishes Forbes, Forbes Asia and Forbes Europe, which together reach a worldwide audience of more than 6.5 million readers. It also publishes ForbesLife magazine, in addition to licensee editions in Africa, Argentina, Bulgaria, China, Croatia, Czech Republic, Estonia, Georgia, India, Indonesia, Israel, Kazakhstan, Korea, Latvia, Middle East, Poland, Romania, Russia, Slovakia, Turkey, and Ukraine.

Other Forbes Media Web sites are:

ForbesWoman.com	http://ForbesWoman.com
RealClearPolitics.com	http://RealClearPolitics.com
RealClearMarkets.com	http://RealClearMarkets.com
RealClearSports.com	http://RealClearSports.com
RealClearWorld.com	http://RealClearWorld.com

Together with Forbes.com, <http://Forbes.com>, these sites reach on average 36 million business decision makers each month.

Steve Forbes serves as Chairman and Editor in Chief. Mike Perlis is President and Chief Executive Officer. Lewis D'Vorkin is Chief Product Officer. Meredith Kopit Levien is Chief Revenue Officer.

About Palo Alto Networks

As the next-generation security company, Palo Alto Networks is leading a new era in cybersecurity by safely enabling all applications and preventing advanced threats against tens of thousands of organizations around the world. We are the fastest-growing security company in the market because of our deep expertise, commitment to innovation, and game-changing security platform. By uniquely integrating our Next-Generation Firewall, Advanced Endpoint Protection, and Threat Intelligence Cloud, we enable our customers to focus on bringing an end to the era of breaches.

Today's cybersecurity challenges

- **Lack of focus on cyber breach prevention puts critical assets at risk.** Building security that simply detects threats, with no other option than incident response, is too little, too late.
- **Security has been categorized as simply an IT problem for too long.** Cyber risks are too important *not* to discuss in the boardroom – this is an existential issue for the entire enterprise.
- **Too many point security products leave gaping holes in security postures.** Piecemeal security systems and point products that don't share context across the entire cyberattack lifecycle are inadequate.
- **Too many manual steps and cycles impede prevention and can't scale.** Most enterprise security teams are not resourced to manually handle thousands of daily alerts.

Our unique answer

The Palo Alto Networks Next-Generation Security Platform addresses these challenges by combining visibility across your network, endpoint, and cloud, with deep threat intelligence to provide automated protection and prevent cyberattacks, not just detect them. With this capability our platform enables customers to:

- **Prevent successful cyberattacks** by eliminating gaping holes in an organization's cybersecurity posture. Our platform natively provides the right security capabilities and applies them at the right place, addressing all stages of the attack lifecycle.
- **Safely enable applications and business operations** because protection is based on fine-grained visibility, correlation, and control of what matters most in today's modern computing environments: applications, users, and content, not just ports and IP addresses.
- **Eliminate the age-old compromise between security posture and business performance** that organizations have faced for years because it is natively architected to operate in modern networks with new technology initiatives such as cloud computing, software-defined data centers, and mobility in mind.

Executive Summary

It has long been recognized that directors and officers have a fiduciary duty to protect the assets of their organizations. Today, this duty extends to digital assets and has been expanded by laws and regulations that impose specific privacy and cybersecurity obligations on companies.

This is the fourth survey that Jody Westby has conducted on how boards of directors and senior management are governing the security of their organizations' information, applications, and networks (digital assets). First conducted in 2008,



2010, and 2012 for Carnegie Mellon CyLab, and now through the Georgia Tech Information Security Center (GTISC), the surveys are intended to detect trends and measure the extent to which cyber governance is improving. The 2012 and 2015 surveys are global governance surveys, enabling a comparison of responses from industry sectors and geographical regions.

“The 2015 survey shows the needle has moved, and most boards have established Risk Committees and shifted risk oversight from the Audit Committee to the Risk Committee. Additionally, boards are now undertaking key oversight activities related to governance of cybersecurity....”

The GTISC survey is based upon results received from 121 respondents at the board or senior executive level from 1,927 Forbes Global 2000 companies (6% response rate). Forty-three percent (43%) of the respondents were inside or outside directors, and the remainder of the respondents was outside non-voting attendees and senior executives. Thirty-four percent (34%) of the respondents were CEO or president, 12% were board chairs, and 46% were chief financial officers. The respondents also included strong representation from board committees: 25% of the respondents serve on a board Risk Committee, 19% serve on a Governance, Compliance, or Ethics Committee, and 14% were members of an Audit Committee. Seventy-three percent (73%) of the respondents were from critical infrastructure companies.

The three previous surveys revealed that boards were not actively managing cyber risks and failed to understand the linkage between information technology (IT) risks and enterprise risk management. The 2015 survey shows the needle has moved, and most boards have established Risk Committees and shifted risk oversight from the Audit Committee to the Risk Committee. The 2015 survey revealed that nearly two-thirds (63%) of boards are actively addressing and governing computer and information security, whereas only about a third were in previous surveys (33% in 2012, 39% in 2010). Boards are now undertaking key oversight activities related to governance of cybersecurity, such as reviewing security program assessments and top-level policies; assigning roles and responsibilities for privacy and security; and receiving regular reports on breaches and IT risks. The weakest areas of cyber governance involved reviewing security budgets and assigning roles/responsibilities for key privacy and security personnel.

The 2015 report shows a significant shift in the number of boards reviewing cyber insurance, indicating that cyber risks are being considered as an enterprise risk. The 2015 survey revealed that 48% of the respondent boards were reviewing their company's insurance for cyber-related risks, compared with 28% in 2012 and 27% in 2010. It is not certain, however, that boards know what type of insurance to purchase or know appropriate coverage limits. Only about half of the respondents (47-54%) indicated that they had quantified their business interruption and loss exposure from cyber events.

Almost all boards are reviewing risk assessments, and an increasing number of them are hiring outside experts to help with risk assessments and risk management. Ninety-three percent (93%) of the respondents indicated their boards review risk assessment reports and 53% said they hire outside experts to assist on risk issues. The highest degree of attention was being paid to cyber risks associated with supplier relationships. Sixty-three percent (63%) of respondents said their board regularly or occasionally reviewed annual security program assessments. Attention to incident response planning was high, with 74% of respondents indicating they had reviewed their company's incident response plan, but only 46% said they had participated in a test scenario of the plan.

Some of the biggest improvements over time have been organizational. Respondents indicated that 53% of boards have a Risk Committee that is separate from an Audit Committee. These results represent a significant improvement since the 2008 survey, when only 8% of boards had Risk Committees. For the first time in all four surveys, the 2015 responses indicate the Risk Committee has the most responsibility for the oversight of risk, overcoming a role previously held by Audit Committees.

Boards also are seeking more third party assistance in managing cyber and IT risks. The survey respondents from 2010-2015 indicate a clear trend in Risk and IT/Technology Committees hiring more outside expertise.

Another positive sign from the survey was the importance that boards are placing upon IT and security/risk expertise in board recruitment. Risk, security, and IT experience were ranked most valuable when recruiting for board directors, right after financial and management experience.

“Another positive sign from the survey was the importance that boards are placing upon IT and security/risk expertise in board recruitment.”

Boards and senior management are improving in establishing key positions for security and risk officers, but lag in establishing privacy positions. The survey results indicate a steady rise in the number of CISOs (73%) at respondents' companies, up from only 30% in 2008. Only about one quarter (27%) of the respondents said they have a full-time CPO, up from 7% in 2008.

Organizations tend to overlap privacy and security responsibilities, not understanding the inherent segregation of duties (SOD) issues associated with assigning responsibility for both roles to one person. More than half of the CISOs (51%) and a quarter of the CSOs (26%) indicated that they are responsible for both privacy and security. Although this is down from 77% of CISOs and 30% of CROs in 2010 having responsibility for both privacy and security, it is a risk flag. CPOs are rarely assigned security responsibilities.

Segregation of duty issues continue to be a problem in CISO/CIO reporting lines. In 2015, 40% of the respondents indicated that the CISO/CSO reported to the CIO in their organization. Twenty-two percent (22%) of the respondents indicated that the CISO/CSO reported to the CEO and 8% indicated that the CISO/CSO reported to the CFO. The surveys from 2010, 2012 and 2015 show little change in this reporting structure, and changes to establish independent reporting likely will require board action.

Another positive sign is the continued growth in cross-organizational committees or teams responsible for managing privacy and security issues across the company. In 2008, only 17% of the respondents indicated their organization had a cross-organizational team, but in 2015, 79% of the respondents said their company has formed such a committee or team.

Regional Conclusions

- North American (85%) and European (58%) boards are paying more attention to computer and information security, up from 40% and 19%, respectively, in 2012. Asia remained unchanged at 38%.
- The biggest jump in board attention to cyber insurance was in North America, where attention doubled from 35% in 2012 to 70% in 2015. Europe had a 26% increase, but Asia was rather static with only a 3% increase.
- All geographic regions had high board involvement in reviewing risk assessments (91-92%), but the North American region relied more heavily (59%) on outside experts to help with risk assessments and risk management. Asia was close behind at 54%.
- Survey respondents indicated a 35% leap in the percentage of North American boards considering cyber risks when reviewing potential major supplier relationships, putting it on par with Europe (64-62%).
- In following best practices for cyber governance, the survey results indicated that Asian boards did best in reviewing annual budgets, roles and responsibilities, and top-level policies, but North American boards excelled in reviewing risk reports, breach and incident reports, and security program assessments.
- The survey revealed that Asia was far ahead of North America and Europe in understanding the importance of having a Risk Committee separate from the board Audit Committee, with 73% of Asian respondents reporting their organization had a Risk Committee. Only 43% of North American boards and 42% of European boards had a Risk Committee separate from the Audit Committee.
- Most Asian boards have a Risk/Security Committee (98%), but North American and European boards lag behind at 48% and 58%, respectively.
- The value of risk and security experience for board service outranked IT experience in every region. The respondents indicated that North American and European boards valued risk and security expertise second only to financial and management experience. Asian respondents valued legal expertise slightly more than risk and security.
- North America and Europe are ahead of Asia in assigning key roles and responsibilities for privacy and security.
- Overlapping privacy and security responsibilities for a CISO/CSO tended to be on the decline in North America and Asia, but on the increase in Europe.
- CIO reporting remains the dominant reporting structure for CISOs/CSOs across all regions, even though it creates SOD issues. Europe is the only region to show a sizable shift from CISO/CSOs reporting to the CIO, moving from 50% in 2012 down to 33% in 2015.

- All geographic regions indicated that 65% or more organizations have a cross-organizational team.

Industry Sector Conclusions

The 2015 survey confirmed the 2012 report's finding that, overall, the financial sector has better privacy and security practices than other industry sectors. The 2015 survey indicated significant improvements in the energy/utilities and industrial sectors, which often had the lowest scores in the 2012 survey.

