

CarnegieMellon

Carnegie Mellon

CyLab

CONFIDENCE FOR A NETWORKED WORLD



## Governance of Enterprise Security Survey: CyLab 2008 Report

Published by: Carnegie Mellon CyLab

**Authors:**

Jody R. Westby  
Adjunct Distinguished Fellow, CyLab  
CEO, Global Cyber Risk LLC

Richard Power  
Distinguished Fellow, CyLab

December 1, 2008

© 2008 by Carnegie Mellon University & Jody R. Westby  
All rights reserved. No part of the contents hereof may be reproduced in any form without the prior  
written consent of the copyright owners.

**Carnegie Mellon CyLab**

Carnegie Mellon University  
5000 Forbes Avenue  
Pittsburgh, PA 15213

(412) 268-5090 • (412) 268-7675 (Fax)

Dean, College of Engineering & Founder / Director, CyLab, Pradeep K. Khosla, Ph.D.

Distinguished Fellow, Richard Power

Adjunct Distinguished Fellow, Jody R. Westby

**Jody R. Westby, Esq.**

CEO

Global Cyber Risk LLC  
5125 MacArthur Blvd., NW  
Third Floor

Washington, DC 20016

(202) 537-5070 • (202) 537-5073

## Acknowledgement and Disclaimer

This report was created using raw data collected by the National Association of Corporate Directors (“NACD”) for its 2008 Public Company Governance Survey. NACD did not provide analysis for this Carnegie Mellon CyLab (“CyLab”) report and had no role in preparing this final report, which reflects only the views of CyLab. The NACD did grant CyLab permission to use the raw data. CyLab appreciates the cooperation of NACD.

## Table of Contents

Abbreviations.....	v
About Carnegie Mellon CyLab .....	vi
Executive Summary .....	1
About the Survey.....	3
I. Introduction.....	4
Purpose of the Governance Survey .....	4
Background: Duty of Boards & Directors .....	4
II. Findings and Conclusions .....	6
Who We Asked .....	6
Findings .....	7
Conclusions .....	11
III. Recommendations.....	12
Endnotes .....	13
Bibliography & Additional References.....	15
Bibliography .....	15
Additional References.....	16

## Abbreviations

ASIS	American Society for Industrial Security
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CoE	Council of Europe
CPO	Chief Privacy Officer
CRO	Chief Risk Officer
CSO	Chief Security Officer
CyLab	Carnegie Mellon CyLab
D&Os	Directors & Officers
EU	European Union
FDA	Food and Drug Administration
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
ISACA	Information Systems Audit and Control Association
ISSA	Information Systems Security Association
IT	Information Technology
ITGI	Information Technology Governance Institute
NACD	National Association of Corporate Directors
PII	Personally Identifiable Information
R&D	Research & Development
RMP	Risk Management Plan
SEC	Securities and Exchange Commission
SOD	Segregation of Duties
U.S.	United States
X-Team	Cross-organizational privacy and security team

## About Carnegie Mellon CyLab

Carnegie Mellon CyLab is the largest university-based research and education center for computer and network security, information security, and software assurance. CyLab is located in the College of Engineering at Carnegie Mellon University and has U.S. campuses in Silicon Valley and Pittsburgh. Foreign campuses are located in Greece, Japan, Portugal, and South Korea.

Recognizing that technology issues today are increasingly impacted by legal/regulatory requirements and operational considerations, CyLab leverages its cross-university involvement with faculty, researchers, and students from Carnegie Mellon's:

- Information Networking Institute;
- Electrical and Computer Engineering Department;
- Engineering and Public Policy Department;
- School of Computer Science;
- Software Engineering Institute;
- Tepper School of Business;
- Statistics Department; and
- H. John Heinz III College

CyLab also brings in first-tier governance, legal, and policy expertise through its Distinguished Fellows. The CyLab research team includes over fifty faculty researchers and over one hundred graduate students.

CyLab is a bold and visionary effort, which establishes public-private partnerships for the research and development (“R&D”) of new technologies for sustainable, resilient, and trustworthy computing and communications systems. With this Governance Survey, CyLab extends the university’s sphere of influence to the governance of enterprise security by boards of directors and senior management.<sup>1</sup>

## Executive Summary

It has long been recognized that directors and officers have a fiduciary duty to protect the assets of their organization. Today, this duty extends to digital assets, and has been expanded by laws and regulations that impose specific privacy and cyber security obligations on companies. The Council of Europe Convention on Cybercrime, which the U.S. has signed and ratified, may subject executives to criminal, administrative, and civil penalties for failure to adequately supervise the security of company computer systems. Shareholder derivative suits are also a possible reaction to drops in stock price or loss of market share caused by cyber breaches where boards and directors appear to have given inadequate attention to the governance of information technology (“IT”) systems.



---

**“The respondents indicated that the vast majority of boards that were reviewing privacy and security issues were not focusing on important activities that could help protect the organization from high risk areas....”**

---

Carnegie Mellon CyLab initiated a study to measure the degree of governance afforded by boards of directors and senior management to the security of their organizations’ information, applications, and networks. The CyLab 2008 report on its *Governance of Enterprise Security Survey* (“Governance Survey”) is based upon data received from 703 individuals serving on U.S.-listed public company boards. More than two-thirds of the respondents were serving as outside board directors, with the remainder of respondents representing inside directors and non-voting board attendees (including senior management, general counsels, and corporate secretaries).

The Survey revealed that boards are taking risk management seriously, but there is still a gap in understanding the linkage between IT and enterprise risk management. Survey results confirmed the belief among

IT security professionals that boards and senior executives are not adequately involved in key areas related to the governance of enterprise security. Of the pool of respondents, only 36% of them indicated that their board had direct involvement with oversight of information security.

There are a number of best practices for board involvement with respect to IT governance, but the survey results indicated that boards are only occasionally or rarely involved in activities related to these best practices. Thus, boards face a learning curve in exercising governance and need to understand what activities serve as good governance control points. The respondents indicated that the vast majority of boards that are reviewing privacy and security issues are not focusing on important activities that could help protect the organization from high risk areas, such as reputational or financial losses flowing from breaches of personally identifiable information.

The Governance Survey also indicated that boards are overly reliant upon Audit Committees to manage IT risk areas. The Survey found that most boards do not separate risk management from audit responsibilities; only 8.5% of respondents indicated their board had a Risk Committee and, of those, only 54% of them had oversight of privacy and security. The Survey report highlights the segregation of duties issues that arise when one board committee both oversees the development of security programs and also audits the controls and effectiveness of such programs.

Survey responses also highlighted organizational deficiencies. Respondents indicated that most companies lack the functional separation of privacy and security; only 12% of the respondents indicated that their organization had separated privacy, security, and IT management into separate roles and responsibilities. Intra-company communication on privacy and security risks was also lacking; only 17% of the respondents indicated that they had a cross-organizational privacy and security team that met regularly to manage privacy and security issues.

## RECOMMENDATIONS

The survey revealed that governance of enterprise security is lacking, with gaps in critical areas. If boards and senior management take the following actions, they could significantly improve their organizations' security posture and reduce the risk of privacy breaches:

- Establish a board Risk Committee separate from the Audit Committee and assign it responsibility for enterprise risks, including IT risks.
- Ensure that privacy and security roles within the organization are separated and responsibilities are appropriately assigned.
- 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 and legal, the chief financial officer (“CFO”), the chief information officer (“CIO”), chief security or risk officer, privacy officer, and business line executives.
- Develop or review existing top-level policies to ensure that a culture of security and respect for privacy are established. Organizations can enhance their reputation by valuing cyber security and the protection of privacy and viewing them as corporate social responsibilities.
- Review the organization's security program and ensure that it comports with best practices and standards and addresses identified gaps or weaknesses.
- Include IT risks in enterprise risk management planning.
- Conduct an annual review of the enterprise security program, to be reviewed by the board Risk Committee.
- Conduct an annual audit of the organization's enterprise security program, to be reviewed by the Audit Committee.
- Require regular reports from senior management on privacy and security risks and review annual budgets for IT risk management.
- Conduct annual privacy compliance audits and require security breach notification plans.