- The 2015 survey revealed large increases in attention to cyber issues across industry sectors. The industrial sector had the largest improvement in oversight of computer and information security, with a 37% increase over 2012 (50% v. 13%). The financial sector was close behind with a 35% increase (79% v. 44%) and energy/utilities and IT/telecom also improving with 33% increases.
- Vendor management is receiving more attention in every sector, with the financial sector leading on this issue.
- The survey revealed a substantial increase in the percentage of industrial sector boards that are reviewing risk assessments (100% in 2015, up from 63% in 2012). The energy/utilities and financial sectors rely on outside experts to help with risk assessments and risk management (62%) more than other sectors.
- The percentage of financial sector boards considering cyber risks when reviewing supplier relationships shot up to 64% from 38% in 2012. Similarly, board attention to cyber risks associated with outsourcing agreements increased in every sector except IT/telecom.
- The financial sector had the highest percentage of board involvement in every best practice area except reviewing roles and responsibilities of key privacy and security personnel. Across the board, the respondents from every sector indicated significant improvements in board governance of cybersecurity through increased activity in every best practice area.
- The financial sector far exceeds other industry sectors in having a board Risk Committee separate from the Audit Committee, with 86% of boards in that sector having a separate Risk Committee.
- Financial sector boards had more board Risk/Security Committees (98%) and IT/Technology Committees (86%) than any other sector in both the 2012 and 2015 surveys. The industrial sector was lowest with 44% of boards having a Risk/Security Committee, and the energy/utilities sector was only slightly ahead at 46%.
- Industry sectors also increased their usage of outside experts by Risk Committees, with dramatic jumps in every sector except the financial sector, which was already the leader in this area and remains so at 38%. The energy/utilities sector's Risk Committees went from 0% in 2012 to 25% in 2015.
- The energy/utilities and financial sectors place risk and security experience in a strong third place when valuing experience in the recruitment of directors, immediately following financial and management experience. The IT/telecom and Industrial sectors placed a higher priority on other areas, such as academic and scientific experience.

- The financial sector has the highest percentage (88%) of CISOs, followed closely by IT/Telecom (86%). The financial sector is the only sector to have 100% CROs, with the next closest sector being IT/Telecom at 57%. The high percentage of CPOs was in the IT/Telecom sector (64%).
- Overlapping privacy and security responsibilities in a single security role occurs in all industry sectors. Energy/utilities and industrial sectors never assign security responsibilities, however, to a CPO. All industry sectors except IT/Telecom have more than half (51-60%) of CISOs saddled with both privacy and security responsibilities. The IT/Telecom sector dropped from 78% of CISOs with dual responsibilities in 2012 to a third (33%) in 2015, whereas the industrial sector went the other way, jumping from only 25% of CISOs assigned dual responsibilities in 2012 to 60% in 2015.
- CISO/CSO reporting to the CIO is on the rise in every industry sector except energy/utilities. Only the energy/utilities and financial sectors increased the percentage of CISO/CSOs reporting to the CEO/COO between 2012 and 2015.
- At least 81% of all industry sectors had a cross-organizational team, except energy/utilities, which lagged behind at 62%.

RECOMMENDATIONS

The survey revealed that governance of enterprise security has moved considerably since the 2008, 2010, and 2012 surveys, but gaps remain in critical areas. If boards and senior management take the following 12 actions, they could significantly improve their organizations' security posture and reduce risk:

1. Establish a board Risk Committee separate from the Audit Committee and assign it responsibility for enterprise risks, including IT risks. Recruit board directors with cybersecurity, IT governance, and risk management expertise.
2. Ensure that privacy and security roles within the organization are separated and that responsibilities are appropriately assigned. The CIO, CISO/CSO, and CPO should report independently to senior management.
3. Evaluate the existing organizational structure and establish a cross-organizational team that is required to meet at least monthly to coordinate and communicate on privacy and security issues. This team should include senior management from human resources, public relations, legal, and procurement, as well as the CFO, the CIO, CISO/CSO, CRO, the CPO, and business line executives.
4. Review existing top-level policies to ensure they set a "tone from the top" and create a culture of cybersecurity and responsibility for systems and data. Organizations can enhance their reputation by valuing cybersecurity and the protection of privacy and emphasizing it as a corporate value.
5. Review assessments of the organization's cybersecurity program and ensure the program comports with best practices and standards and includes incident response, breach notification, business continuity/disaster recovery, and crisis communications plans.
6. Ensure that privacy and cybersecurity requirements for vendors (including law firms and cloud and outsource providers) are based upon key aspects of the organization's cybersecurity program

and includes annual audits and control requirements. Carefully review vendor notification procedures in the event of a breach or security incident.

7. Conduct an annual audit of the organization's enterprise cybersecurity program, to be reviewed by the Audit Committee.
8. Conduct a separate annual risk assessment of the cybersecurity program and effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed.
9. Require regular reports from senior management on the status of the cybersecurity program, remediation activities, and recent incidents.
10. Require annual board review of the budget for the cybersecurity program and its linkage to cyber risk management.
11. Ensure incident response plans are comprehensive and can address a multi-pronged attack and dovetail with business continuity/disaster recovery plans. Conduct a robust annual test of the plans, involving executives and board members.
12. Evaluate cyber risks and potential business interruption and loss exposure costs and review adequacy of cyber insurance coverage.

About the Survey

GTISC sent a personal letter signed by Gov. Tim Pawlenty, CEO of the Financial Services Roundtable, and Mark McLaughlin, CEO of Palo Alto Networks, to directors and officers of Forbes Global 2000 companies, asking them to complete a brief survey designed to help GTISC understand how boards and business leaders are managing cyber risks. Only one response per company was used in calculating response rates.

The GTISC 2015 report on *Governance of Cybersecurity* is based upon 121 responses, representing a response rate of 6% out of a total of 1,927 surveys (based on one per company), which is equivalent to the 2012 survey. Forty-one percent (41%) of the respondents are inside directors, 2% are outside directors, and 55% are non-directors, such as non-voting attendees and senior executives. Thirty-four percent (34%) of the respondents are CEO or president of their organization and 12% are board chairs. Exactly half of the respondents are senior executives, with chief financial officers comprising 38% of the respondents and corporate secretaries accounting for 6%.

Since respondents may serve on several boards, the survey asked them to select only one organization as the focus of their responses and to base all of their answers on that one organization.

The findings were analyzed according to actual responses, i.e., percentages reflect the number of participants who responded to the particular question, rather than the total number of participants.

Please note that this survey is exploratory in nature and is based on voluntary (rather than randomly selected) respondents, and that these findings do not purport to represent the entire population of directors.

GTISC and Jody Westby wish to gratefully acknowledge the assistance of Alison Hawkins, Vice President of Communications for the Financial Services Roundtable, who assisted in the finalization of this report, and Aneesh Khan, an employee of the Georgia Tech Information Security Center, who assisted in the calculation of the survey results and provided graphics assistance.

I. Introduction

PURPOSE OF THE GOVERNANCE SURVEY

This is the fourth survey conducted by Jody Westby to determine the degree to which boards and senior executives are governing privacy and security risks within their organizations. As Distinguished Fellow, Ms. Westby conducted the 2008, 2010, and 2012 surveys and reports through Carnegie Mellon CyLab. As Adjunct Professor at Georgia Tech, she conducted the 2015 survey through the Georgia Tech Information Security Center (GTISC). The surveys have remained consistent to enable the detection of trends and:

- Determine the degree to which boards and senior executives are exercising governance over cyber risks and implementing effective cyber risk strategies;
- Ascertain the board and organizational structure that is established for such governance; and
- Identify the degree to which companies are following best practices for securing their digital assets and establishing cybersecurity programs.

BACKGROUND: DUTY OF BOARDS & DIRECTORS

The governance responsibilities of directors and officers (D&Os) have been in the spotlight since 2002 with the fall of Enron and Arthur Andersen and the enactment of Sarbanes-Oxley. D&O responsibility for cyber risks emerged with certainty following the Target breach in December 2013.

Following Target, the multi-pronged attack on Sony Entertainment that resulted in (1) destruction of data, (2) disruption of networks, (3) theft of valuable intellectual property (movies), and (4) the theft and disclosure of highly confidential internal communications nearly brought Sony to its knees – the clear objective of the attackers. Other attacks since then also have intended to inflict harm upon the target.

The dependency of all organizations upon information technology (IT) systems and global networks has extended governance responsibilities to the use of IT and the protection of data and systems. So, what is IT governance? The IT Governance Institute (ITGI) states that:

IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.²

Cybersecurity governance has now evolved into an international standard. The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have developed a standard for governance of information security, ISO/IEC 27014. The standard sets out roles for both "executive management" and the "governing body." The governing body is the "person or group of people who are accountable for the performance and conformance of the organization."³ Executive management is responsible for implementing the strategies and policies set by the governing body. The standard explains what this governance means:

Governance of information security needs to align objectives and strategies for information security with business objectives and strategies, and requires compliance with legislation, regulations and contracts. It should be assessed, analyzed and implemented through a risk management approach, supported by an internal control system.⁴

It has long been recognized that D&Os have a fiduciary duty to protect the assets of their organizations.⁵ Today, this duty extends to “digital assets” – information, applications, and networks. The 1996 Delaware *Caremark Derivative Litigation* case set forth important case law regarding a board’s duty to ensure that it has adequate information flows on risks. The court noted, “a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.”⁶ The boards need to ensure they have adequate information flows and reporting on IT and cyber risks.

“It has long been recognized that D&Os have a fiduciary duty to protect the assets of their organizations. Today, this duty extends to ‘digital assets’ – information, applications, networks.”

Regulatory pressure for better IT controls began with Sarbanes-Oxley, which requires both management and external auditors to attest to the effectiveness of internal controls that provide meaningful assurance about the security of information assets.⁷ Initially, the SEC took a narrow interpretation of Sarbanes-Oxley and focused only on financial controls.⁸ In late 2011, the Securities and Exchange Commission (SEC) issued guidelines that require public companies to disclose the risk of cyber incidents if they materially affect a registrant’s products, services, relationships with customers or suppliers, or competitive conditions, or if they make an investment in the company speculative or risky.⁹ Following the Target attack, the SEC opened examinations of several companies, probing whether they had properly handled and disclosed recent cyber incidents.¹⁰ More recently, the SEC has expanded its view of security controls and surveyed investment advisors and investment funds on their cybersecurity programs. It subsequently issued guidance for these firms in April 2015 on measures to consider when addressing cybersecurity risks.¹¹

The Federal Reserve always has taken a broad view of cyber risk management, recommending reviews of all controls for cybersecurity, not just those related to financial reporting. In 2015, the Federal Reserve Board issued a Cybersecurity Assessment Tool, which incorporates principles from the Federal Financial Institution Examination Council’s (FFIEC) *Information Technology Examination Handbook*, and includes a comprehensive review of IT controls. The explanation of the Tool includes a section on “Overview for Chief Executive Officers and Boards of Directors.”¹²

The enactment of state and federal laws and regulations that impose specific privacy and security requirements on targeted industry sectors and types of data continues to grow. For example, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and state and foreign breach laws impose specific requirements pertaining to the security and privacy of data and networks and reporting of incidents.

The pressure on critical infrastructure industry sectors to secure their systems according to best practices and standards persists, with the U.S. energy sector already subject to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.¹³ In 2014, the National Institute of Standards and Technology (NIST) released a voluntary Framework for Improving Critical Infrastructure, pursuant to Executive Order 13636, which set forth recommended measures for a cybersecurity program.¹⁴

The Target breach brought D&O responsibility for governing cybersecurity front and center. Following the breach, the company's chairman, CEO, and president, Gregg Steinhafel, was dismissed by the board, and the Institutional Shareholder Services (ISS) called for the ouster of seven of the ten Target board members for failure to take appropriate actions to protect Target's data and systems.¹⁵ Although the board members were reelected, ISS's actions sent tremors through boardrooms around the globe.

Subsequently, Target shareholders filed two derivative lawsuits against the directors and officers of Target as well as the company itself, claiming that the company knew the importance of protecting customer and cardholder data and failed to take appropriate steps to prevent the breach. The claims included breach of fiduciary duty, waste of assets, gross mismanagement, and abuse of control.¹⁶ Although a similar derivative suit against Wyndham Worldwide was dismissed, Target's case and a more recent one against Home Depot remain in the courts,¹⁷ and the Seventh Circuit Court of Appeals recently reinstated a class action against Neiman-Marcus stemming from a breach, stating that "the Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objective reasonable likelihood' that such an injury will occur."¹⁸

"We have entered a new era of cybercrime; attacks are targeting companies and intending to inflict harm. Companies that do not prepare for multi-pronged attacks are at risk."

Corporate data is at a higher risk of theft or misuse than ever before, and the systemic nature of recent attacks has alarmed both industry leaders and government officials around the world. We have entered a new era of cybercrime; attacks are targeting companies and intending to inflict harm. Companies that do not prepare for multi-pronged attacks are at risk.

Managing these cyber risks now requires active oversight by boards and senior executives. Failure to properly govern cybersecurity and privacy may result in legal actions by shareholders, victims, and regulators. Although Delaware case law provides strong protections to

D&Os under the business judgment rule and recent case law,¹⁹ harm caused by security breaches *may* receive stricter scrutiny because:

- Security best practices and standards are well-developed, harmonized, and widely available;
- Many privacy and security laws require organizations to have an enterprise security program that is regularly reviewed and tested;
- The Council of Europe Convention on Cybercrime,²⁰ which has been signed by 54 countries and ratified by 47 (including the U.S.), holds companies civilly, administratively, or criminally liable for cybercrimes that benefit the company and were made possible due to the lack of supervision or control by someone in a senior management position, such as an officer or director. Article 9 of

the European Union's (EU) Council Framework Decision on attacks against information systems,²¹ which applies to all 28 EU member countries, mirrors the CoE language.

At the core of cyber governance is the very difficult issue of (1) identifying the types of attacks that could cause a material impact on the company's bottom line or operations, and (2) quantifying the impact of each type of attack. Quantification takes specialized expertise. As John Dempsey, global practice leader at Aon Global Risk Consulting, recently noted:

Risk managers regularly model and quantify the potential severity of natural catastrophes, and while there are parallels, cyber risk quantification poses unique challenges. We are now witnessing a paradigm shift in cyber loss exposure assessment. Impacts can be global in scale and affect every facet of operations. Recovery efforts can span months. Reputational losses threaten survival. Gone is the notion that a cyber-attack will cost a couple hundred bucks per breached record. We are now realizing that a single well-planned malicious attack could wipe billions from the balance sheet.²²

Turning the tide against cybercriminals will require a dedicated, coordinated, vigilant effort and comprehensive risk management strategies that must be reviewed and refined on an ongoing basis to take into account changes in the threat environment, new innovations, and new legal and operational considerations.

II. Findings & Conclusion

WHO WE ASKED

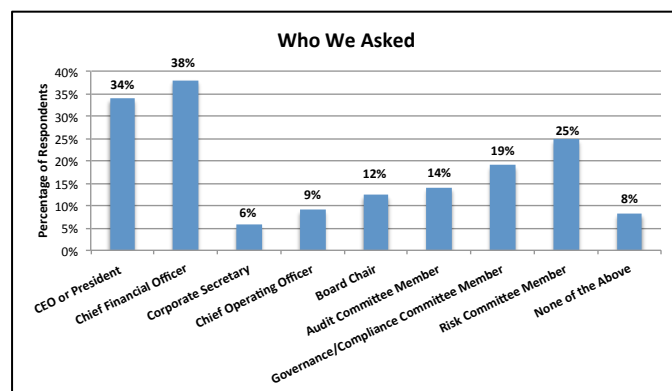
The Governance Survey respondents were almost half (43%) board members and half (54%) senior executives or non-voting attendees.

Forty-one percent (41%) of respondents were inside directors and 2% were outside directors. Twelve percent (12%) of these directors were board chairs. The respondents also indicated that:

- 14% of respondents were Audit Committee members;
- 19% of respondents were Governance, Compliance, or Ethics Committee members; and
- 25% of respondents were Risk Committee members.

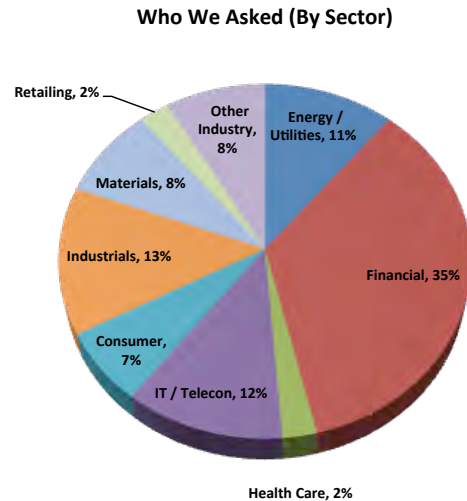
Internal respondents were:

CEO or President (34%)
CFO (38%)
COO (9%)
Corporate Secretary (6%).



The majority of the Governance Survey respondents (73%) were from critical infrastructure industry sectors, which increasingly face government pressure and/or regulatory compliance requirements with respect to the security of their IT systems and data. These survey respondents represented:

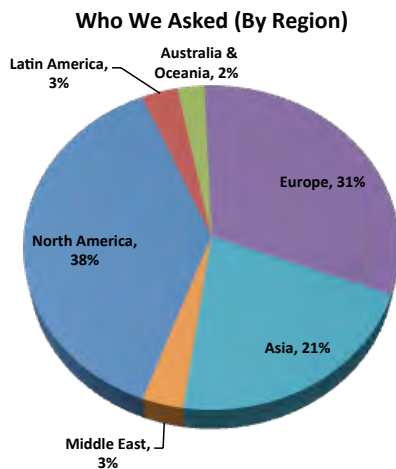
- Energy and utility companies – 11%
- Financial sector – 35%
- Health care – 2%
- Industrials – 13%
- IT and telecommunications companies – 12%.



The remaining 27% of respondents represented consumer, materials, professional services, retailing, and other types of companies.

Responses from four industry sectors had an 11% or higher response rate and are compared in this report: energy/utilities, financial, IT/telecom, and industrials.

Survey respondents represented large to very large corporations. Since the respondent pool was drawn from the Forbes Global 2000 list, the respondents represented large or very large corporations. Half (50%) of the respondents were from very large corporations with annual revenues greater than USD10 billion. Thirty-six percent (36%) of the Governance Survey respondents came from large companies with annual revenues ranging between USD2.5 billion and USD10 billion, and 12% of respondents represented companies with revenues between USD1 billion and USD2.5 billion.



Using the Forbes Global 2000 list, the 2015 survey represents the second analysis of cyber governance postures of major corporations around the world. The first global survey was conducted in 2012. Regions were aligned with those used by Internet World Stats to enable analysis of responses against Internet usage.²³ Responses were primarily from three geographical regions: North America (38%), Europe (31%), and Asia (21%), although a smaller percentage of responses also were received from Latin America, Australia and Oceania, the Middle East, and Africa. Responses from three regions are compared in this report, with key countries noted below by Internet usage:

North America: United States and Canada

Europe: EU countries, Russia, Turkey, Ukraine, and Switzerland

Asia: China, India, Japan, Indonesia, South Korea, Philippines, Vietnam, Pakistan, and Thailand.

This report analyzes and compares 2015 and 2012 results by geographic region and industry sector. These comparisons are particularly valid because the regional and industry respondent pools from the 2015 and 2012 surveys are similar.

Respondents by Geographic Region and Industry Sector

	North America	Europe	Asia	Energy/Utilities	Finance	IT/Telecom	Industrials
2015	NA 38%	EU 31%	Asia 21%	Energy/Utilities 11%	Finance 35%	IT/Telecom 12%	Industrials 13%
2012	NA 40%	EU 30%	Asia 19%	Energy/Utilities 13%	Finance 33%	IT/Telecom 12%	Industrials 15%

General survey questions may have comparisons from all four surveys (2015, 2012, 2010, 2008), but some questions were not asked in 2008, so only the last three survey responses are compared for these.

FINDINGS

Oversight & Governance

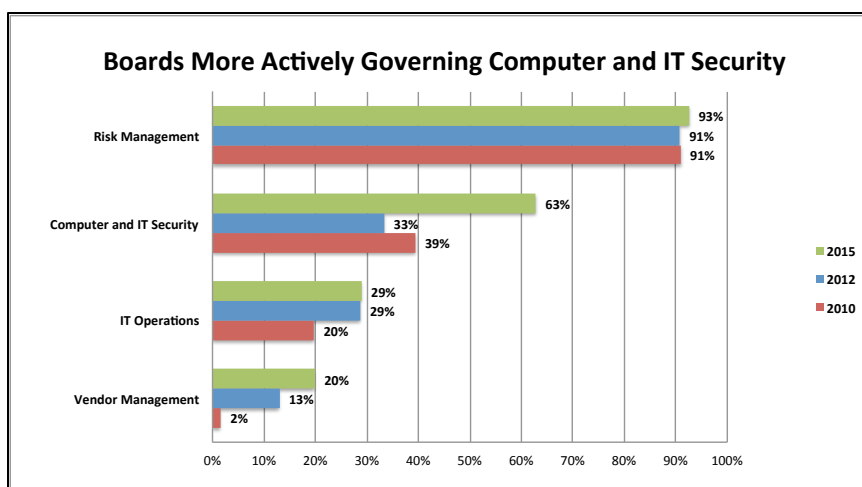
The findings from the 2015 Governance Survey indicate that boards are finally paying attention to cybersecurity issues. The 2010 and 2012 surveys showed that boards were actively addressing risk management, but attention to IT operations and computer and information security were two of the lowest ranked issues.

In 2015, the percentage of boards actively addressing and governing computer and information security nearly doubled from previous surveys. The 2015 survey revealed that nearly two-thirds (63%) of boards are actively addressing and governing computer and information security, whereas only about a third were in previous surveys (33% in 2012, 39% in 2010). Computer and information security was the fifth highest rated issue of importance to boards in 2015, only surpassed by long term strategy and operational goals, risk management, compliance, and mergers and acquisitions.

Board attention to IT operations remained fairly static: 29% of boards actively addressed and governed IT operations in 2015 and 2012 and 20% did in 2010.

The area receiving the least attention was vendor management, but this area still showed a significant increase in attention from 2% in 2010, to 13% in 2012, and to 20% in 2015. The lack of

attention to vendor management is particularly concerning since this includes cloud providers and outsourcing of IT operations and business processes.



North American and European boards are paying more attention to computer and information security, but Asia is static. Asia, however, remained unchanged at 38%.

**Regional Comparison Table:
Issues Actively Addressed
By Boards**

Issue Addressed By Boards	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
Computer & Info Sec	85%	40%	58%	19%	38%	38%
IT Operations	39%	30%	24%	19%	24%	24%
Vendor Management	28%	12%	13%	9%	19%	10%

The 2015 survey also revealed large increases in attention to cyber issues across industry sectors. The industrial sector had the largest improvement in oversight of computer and information security, with a 37% increase over 2012 (50% v. 13%). The financial sector was close behind with a 35% increase (79% v. 44%) and energy/utilities and IT/telecom also showed improvement with 33% increases. The 2015 survey also indicated that vendor management is receiving more attention in every sector, particularly energy/utilities, with a 23% increase over 2012, IT/telecom with a 15% increase, financial with a 12% increase, and industrial with a 6% increase. Boards in the financial sector pay the most attention to vendor management, with 36% of the respondent boards actively addressing this issue.