## About the Survey

This report was created using raw data collected by the National Association of Corporate Directors (“NACD”) for its 2008 Public Company Governance Survey, which ran from April to June 2008. Invitations to complete the online survey were sent electronically to constituents of the NACD and other companies and organizations identified by Carnegie Mellon CyLab. NACD did not provide analysis for this CyLab report and had no role in preparing this final report, which reflects only the views of CyLab. The NACD did grant CyLab permission to use the raw data.

The CyLab 2008 report on its *Governance of Enterprise Security Survey* (“Governance Survey”) is based upon data received from 703 individuals serving on U.S.-listed public company boards. Of these, 485 were from outside directors and 218 were from inside directors and non-voting attendees (including senior management, general counsel, and corporate secretaries.)

Survey respondents opted to answer a public company, private company, or nonprofit organization survey. Since respondents may serve on several boards, the survey asked respondents to “select only one organization” as the focus of their responses and to base all their answers on that one organization. Those who serve on multiple boards were encouraged to fill out a survey reflecting their experiences with each.

This report focuses on responses from only the public company survey. The findings are 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 based on voluntary (rather than randomly selected) respondents, and these findings do not purport to represent the entire population of directors.

# I. Introduction

## PURPOSE OF THE GOVERNANCE SURVEY

Despite the enactment of legal compliance requirements and the reality of security breach lawsuits, IT experts continue to claim that their boards and senior management do not pay adequate attention to the security of their organizations' data and information technology ("IT") systems. The CyLab 2008 *Governance of Enterprise Security Survey* ("Governance Survey") was designed to determine:

- If these claims are valid;
- The degree to which boards of directors and officers ("D&Os") are actually exercising oversight of privacy and security;
- The board and organizational structure for such governance; and
- The degree to which companies are following best practices for governance of privacy and security.

## BACKGROUND: DUTY OF BOARDS & DIRECTORS

The governance responsibilities of D&Os have been in the spotlight since 2002 with the fall of Enron and Arthur Andersen and the enactment of Sarbanes-Oxley. The dependency of all organizations upon IT systems and global networks has extended enterprise governance responsibilities to an organization's use of technology. The IT Governance Institute ("ITGI") declares 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.<sup>2</sup>

Enterprise governance and IT governance increasingly encompass the security of IT systems and information. The American Society for Industrial Security ("ASIS"), the Information Systems Security Association ("ISSA"), and the Information Systems Audit and Control Association ("ISACA") note in their report, *Convergence of Enterprise Security Organizations*, that:

As new technologies emerge and threats become increasingly complex and unpredictable, senior security executives recognize the need to merge security functions throughout the entire enterprise.<sup>3</sup>

It has long been recognized that D&Os have a fiduciary duty to protect the assets of their organization.<sup>4</sup> Today, this duty extends to "digital assets" – a company's information, applications, and networks. This duty has been expanded by the enactment of new laws and regulations that impose specific privacy/security compliance requirements on targeted industry sectors. For example, the Gramm-Leach-Bliley Act ("GLBA") and the Health Insurance Portability and Accountability Act ("HIPAA") impose specific requirements pertaining to the security and privacy of data and networks, and Sarbanes-Oxley requires both management and external auditors to attest to the effectiveness of internal controls that provide meaningful assurance about the security of information assets.<sup>5</sup>

---

**"It has long been recognized that D&Os have a fiduciary duty to protect the assets of their organization. Today, this duty extends to "digital assets" – a company's information, applications, and networks."**

---

Other U.S. regulations also require the security of information, such as Internal Revenue Service regulations pertaining to the security of electronic tax records and certain Securities and Exchange Commission (“SEC”) and Food and Drug Administration (“FDA”) regulations.<sup>6</sup> The pressure on critical infrastructure industry sectors to secure their systems according to best practices and standards persists, with the U.S. energy sector recently agreeing to regulations.<sup>7</sup>