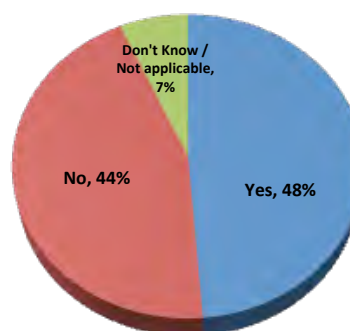
**Industry Comparison Table:
Issues Actively Addressed by Boards**

Issue Addressed By Boards	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
Computer & Info Sec	62%	29%	79%	44%	64%	31%	50%	13%
IT Operations	23%	14%	48%	36%	14%	31%	25%	19%
Vendor Management	23%	0%	36%	28%	0%	15%	6%	0%

The 2015 report shows a significant shift in the number of boards reviewing cyber insurance, indicating cyber risks are being considered as an enterprise risk.

The 2015 survey revealed that 48% of the respondent boards were reviewing their company’s insurance for cyber-related risks, compared with 28% in 2012 and 27% in 2010.

Boards Not Reviewing Insurance Coverage for Cyber Risks



The biggest jump in board attention to cyber insurance was in North America, where attention doubled from 35% in 2012 to 70% in 2015. Europe had a 26% increase (up to 45% from 19%), but Asia was rather static with only a 3% increase.

**Regional Comparison Table:
Boards Reviewing Cyber Insurance Coverage**

Boards Reviewing Cyber Insurance Coverage	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
	70%	35%	45%	19%	27%	24%

All of these critical infrastructure sectors showed a sizeable improvement in board attention to cyber insurance coverage, with the utility/energy sector showing a gain of 48%. It is surprising that the IT/telecom sector did not indicate a similar increase in board attention to this important risk area.

**Industry Comparison Table:
Boards Reviewing Cyber Insurance Coverage**

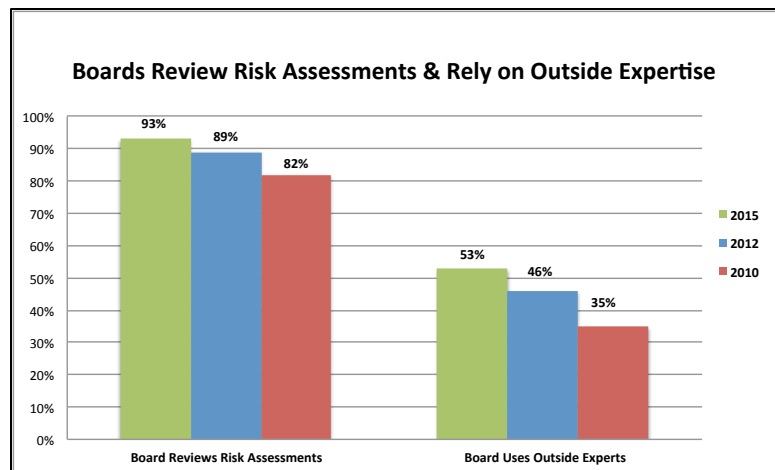
Boards Reviewing Cyber Insurance Coverage	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
	62%	14%	52%	34%	29%	15%	75%	38%

It is not certain that boards know what type of insurance to purchase or coverage limits. When asked if their company had quantified the business interruption or loss exposure from a cyber incident, 50% of the respondents said yes. The regions and industry sectors were fairly consistent in their responses to this question.

Companies Quantifying Cyber Loss Exposure & Business Interruption	North America	Europe	Asia	Energy / Utilities	Financial	IT / Telecom	Industrials
	54%	47%	50%	54%	60%	43%	44%

Almost all boards are reviewing risk assessments and an increasing number of them are hiring outside experts to help with risk assessments and risk management.

Ninety-three percent (93%) of the respondents indicated their boards reviewed risk assessment reports, compared with 89% in 2012 and 82% in 2010. Fifty-three percent (53%) said their boards used outside experts to help with risk assessments and risk management, up from 46% in 2012 and 35% in 2010. Most of this expertise was obtained from risk services (30%) and professional advisory services firms (70%).



All geographic regions had high board involvement in reviewing risk assessments, but the North American region relied more heavily on outside experts to help with risk assessments and risk management (59%) than other regions. Asia was close behind at 54%.

**Regional Comparison Table:
Boards Reviewing Risk Assessments & Obtaining Outside Expertise**

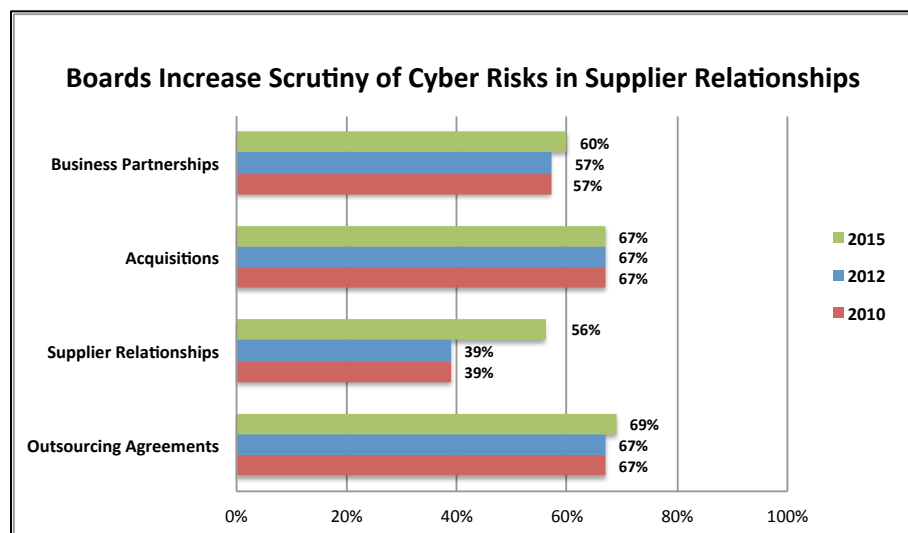
Board Risk Management	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
Reviewing Risk Assessments	91%	91%	92%	88%	92%	86%
Use Outside Experts	59%	30%	42%	47%	54%	67%

The survey revealed a substantial increase in the percentage of industrial sector boards that are reviewing risk assessments (100% in 2015, up from 63% in 2012). Energy/utilities board review of risk assessments also was 100%, but up a smaller amount from 93%. The energy/utilities and financial sectors rely on outside experts to help with risk assessments and risk management (62%) more than other sectors.

**Industry Comparison Table:
Boards Reviewing Risk Assessments & Obtaining Outside Expertise**

Board Risk Management	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
Reviewing Risk Assessments	100%	93%	93%	97%	86%	85%	100%	63%
Use Outside Experts	62%	43%	62%	64%	36%	23%	31%	38%

There was a substantial increase in board attention to cyber risks when reviewing major supplier relationships. This jumped from 39% in 2010 and 2012 to 56% in 2015. There was not much change, however, in boards considering cyber risks when reviewing potential major business partnerships, acquisitions, or outsourcing relationships.



Survey respondents indicated a 35% leap in the percentage of North American boards considering cyber risks when reviewing potential major supplier relationships, putting it on par with Europe.

Asian boards lag behind in this area at 41%.

Regional Comparison Table:

Boards Considering Cyber Risks

Boards Considering Cyber Risks When Reviewing:	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
Business Partnership	62%	35%	64%	65%	41%	76%
Acquisition	74%	65%	68%	76%	47%	53%
Supplier Relationship	62%	27%	64%	59%	41%	47%
Outsourcing Agreements	62%	62%	79%	82%	65%	59%

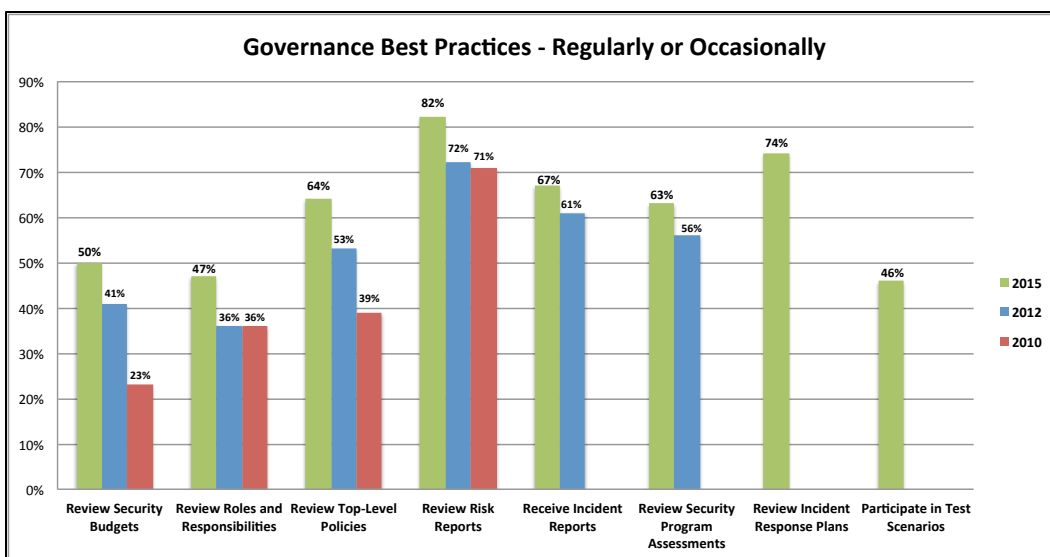
The percentage of financial sector boards considering cyber risks when reviewing supplier relationships shot up to 64% from 38% in 2012. Similarly, board attention to cyber risks associated with outsourcing agreements increased in every sector except IT/telecom. Overall, the industry sector data was harder to analyze in this area; some areas of consideration received more attention regarding cyber risks in 2015, while other went down from the 2012 survey. For example, the percentage of energy/utility boards considering cyber risks when reviewing potential major business partnerships increased by 30%, whereas the percentage of industrial sector boards doing this declined by 17%. These statistics may be more reflective of the issues that the respondent boards focused on in 2015.

Industry Comparison Table:

Boards Considering Cyber Risks

Boards Considering Cyber Risks When Reviewing:	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
Business Partnership	50%	20%	73%	73%	78%	44%	38%	55%
Acquisition	25%	40%	73%	77%	78%	56%	88%	45%
Supplier Relationship	63%	60%	64%	38%	44%	44%	38%	45%
Outsourcing Agreements	100%	80%	76%	73%	44%	67%	63%	55%

For the first time, the survey indicated that more boards regularly or occasionally engaged in every area of governance best practices related to privacy and security. Board and executive governance activities considered best practices include reviewing security budgets, designating roles and responsibilities for the management of privacy and security, developing and reviewing top-level policies, receiving regular reports on security risks and incidents, reviewing annual risk assessments of the security program, and reviewing cyber incident response plans. These activities strengthen the security posture of the company and help protect it against cyber attacks. Although there were improvements in every area across the 2010, 2012, and 2015 reports, there is still room for improvement. The weakest governance areas were reviewing annual security budgets and roles and responsibilities for privacy and security personnel; in 2012, respondents indicated more than half (53-56%) of the boards rarely or never engaged in these two activities, which are central to any security program.