Action taken in multinational fora also has increased attention on digital corporate governance. Article 12 of the Council of Europe (“CoE”) Convention on Cybercrime,<sup>8</sup> which at the time of this report, has been signed by 45 countries and ratified by 23 (including the U.S.), requires signatory states to establish laws that hold companies civilly, administratively, or criminally liable for acts committed for their benefit either by an executive or as a result of the lack of supervision by an executive. Article 9 of the European Union’s (“EU”) Council Framework Decision on attacks against information systems<sup>9</sup> mirrors the CoE language and is binding on all Member States. The EU Decision effectively extends the same penalties across the EU’s 27 Member States to ensure their legal frameworks are harmonized.<sup>10</sup>

---

**“With estimated costs of \$90 to \$305 per disclosed record, the reputational and financial consequences to an organization can be significant.”**

---

There are also high-risk situations where higher standards apply to directors and officers, such as acquisitions, takeovers, responses to shareholder suits, and distribution of assets to shareholders in preference over creditors. In these circumstances, directors and officers are required to obtain professional assistance or perform adequate analyses to mitigate the risks that ordinarily accompany these activities. Some information assurance experts assert that a “higher degree of care will also be required of Directors and Officers regarding the complex nature of issues involved in information assurance.”<sup>11</sup>

Securities laws and regulations also require public corporations to adequately disclose in public filings and communications the risks relevant to the corporation and its assets. The *Independent Director* put this in the context of information systems by reporting that:

Management of information risk is central to the success of any organization operating today. For Directors, this means that Board performance is increasingly being judged by how well their company measures up to internationally accepted codes and guidelines on preferred Information Assurance practice.<sup>12</sup>

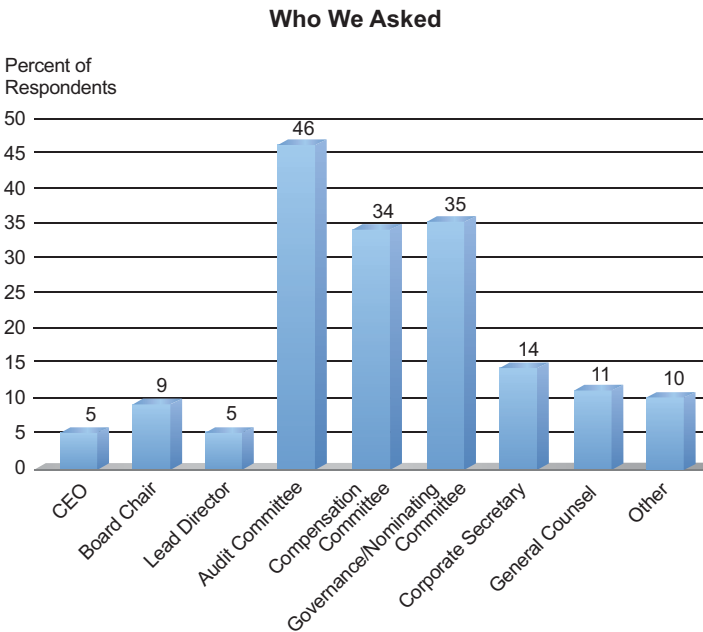
Additionally, when a company is a victim of an attack on its information systems, whether from an insider or an outside bad actor, studies have shown that this can result in a lack of confidence in the company and even a drop in the company stock price.<sup>13</sup> Security breach notification laws are forcing companies to disclose security breaches of personally identifiable information (“PII”). Such disclosures are resulting in civil and class action lawsuits. With estimated costs of \$90 to \$305 per disclosed record, the reputational and financial consequences to an organization can be significant. For example, the TJ Maxx breach has been estimated to cost the company \$4.5 billion.<sup>14</sup> Consequently, in addition to civil and class action lawsuits, D&Os may find themselves subject to a shareholder derivative suit for losses on stock price or market share caused by inadequate attention by officers and directors to the security of the company’s data, applications, and networks. Clearly, directors and officers need to undertake a certain level of involvement and oversight to ensure that the organization is properly secured against data breaches or other activities that could lead to shareholder derivative suits.