When asked whether their boards receive information or are involved in activities related to these best practices, respondents indicated that boards regularly or occasionally engaged in them:

- **Review annual budgets.** Fifty percent (50%) of respondents said their board regularly or occasionally reviewed and approved annual budgets for privacy and IT security programs, up from 41% in 2012, and 23% in 2010.
- **Review roles and responsibilities.** Forty-seven percent (47%) of respondents indicated their board regularly or occasionally reviewed and approved roles and responsibilities of personnel responsible for privacy and security risks, up from 36% in 2012 and 2010.
- **Review top-level policies.** Sixty-four percent (64%) of respondents said their board regularly or occasionally reviewed and approved top-level policies regarding privacy and security risks, up from 53% in 2012 and 39% in 2010.
- **Receive reports on privacy and security risks.** Eighty-two percent (82%) of respondents said their board regularly or occasionally received reports from senior management regarding privacy and IT security risks, up from 72% in 2012 and 71% in 2010.
- **Receive reports on security breaches or loss of data.** Sixty-nine percent (69%) of respondents said their board regularly or occasionally reviewed reports of security breaches or incidents involving the disclosure of personally identifiable information or theft of corporate data, up from 61% in 2012. This question was not asked in 2010.
- **Review annual computer security program assessments.** Sixty-three percent (63%) of respondents said their board regularly or occasionally reviewed annual security program assessments, up from 56% in 2012. This question was not asked in 2010.
- **Review incident response plans and participate in test scenarios.** This was a new question for 2015. Seventy-four percent (74%) of the respondents indicated that they had reviewed their company's incident response plan, but only 46% said they had participated in a test scenario against the plan.

An analysis of the regional results indicated that Asian boards did best in reviewing annual budgets, roles and responsibilities, and top-level policies, but North American boards excelled in reviewing risk reports, breach and incident reports, and security program assessments. North American respondents also indicated significant gains in engaging in reviewing annual budgets, roles and responsibilities, and top-level policies.

**Regional Comparison Table:
Boards Regularly or Occasionally Engaging in Best Practices**

Boards Regularly or Occasionally Engaging in Best Practices	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
Review Annual Budgets	41%	14%	50%	47%	65%	67%
Review Roles & Responsibilities	48%	28%	47%	41%	58%	48%
Review Top-level Policies	59%	42%	63%	50%	81%	62%
Review Risk Reports	91%	74%	71%	69%	85%	71%
Review Security Incident & Breach Reports	70%	77%	66%	50%	54%	48%
Review Security Program Assessments	80%	58%	55%	53%	54%	48%
Review Incident Response Plans	74%	N/A	71%	N/A	85%	N/A
Participated in Test Scenario Against Response Plan	41%	N/A	50%	N/A	50%	N/A

The financial sector continues to live up to its reputation of having the best security practices. The sector had the highest percentage of board involvement in every best practice area except reviewing roles and responsibilities of key privacy and security personnel. The increased attention to cybersecurity issues is obvious when there are increases from 2012 of more than 30 percentage points. Across the board, the respondents from every sector indicated significant improvements in board governance of cybersecurity through increased activity in every best practice area.

“The increased attention to cybersecurity issues is obvious when there are increases from 2012 of more than 30 percentage points.”

**Industry Comparison Table:
Boards Regularly or Occasionally Engaging in Best Practices**

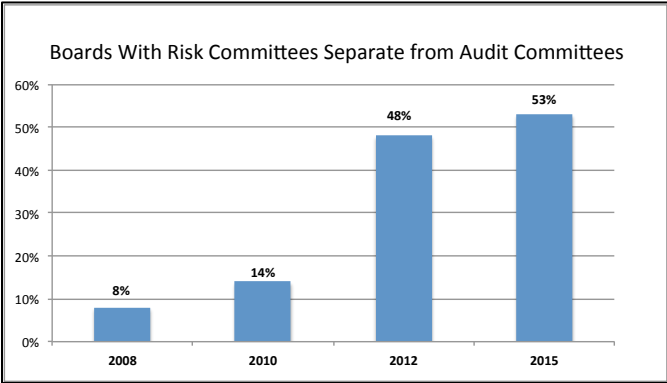
Boards Regularly or Occasionally Engaging in Best Practices	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
Review Annual Budgets	38%	29%	69%	47%	43%	38%	44%	44%
Review Roles & Responsibilities	31%	21%	50%	50%	43%	31%	56%	25%
Review Top-level Policies	54%	21%	83%	75%	50%	46%	63%	38%
Review Risk Reports	85%	71%	90%	86%	86%	69%	81%	50%
Review Security Incident & Breach Reports	77%	50%	83%	69%	86%	62%	63%	56%
Review Security Program Assessments	69%	36%	76%	78%	71%	46%	44%	50%
Review Incident Response Plans	77%	N/A	83%	N/A	79%	N/A	63%	N/A
Participated in Test Scenario Against Response Plan	39%	N/A	67%	N/A	43%	N/A	31%	N/A

Board Committee Structure

Some of the biggest improvements over time have been organizational. How a board is organized and how it assigns committee responsibilities can significantly influence the effectiveness of its management activities and security posture. Traditionally, boards have not separated risk management and audit responsibilities and established separate Risk and Audit Committees.

Respondents indicated that 53% of boards have a Risk Committee that is separate from an Audit Committee.

These results represent a significant improvement from the 2008 survey, when only 8% of boards had Risk Committees.



The survey revealed that Asia is far ahead of North America and Europe in understanding the importance of having a Risk Committee separate from the board Audit Committee.

Regional Comparison Table: Boards With Risk Committee

Boards With Risk Committee	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
	43%	35%	42%	41%	73%	78%

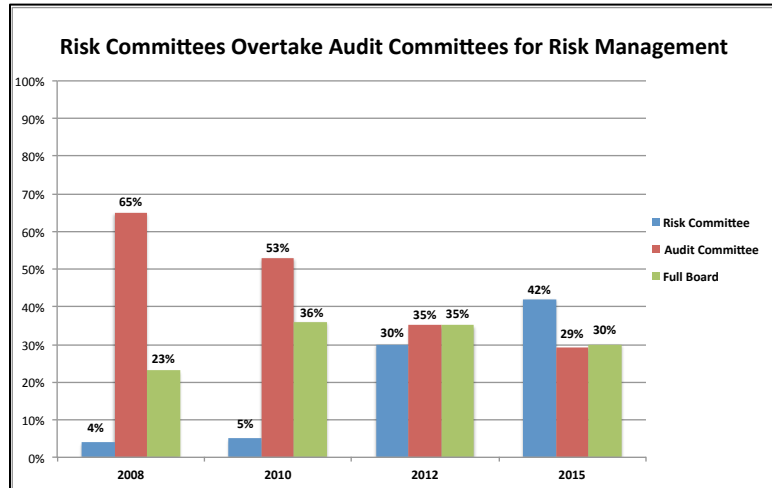
The financial sector far exceeds other industry sectors in having a board Risk Committee separate from the Audit Committee, with 86% of boards in that sector having a separate Risk Committee.

Industry Comparison Table: Boards With Risk Committee

Boards With Risk Committee	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
	23%	36%	86%	78%	43%	31%	38%	44%

The establishment of Risk Committees has led to the transfer of oversight of risk from Audit Committees to Risk Committees. For the first time in all four surveys, the 2015 responses indicate the Risk Committee has the most responsibility for the oversight of risk.

In 2008, only 4% of respondents indicated their board had assigned oversight of risk to a Risk Committee. In 2010, that increased to 5%, in 2012 it went up to 30%, and in 2015 the Risk Committee surpassed all other committees for oversight of risk at 42%. In previous surveys, the Audit Committee was the dominant committee for risk management.



Best practices and industry standards separate the audit and risk functions. The reliance upon Audit Committees to manage risk issues creates segregation of duties (SOD) issues at the board level since the same committee that exercised oversight of operational aspects of privacy and security also conducted audits in these areas. Carnegie Mellon's *Governing for Enterprise Security Implementation Guide* provides step-by-step guidance on Risk Committee responsibilities for managing IT security risks.²⁴

Asian boards are the frontrunners in assigning responsibility for risk to a Risk Committee, leading the way at 48%. It appears they shifted most responsibility from the full board to the Risk Committee, as the 15% drop in full board responsibility seems to have added 10% to the Risk Committee and 5% to the Audit Committee. For the first time, North American boards also assigned Risk Committees the most responsibility for risk issues.

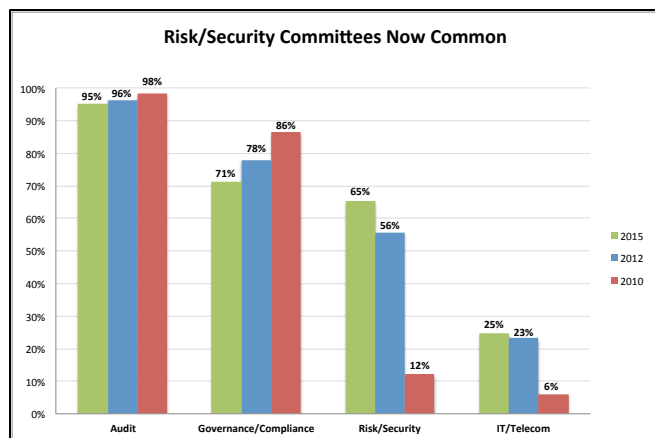
**Regional Comparison Table:
Most Responsibility for Oversight of Risk**

Most Responsibility for Oversight of Risk	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
Risk Committee	35%	23%	28%	22%	48%	38%
Audit Committee	33%	42%	36%	41%	19%	14%
Full Board	29%	33%	33%	34%	33%	48%

The financial sector leads all industry sectors, with 70% of their boards assigning the Risk Committee the most responsibility for risk matters. Energy/utilities and the IT/telecom sectors also showed significant gains in the percentage of Risk Committees having oversight of risk issues. The industrial sector, however, moved the responsibility for risk management to the full board, with 63% of these respondents indicating these issues were mostly managed at the board level.

**Industry Comparison Table:
Most Responsibility for Oversight of Risk**

Most Responsibility for Oversight of Risk	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
Risk Committee	23%	14%	70%	58%	33%	23%	19%	25%
Full Committee	38%	43%	20%	31%	13%	23%	63%	44%



There is a clear trend of board Risk/Security Committees surpassing IT/Technology Committees in getting boards' attention. When polled about the types of committees their boards have, respondents indicated that 65% of boards have a Risk/Security Committee, up from 56% in 2012 and 12% in 2010. IT/Technology Committees remained static between 2012-15, staying in the 23-25% range, but that is still an improvement over 12% in 2010.

Most Asian boards had a Risk/Security Committee, but North American and European boards lagged behind at 48% and 58%, respectively. North American boards showed a 20% gain in Risk/Security Committees between 2012 and 2015. IT/Technology Committees showed little growth, except in Europe with a 10% gain.

**Regional Comparison Table:
Boards With Risk/Security & IT/Technology Committees**

Boards With Risk/Security & IT/Tech Committees	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
Risk/Security Committee	48%	28%	58%	59%	92%	95%
IT/Tech Committee	17%	16%	32%	22%	31%	38%

Financial sector boards have more board Risk/Security Committees (98%) and IT/Technology Committees (43%) than any other sector in both the 2012 and 2015 surveys. Risk/Security Committees increased substantially in every sector.

**Industry Comparison Table:
Boards With Risk/Security & IT/Technology Committees**

Boards With Risk/Security & IT/Tech Committees	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
Risk/Security Committee	46%	36%	98%	86%	64%	46%	44%	63%
IT/Tech Committee	15%	14%	43%	39%	29%	0%	31%	12%

The survey respondents from 2010-2015 indicated a clear trend in Risk and IT/Technology Committees hiring more outside expertise. In 2015, the Risk Committee hired outside expertise 30% of the time, up from 16% in 2012 and 5% in 2010.