## II. Findings and Conclusions

### WHO WE ASKED

*The Governance Survey respondents were overwhelmingly board directors:* 69% of respondents were outside directors, with 14.8% of these respondents representing board chairs or lead directors. These respondents were also actively involved in board responsibilities:

- 46% of respondents were Audit Committee members;
- 34% of respondents were on the Compensation Committee; and
- 35% of respondents were on the Governance/Nominating Committee.



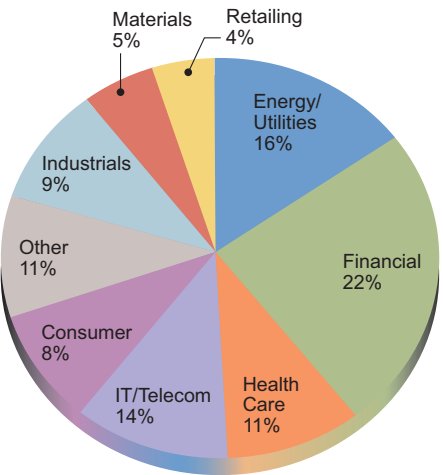
*Internal respondents were holding positions as inside directors and non-voting board attendees.*

They held positions of:

- CEO (5%);
- General Counsel (11%); and
- Corporate Secretary (14%).

*Governance Survey respondents (63%) were largely from critical infrastructure industry sectors* who increasingly face government pressure and/or regulatory compliance requirements with respect to the security of their IT systems and data. These survey respondents represented:

#### Who We Asked (by Sector)

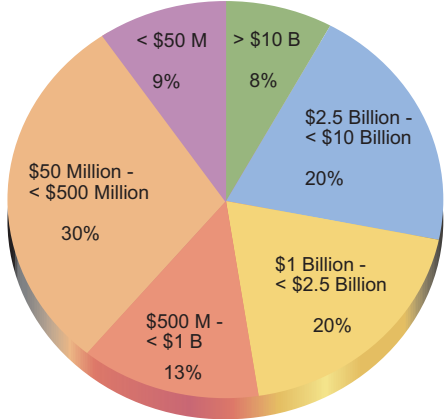


- Energy and utility companies – 16%
- Financial sector – 22%
- Health care companies – 11%
- IT and telecommunications companies – 14%.

The remaining 37% of respondents represented consumers, industrials, materials, retail, and other types of companies.

Survey respondents represented both very large corporations and smaller companies. Nearly half of the Governance Survey respondents (48%) came from large to medium-sized companies with annual revenues ranging from \$1 billion to more than \$10 billion. The remainder of respondents was from companies with annual revenues between \$1 billion and less than \$50 million, with 30% of these respondents from smaller businesses whose annual revenues were in the \$500 million to \$50 million range.

Who We Asked (by Annual Revenues)

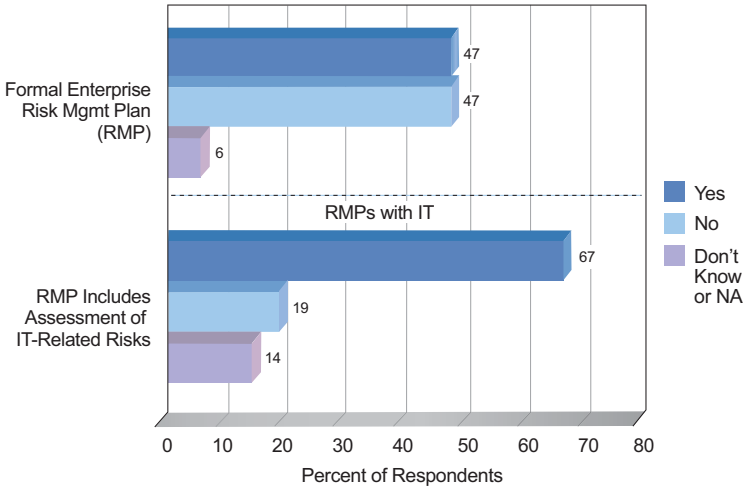


**FINDINGS**

*Oversight & Governance*

*The survey revealed that boards are taking risk management seriously, but there is still a gap in understanding the linkage between IT risks and enterprise risk management.*

IT Risks Not Usually in Risk Management



Less than half – 47% – of the respondents said their organizations had adopted a formal enterprise Risk Management Plan (RMP) or other program that provided a structured, consistent, and coordinated framework for assessing, responding to, and reporting on risks that impact the achievement of the organization’s objectives. Two-thirds (67%) of those respondents indicated that their risk management program included IT-related risks. This is encouraging.