Risk Committees are hiring more outside expertise for risk management assistance in every region, with Asia leading at 36%. In Asia the use of outside expertise for risk management equaled that of the Compensation Committee in both 2012 and 2015. IT/Technology Committees also had an increase in the usage of outside experts, except in Asia, where respondents indicated a sharp decrease.

**Regional Comparison Table:
Boards Hiring Outside
Expertise**

Boards Hiring Outside Expertise	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
Full Board	68%	29%	50%	45%	43%	67%
Audit Committee	68%	85%	54%	50%	43%	56%
Compensation Committee	86%	91%	32%	55%	36%	33%
Gov/Compliance/Ethics Committee	29%	50%	23%	25%	14%	22%
Risk Committee	26%	18%	32%	10%	36%	33%
IT/Technology Committee	13%	3%	27%	15%	7%	22%

Industry sectors also increased their usage of outside experts by Risk Committees, with dramatic jumps in every sector except the financial sector, which already was the leader in this area and remained so at 38%. The use of outside experts by IT/Technology Committees in the industrial sector increased from 0% to 40%; other sectors also increased in this area.

**Industry Comparison Table:
Boards Hiring Outside Expertise**

Boards Hiring Outside Expertise	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
Full Board	38%	50%	65%	48%	43%	27%	50%	25%
Audit Committee	75%	80%	47%	61%	57%	73%	60%	75%
Compensation Committee	75%	90%	50%	52%	86%	64%	80%	83%
Gov/Compliance/Ethics Committee	38%	60%	26%	22%	43%	36%	30%	50%
Risk Committee	25%	0%	38%	35%	29%	9%	30%	17%
IT/Technology Committee	13%	10%	18%	13%	14%	0%	40%	0%

Fifty-nine percent (59%) of the respondents indicated that their board had an outside director with risk expertise and 23% said they had a director with cybersecurity expertise. These percentages have been generally consistent in the 2012 and 2010 surveys.

Fifty-one percent (51%) of respondents indicated that their boards retain professional search firms to seek qualified candidates for their board, which is the same percentage as the 2012 survey.

Geeks are good for boards. Risk and security and IT experience ranked most valuable when recruiting for board directors after financial and management experience. Early surveys indicated that boards favored traditional experience, such as financial, management, and legal backgrounds. The value boards are placing on directors having risk, security, or IT experience, however, has experienced steady growth since the 2010 survey, with risk and security expertise valued more than IT.



Risk and security experience outranked IT experience in every region. The respondents indicated that North American and European boards valued risk and security expertise second only to financial and management experience. Asian respondents valued legal expertise slightly more than risk and security.

**Regional Comparison Table:
Expertise Very Important or Important When Recruiting Directors**

Expertise Very Important or Important When Recruiting	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
Financial	87%	95%	87%	94%	85%	95%
Management	87%	95%	87%	97%	85%	86%
Academic	13%	12%	42%	38%	32%	52%
IT	46%	42%	42%	22%	27%	48%
Risk and Security	67%	63%	66%	56%	54%	62%
Legal	24%	37%	34%	41%	58%	81%
Scientific	26%	42%	37%	25%	19%	24%
Government	9%	9%	16%	9%	31%	33%

In 2015, the energy/utilities and financial sectors placed risk and security experience in a strong third place for importance in experience when recruiting directors, immediately following financial and management experience. The IT/telecom and Industrial sectors placed a higher priority on other areas, such as academic and scientific experience.

**Industry Comparison Table:
Expertise Very Important or
Important When Recruiting
Directors**

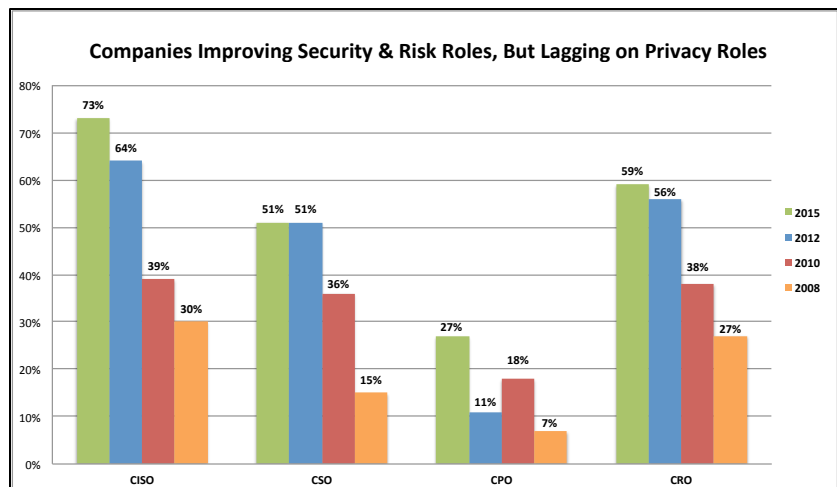
Expertise Very Important or Important When Recruiting	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
Financial	100%	86%	86%	100%	86%	92%	94%	94%
Management	100%	79%	83%	97%	86%	85%	94%	88%
Academic	31%	43%	29%	33%	57%	31%	27%	25%
IT	23%	7%	52%	42%	50%	62%	31%	31%
Risk and Security	85%	50%	76%	75%	43%	69%	50%	50%
Legal	31%	21%	43%	58%	14%	62%	38%	44%
Scientific	54%	64%	2%	11%	43%	54%	56%	0%
Government	23%	14%	12%	22%	21%	15%	19%	25%

Internal Organizational Roles & Responsibilities

Boards and senior management are improving in establishing key positions for security and risk officers, but lagging in establishing privacy positions. The survey results indicated a steady rise in the number of CISOs at respondent companies. Best practices call for clear roles and responsibilities with respect to privacy and security, with dedicated full-time personnel leading each area. The delegation of privacy and security responsibilities should serve as a check and balance and protect the company against segregation of duties (SOD) issues that can increase risk.

The various titles for personnel responsible for privacy and security were given four options on the survey: chief privacy officer (CPO), chief information security officer (CISO), chief security officer (CSO), and chief risk officer (CRO).

- Almost three-fourths (73%) of the respondents indicated that their company has a full-time CISO, up from only 30% in 2008.
- Half (51%) of the respondents said they have a CSO, up from 15% in 2008.
- Fifty-nine percent (59%) of the respondents indicated that they have a CRO, up from 27% in 2008.
- Only about one quarter (27%) of the respondents said they have a full-time CPO, up from 7% in 2008.



The management of privacy issues is concerning. ***With a patchwork of laws and regulations around the globe on privacy and increased scrutiny by regulators, it is a red flag that only one-fourth (27%) of the Forbes Global 2000 respondents indicated they have a dedicated privacy officer.*** This is not consistent with internationally accepted best practices and standards. It is possible that some respondents indicated that they did not have someone in a particular position because the person in their organization did not have that specific title. *Any organization large enough to be included in the Forbes Global 2000 list should have a dedicated CIO, CISO/CSO, CPO, and CRO.*

North America and Europe are ahead of Asia in assigning key roles and responsibilities for privacy and security, however both Asia and Europe substantially increased the percentage of CPOs between the 2012 and 2015 surveys.

**Regional Comparison Table:
CISO, CSO, CPO, CRO**

Companies with Full-time Dedicated Personnel for Role	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
CISO	78%	58%	82%	72%	46%	52%
CSO	52%	47%	66%	63%	35%	38%
CPO	33%	23%	29%	3%	23%	5%
CRO	61%	49%	61%	56%	46%	57%

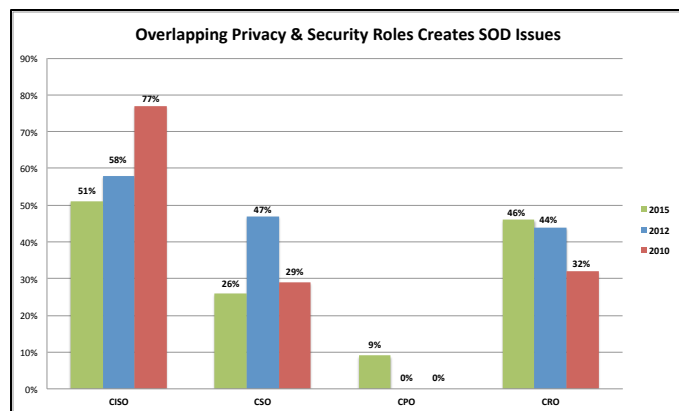
The financial sector leads in the percentage (88%) of CISOs, followed closely by IT/Telecom (86%). The financial sector is the only sector to have 100% CROs, with the next closest sector being IT/Telecom at 57%. The IT/Telecom sector had the highest percentage of CPOs (64%), which was likely due to requests for data from law enforcement and civil actions and other compliance requirements associated with its industry.

**Industry Comparison Table:
CISO, CSO, CPO, CRO**

Companies with Full-time Dedicated Personnel for Role	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
CISO	69%	50%	88%	81%	86%	69%	63%	50%
CSO	46%	57%	62%	67%	79%	79%	25%	38%
CPO	8%	7%	31%	17%	64%	0%	13%	13%
CRO	38%	57%	100%	89%	57%	54%	38%	25%

Organizations tend to overlap privacy and security responsibilities, not understanding the inherent SOD issues. It is important that privacy and security responsibilities be separated to prevent a single point of failure, which can occur (a) when security personnel do not understand compliance requirements or needed privacy controls, or (b) when privacy personnel do not understand the technical security configuration or technical controls.²⁵

The survey revealed serious SOD issues between privacy and security roles. More than half of the CISOs (51%) and a quarter of the CSOs (26%)



indicated that they were responsible for both privacy and security. Although this was down from 77% of CISOs and 30% of CROs in 2010 with responsible for both privacy and security, it is a risk flag. Since 2010, however, the surveys have indicated that CPOs rarely are assigned security responsibilities.

Privacy is much more compliance driven and few IT and security technical personnel are attorneys, so saddling the CISO/CSO with privacy responsibilities invites a compliance issue or potential reputational and financial harm to the company. **Clearly, the designation of privacy and security roles and responsibilities is an area that requires more board attention.**

Overlapping responsibilities tend to be on the decline in North America and Asia but on the increase in Europe. In North America, respondents indicated that overlapping security and privacy roles was on the decline, particularly with respect to CSO and CRO positions. The same applied to Asia, except respondents indicated 17% of CPOs had overlapping responsibilities for security. In Europe, unfortunately, there is a reverse trend, with more overlapping privacy and security responsibilities being assigned to one role.

**Regional Comparison Table:
Overlapping Privacy &
Security Responsibilities**

Role Has Responsibility For Privacy & Security	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
CISO	42%	44%	58%	48%	42%	82%
CSO	13%	35%	40%	40%	22%	62%
CPO	0%	0%	18%	0%	17%	0%
CRO	25%	48%	70%	22%	33%	67%

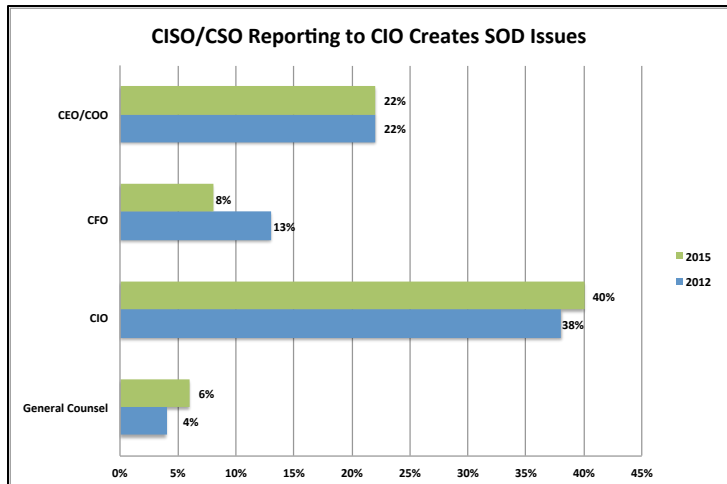
Overlapping privacy and security responsibilities in a single security role occurs in all industry sectors. CISOs, CSO, and CROs have responsibility for both privacy and security at a much higher rate than CPOs. Energy/utilities and industrial sectors never assign security responsibilities, however, to a CPO. All industry sectors except IT/Telecom had more than half (51-60%) of CISOs saddled with both privacy and security responsibilities. The IT/Telecom sector dropped from 78% of CISOs with dual responsibilities in 2012 to a third (33%) in 2015.

**Industry Comparison Table:
Overlapping Privacy &
Security Responsibilities**

Role Has Responsibility For Privacy & Security	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
CISO	56%	43%	51%	76%	33%	78%	60%	25%
CSO	33%	38%	35%	63%	18%	67%	25%	33%
CPO	0%	0%	8%	0%	11%	0%	0%	0%
CRO	0%	0%	57%	56%	38%	86%	17%	0%

There also are SOD issues in reporting lines when CISOs/CSOs report to chief information officers (CIOs), because the CIO then controls the budget for the security program and may override security configuration decisions or policies in favor of his/her own infrastructure architecture preferences, thereby compromising security. In addition, the CIO may interfere with security procurements by favoring certain vendors or products without understanding the technological security differences between the products.

Although such reporting relationships are against best practices, in 2015, 40% of the respondents indicated that the CISO/CSO reported to the CIO in their organization. Twenty-two percent (22%) of the respondents indicated that the CISO/CSO reported to the CEO and 8% indicated that the CISO/CSO reported to the CFO. The surveys from 2010, 2012 and 2015 show little change in this reporting structure, and independent reporting lines likely will require board action.



CIO reporting remains the dominant reporting structure for CISOs/CSOs across all regions. Although the Asian respondents indicated a preference for the CISO/CSO reporting to the CEO in 2012, that has reversed with the percentage dropping from 57% to 19%. Likewise, in 2012, the North American respondents indicated that the CFO was a favored second choice for CISO/CSO reporting, but that dropped from 23% in 2012 to 9% in 2015. Europe is the only region to show a sizable shift from CISO/CSOs reporting to the CIO, moving from 50% in 2012 to 33% in 2015.

**Regional Comparison Table:
CISO/CSO Reporting Structure**

CISO/CSO Reports to	2015 North America	2012 North America	2015 Europe	2012 Europe	2015 Asia	2012 Asia
CEO/COO	15%	5%	33%	13%	19%	57%
CFO	9%	23%	10%	3%	7%	5%
CIO	51%	44%	33%	50%	26%	19%
General Counsel	4%	9%	10%	0%	4%	0%

Likewise, CISO/CSO reporting to the CIO is on the rise in every industry sector except energy/utilities. Only the energy/utilities and financial sectors increased the percentage of CISO/CSOs reporting to the CEO/COO between 2012 and 2015. In 2015, the IT/Telecom sector respondents dramatically reduced the percentage of CISO/CSOs reporting to CEOs from 54% to 29%. *The industrial sector jumped from 25% of CISO/CSOs reporting to CIOs in 2012 to 47% in 2015.* Having the CISO/CSO report to the CFO appears to be falling out of favor in every sector except energy/utilities.

**Industry Comparison Table:
CISO/CSO Reporting Structure**

CISO/CSO Reports to	2015 Energy/Utilities	2012 Energy/Utilities	2015 Finance	2012 Finance	2015 IT/Telecom	2012 IT/Telecom	2015 Industrial	2012 Industrial
CEO/COO	21%	7%	30%	28%	29%	54%	6%	19%
CFO	21%	14%	2%	3%	7%	8%	12%	44%
CIO	43%	50%	47%	42%	29%	15%	47%	25%
General Counsel	7%	0%	2%	3%	7%	0%	12%	6%

Organizations are showing significant gains in cross-organizational communication.

One of the most significant improvements from the results of the four Governance Surveys is in the establishment of internal cross-organizational groups for communicating about privacy and security issues.

- In 2008, only 17% of the respondents indicated that their organizations had a cross-organizational team
- In 2010, 65% of the organizations did;
- In 2012, 72% of the respondents indicated that such a committee had been established, and
- In 2015, 79% of the respondents had a cross-organizational committee or team.

This is very encouraging and indicates that companies are learning that cross-organizational communication is essential to addressing insider threats, combating external attacks, closing governance gaps, and reducing legal liability.

The benefit of cross-organizational committees is realized across the globe; all geographic regions indicated that 65% or more organizations had a cross-organizational team. At least 81% of all industry sectors have a cross-organizational team, except energy/utilities, which lags behind at 62%.

Organizations with cross-Organizational committee	North America	Europe	Asia	Energy / Utilities	Financial	IT / Telecom	Industrials
	91%	76%	65%	61%	86%	86%	81%

CONCLUSIONS

The following conclusions can be drawn from the findings of the 2015 GTISC Governance Survey:

- In 2015, the percentage of boards actively addressing and governing computer and information security nearly doubled from previous surveys. The 2015 survey revealed that nearly two-thirds (63%) of boards are actively addressing and governing computer and information security, whereas only about a third were in previous surveys (33% in 2012, 39% in 2010).
- The 2015 report shows a significant shift in the number of boards reviewing cyber insurance, indicating cyber risks are being considered as an enterprise risk. The 2015 survey revealed that 48% of the respondent boards were reviewing their company’s insurance for cyber-related risks, compared with 28% in 2012 and 27% in 2010.
- It is not certain that boards know what type of insurance to purchase or appropriate coverage limits. Only about half of the respondents (47-54%) indicated they had quantified their business interruption and loss exposure from cyber events.
- Almost all boards are reviewing risk assessments and an increasing number of them are hiring outside experts to help with risk assessments and risk management. Ninety-three percent (93%) of the respondents indicated their boards review risk assessment reports and 53% said they hire outside experts to assist on risk issues.
- There was a substantial increase in board attention to cyber risks when reviewing major supplier relationships. This jumped from 39% in 2010 and 2012 to 56% in 2015. There was not much

change, however, in boards considering cyber risks when reviewing potential major business partnerships, acquisitions, or outsourcing relationships.

- For the first time, the 2015 survey shows that more boards are regularly or occasionally engaging in every area of governance best practices related to the governance of privacy and security. The weakest areas of oversight continue to be reviewing annual security budgets and assigning roles and responsibilities for personnel responsible for these areas.
- Sixty-three percent (63%) of respondents said their board regularly or occasionally reviewed annual security program assessments. Attention to incident response planning was high, with 74% of respondents indicating they had reviewed their company's plan, but only 46% said they had participated in a test scenario of the plan.
- Some of the biggest improvements over time have been organizational. Respondents indicated that 53% of boards have a Risk Committee that is separate from an Audit Committee. These results represented a significant improvement since the 2008 survey, when only 8% of boards had Risk Committees.
- The establishment of Risk Committees has led to the transfer of oversight of risk from Audit Committees to Risk Committees. For the first time in all four surveys, the 2015 responses indicate the Risk Committee has the most responsibility for the oversight of risk, overcoming a role previously held by Audit Committees. In 2008, only 4% of respondents indicated their board had assigned oversight of risk to a Risk Committee. In 2010, that increased to 5%, in 2012 it went up to 30%, and in 2015 the Risk Committee surpassed all other committees for oversight of risk at 42%.
- There is a clear trend of board Risk/Security Committees (65%) surpassing IT/Technology Committees (23-25%) in getting boards' attention; in 2010 only 12% of boards had Risk/Security and IT/Technology Committees.
- The survey respondents from 2010-2015, however, indicate a clear trend in Risk and IT/Technology Committees hiring more outside expertise.
- Fifty-nine percent (59%) of the respondents indicated that their board had an outside director with risk expertise and 23% said they had a director with cybersecurity expertise.
- Risk and security and IT experience ranked most valuable when recruiting for board directors after financial and management experience.
- Boards and senior management are improving in establishing key positions for security and risk officers, but lag in establishing privacy positions. The survey results indicated a steady rise in the number of CISOs (73%) at respondents' companies, up from only 30% in 2008. Only about one quarter (27%) of the respondents said they have a full-time CPO, up from 7% in 2008.
- Organizations tend to overlap privacy and security responsibilities, not understanding the inherent SOD issues. More than half of the CISOs (51%) and a quarter of the CSOs (26%) indicated that they are responsible for both privacy and security. Although this is down from 77% of CISOs and 30% of CROs in 2010 with responsible for both privacy and security, it is a risk flag. CPOs are rarely assigned security responsibilities.
- In 2015, 40% of the respondents indicated that the CISO/CSO reported to the CIO in their organization. Twenty-two percent (22%) of the respondents indicated that the CISO/CSO

reported to the CEO and 8% indicated that the CISO/CSO reported to the CFO. The surveys from 2010, 2012 and 2015 show little change in this reporting structure, and changes to require independent reporting likely will require board action.

- Organizations are showing significant gains in cross-organizational committees or teams, up from 17% in 2008 to 79% in 2015.

Regional Conclusions

- North American (85%) and European (58%) boards are paying more attention to computer and information security, up from 40% and 19%, respectively, in 2012. Asia remained unchanged at 38%.
- The biggest jump in board attention to cyber insurance was in North America, where attention doubled from 35% in 2012 to 70% in 2015. Europe had a 26% increase, but Asia was rather static with only a 3% increase.
- All geographic regions had high board involvement in reviewing risk assessments (91-92%), but the North American region relied more heavily (59%) on outside experts to help with risk assessments and risk management. Asia was close behind at 54%.
- Survey respondents indicated a 35% leap in the percentage of North American boards considering cyber risks when reviewing potential major supplier relationships, putting it on par with Europe (64-62%).
- In following best practices for cyber governance, the survey results indicated that Asian boards did best in reviewing annual budgets, roles and responsibilities, and top-level policies, but North American boards excelled in reviewing risk reports, breach and incident reports, and security program assessments.
- The survey revealed that Asia was far ahead of North America and Europe in understanding the importance of having a Risk Committee separate from the board Audit Committee, with 73% of Asian respondents reporting their organization had a Risk Committee. Only 43% of North American boards and 42% of European boards had a Risk Committee separate from the Audit Committee.
- Most Asian boards have a Risk/Security Committee (98%), but North American and European boards lag behind at 48% and 58%, respectively.
- The value of risk and security experience for board service outranked IT experience in every region. The respondents indicated that North American and European boards valued risk and security expertise second only to financial and management experience. Asian respondents valued legal expertise slightly more than risk and security.
- North America and Europe are ahead of Asia in assigning key roles and responsibilities for privacy and security.
- Overlapping privacy and security responsibilities for a CISO/CSO tended to be on the decline in North America and Asia, but on the increase in Europe.

- CIO reporting remains the dominant reporting structure for CISOs/CSOs across all regions, even though it creates SOD issues. Europe is the only region to show a sizable shift from CISO/CSOs reporting to the CIO, moving from 50% in 2012 down to 33% in 2015.
- All geographic regions indicated that 65% or more organizations have a cross-organizational team.

Industry Sector Conclusions

The 2015 survey confirmed the 2012 report's finding that, overall, the financial sector has better privacy and security practices than other industry sectors. The 2015 survey indicated significant improvements in the energy/utilities and industrial sectors, which often had the lowest scores in the 2012 survey.

- The 2015 survey revealed large increases in attention to cyber issues across industry sectors. The industrial sector had the largest improvement in oversight of computer and information security, with a 37% increase over 2012 (50% v. 13%). The financial sector was close behind with a 35% increase (79% v. 44%) and energy/utilities and IT/telecom also improving with 33% increases.
- Vendor management is receiving more attention in every sector, with the financial sector leading on this issue.
- The survey revealed a substantial increase in the percentage of industrial sector boards that are reviewing risk assessments (100% in 2015, up from 63% in 2012). The energy/utilities and financial sectors rely on outside experts to help with risk assessments and risk management (62%) more than other sectors.
- The percentage of financial sector boards considering cyber risks when reviewing supplier relationships shot up to 64% from 38% in 2012. Similarly, board attention to cyber risks associated with outsourcing agreements increased in every sector except IT/telecom.
- The financial sector had the highest percentage of board involvement in every best practice area except reviewing roles and responsibilities of key privacy and security personnel. Across the board, the respondents from every sector indicated significant improvements in board governance of cybersecurity through increased activity in every best practice area.
- The financial sector far exceeds other industry sectors in having a board Risk Committee separate from the Audit Committee, with 86% of boards in that sector having a separate Risk Committee.
- Financial sector boards had more board Risk/Security Committees (98%) and IT/Technology Committees (86%) than any other sector in both the 2012 and 2015 surveys. The industrial sector was lowest with 44% of boards having a Risk/Security Committee, and the energy/utilities sector was only slightly ahead at 46%.
- Industry sectors also increased their usage of outside experts by Risk Committees, with dramatic jumps in every sector except the financial sector, which was already the leader in this area and remains so at 38%. The energy/utilities sector's Risk Committees went from 0% in 2012 to 25% in 2015.

- The energy/utilities and financial sectors place risk and security experience in a strong third place when valuing experience in the recruitment of directors, immediately following financial and management experience. The IT/telecom and Industrial sectors placed a higher priority on other areas, such as academic and scientific experience.
- The financial sector has the highest percentage (88%) of CISOs, followed closely by IT/Telecom (86%). The financial sector is the only sector to have 100% CROs, with the next closest sector being IT/Telecom at 57%. The high percentage of CPOs was in the IT/Telecom sector (64%).
- Overlapping privacy and security responsibilities in a single security role occurs in all industry sectors. Energy/utilities and industrial sectors never assign security responsibilities, however, to a CPO. All industry sectors except IT/Telecom have more than half (51-60%) of CISOs saddled with both privacy and security responsibilities. The IT/Telecom sector dropped from 78% of CISOs with dual responsibilities in 2012 to a third (33%) in 2015, whereas the industrial sector went the other way, jumping from only 25% of CISOs assigned dual responsibilities in 2012 to 60% in 2015.
- CISO/CSO reporting to the CIO is on the rise in every industry sector except energy/utilities. Only the energy/utilities and financial sectors increased the percentage of CISO/CSOs reporting to the CEO/COO between 2012 and 2015.
- At least 81% of all industry sectors had a cross-organizational team, except energy/utilities, which lagged behind at 62%.

III. Recommendations

The survey revealed that governance of enterprise security has moved considerably since the 2008, 2010, and 2012 surveys, but gaps remain in critical areas. If boards and senior management take the following 12 actions, they could significantly improve their organizations' security posture and reduce risk:

1. Establish a board Risk Committee separate from the Audit Committee and assign it responsibility for enterprise risks, including IT risks. Recruit board directors with cybersecurity, IT governance, and risk management expertise.
2. Ensure that privacy and security roles within the organization are separated and that responsibilities are appropriately assigned. The CIO, CISO/CSO, and CPO should report independently to senior management.
3. Evaluate the existing organizational structure and establish a cross-organizational team that is required to meet at least monthly to coordinate and communicate on privacy and security issues. This team should include senior management from human resources, public relations, legal, and procurement, as well as the CFO, the CIO, CISO/CSO, CRO, the CPO, and business line executives.
4. Review existing top-level policies to ensure they set a "tone from the top" and create a culture of cybersecurity and responsibility for systems and data. Organizations can enhance their reputation by valuing cybersecurity and the protection of privacy and emphasizing it as a corporate value.

5. Review assessments of the organization's cybersecurity program and ensure the program comports with best practices and standards and includes incident response, breach notification, business continuity/disaster recovery, and crisis communications plans.
6. Ensure that privacy and cybersecurity requirements for vendors (including law firms and cloud and outsource providers) are based upon key aspects of the organization's cybersecurity program and includes annual audits and control requirements. Carefully review vendor notification procedures in the event of a breach or security incident.
7. Conduct an annual audit of the organization's enterprise cybersecurity program, to be reviewed by the Audit Committee.
8. Conduct a separate annual risk assessment of the cybersecurity program and effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed.
9. Require regular reports from senior management on the status of the cybersecurity program, remediation activities, and recent incidents.
10. Require annual board review of the budget for the cybersecurity program and its linkage to cyber risk management.
11. Ensure incident response plans are comprehensive and can address a multi-pronged attack and dovetail with business continuity/disaster recovery plans. Conduct a robust annual test of the plans, involving executives and board members.
12. Evaluate cyber risks and potential business interruption and loss exposure costs and review adequacy of cyber insurance coverage.

Endnotes

¹ Jody R. Westby & Julia Allen, *Governing for Enterprise Security Implementation Guide*, Carnegie Mellon University, Software Engineering Institute, Technical Note CMU/SEI-2000-TN-020, 2007, http://www.sei.cmu.edu/publications/documents/07_reports/07tn020.html (hereinafter “Westby & Allen”).

² *Board Briefing on IT Governance*, 2nd ed., IT Governance Institute, 2003 at 10, <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx> (emphasis added).

³ International Organization for Standardization & International Electro technical Commission, *Governance of Information Security*, ISO/IEC 27014 (2013), Section 3.2, <https://www.iso.org/obp/ui/#iso:std:iso-iec:27014:ed-1:v1:en> (hereinafter “ISO/IEC 27014”).

⁴ ISO/IEC 27014 at section 4.1.

⁵ See Jody R. Westby, *Testimony Before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census*, Sept. 22, 2004, <http://www.cccure.org/Documents/Governance/westby1.pdf>. For a discussion regarding the fiduciary duty of boards and officers and the extension of that duty to protect the digital assets of their organizations, see Jody R. Westby, ed., *International Guide to Cyber Security*, American Bar Assn., Privacy & Computer Crime Committee, 2004 at 189-93.

⁶ *In re Caremark Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996), <http://www.wlrk.com/docs/INRECAREMARKINTERNATIONALINCDERIVATIVELITIGATION.pdf>.

⁷ Sarbanes-Oxley Act of 2002, Pub. Law 107-204, Sections 302, 404, <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>.

⁸ See, “Commission Guidance Regarding Management’s Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934,” 17 CFR Part 241, June 27, 2007 at 4-5, <https://www.sec.gov/rules/interp/2007/33-8810.pdf>.

⁹ “CF Disclosure Guidance: Topic 2, Cybersecurity,” Securities and Exchange Commission, Division of Corporate Finance, Oct. 13, 2011, <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

¹⁰ David Michaels, “Hacked Companies Face SEC Scrutiny Over Disclosure,” *BloombergBusiness*, July 7, 2014, <http://www.bloomberg.com/news/articles/2014-07-02/hacked-companies-face-sec-scrutiny-over-disclosure>.

¹¹ “Cybersecurity Guidance, U.S. Securities and Exchange Commission, Division of Investment Management, April, 2015, <http://www.sec.gov/investment/im-guidance-2015-02.pdf>.

¹² FFIEC Cybersecurity Assessment Tool, “Overview for Chief Executive Officers and Boards of Directors,” <http://www.ffiec.gov/cyberassessmenttool.htm>.

¹³ North American Electric Reliability Corporation, CIP Standards, <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx> .

¹⁴ Cybersecurity Framework, National Institute of Standards and Technology, <http://www.nist.gov/cyberframework/>.

¹⁵ Paul Ziabro and Joanne S. Lublin, “ISS’s View on Target Directors Is a Signal on Cybersecurity,” *The Wall Street Journal*, May 28, 2014, <http://www.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278>; see also Elizabeth A. Harris, “Advisory Group Opposes Re-election of Most of Target’s Board,” *The New York Times*, May 28, 2014, http://www.nytimes.com/2014/05/29/business/advisory-group-opposes-re-election-of-most-of-targets-board.html?_r=0.

¹⁶ Kevin LaCroix, “Target Directors and Officers Hit with Derivative Suits Based on Data Breach,” Feb. 3, 2014, <http://www.dandodiary.com/2014/02/articles/cyber-liability/target-directors-and-officers-hit-with-derivative-suits-based-on-data-breach/>.

¹⁷ Kevin LaCroix, “Dismissal Granted in Cyber Breach-Related Derivative Suit Filed Against Wyndham Officials,” Oct. 21, 2014, <http://www.dandodiary.com/2014/10/articles/cyber-liability/dismissal-granted-in-cyber-breach-related-derivative-suit-filed-against-wyndham-officials/>.

¹⁸ “Data Breach Plaintiffs Have Standing Against Neiman-Marcus,” PRWeb News Release, Sept. 13, 2015, <http://www.prweb.com/releases/2015/07/prweb12859656.htm>.

¹⁹ In re *Citigroup Inc. Shareholder Derivative Action*, No. 3338-CC, 2009 WL 481906 (Del. Ch. Feb. 24, 2009), [http://www.delawarelitigation.com/uploads/file/int99\(1\).pdf](http://www.delawarelitigation.com/uploads/file/int99(1).pdf) ; *Stone v. Ritter*, 911 A.2d 362, 366–67 (Del. 2006), <http://caselaw.lp.findlaw.com/data2/delawarestatecases/93-2006.pdf>.

²⁰ Council of Europe *Convention on Cybercrime* – Budapest, 23.XI.2001 (ETS No. 185) (2002), <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>, Council of Europe *Convention on Cybercrime Explanatory Report*, Nov. 8, 2001, <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

²¹ *Proposal for a Council Framework Decision on attacks against information systems*, Commission of the European Communities, Article 9, Apr. 19, 2002, COM(2002) 173 final, 2002/0086 (CNS), <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52002PC0173>; see also *Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, Explanatory Memorandum, European Commission, COM(2010) 517, http://ec.europa.eu/dgs/home-affairs/policies/crime/1_en_act_part1_v101.pdf.

²² Email from John D. Dempsey to Jody R. Westby, Sept. 6, 2015, 11:42 a.m. Disclosure: The author's firm, Global Cyber Risk LLC, is a strategic partner of Aon Global Risk Consulting, and the two companies jointly offer a service evaluating cybersecurity programs and quantifying cyber risks.

²³ See Internet World Stats, <http://www.internetworldstats.com>.

²⁴ Westby & Allen at 57-58.

²⁵ For a full discussion on the appropriate assignment of roles and responsibilities for all organizational personnel and boards of directors, see Westby and Allen at 19-31, Appendix C.