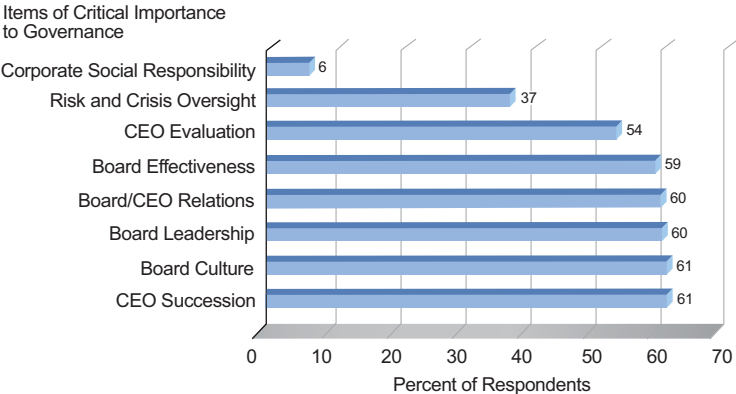
How D&Os view risk is an important indicator of why privacy and security is given short shrift. Although nearly half (49.5%)

of the respondents indicated that risk and crisis oversight was important, *only 37% of them believed that it was a critical governance issue*, placing more emphasis on areas such as board culture, board effectiveness, board/CEO relations, CEO succession and evaluation, and corporate performance.

*The view that the protection of corporate and customer data is a corporate social responsibility is not likely to motivate boards to pay more attention to enterprise security.*

Although organizations today face public and regulatory scrutiny with respect to environmental behavior, transparency in operations, avoidance of conflicts of interest, and compliance, *corporate social responsibility was viewed as critical to board governance by only 6.35% of the respondents*. Thus, the notion put forth by privacy advocates and consumers that companies should be good cyber citizens needs to be more fully developed and understood by D&Os.

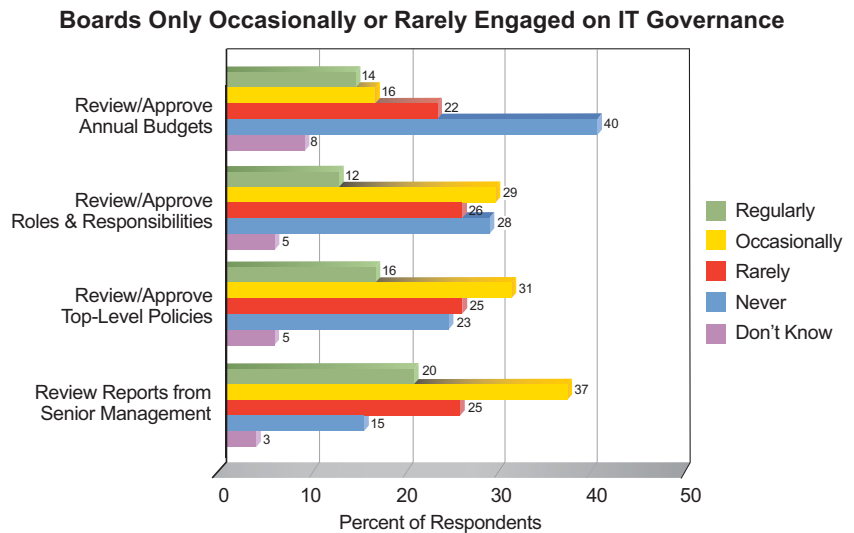
Risks & Crisis Not Viewed as Critically Important



*The Governance Survey confirmed the belief among IT security professionals that boards and senior executives are not involved in key areas related to governance over enterprise security.* This may be due to the widespread belief that privacy and security are “tech” issues that are best managed by IT staff.

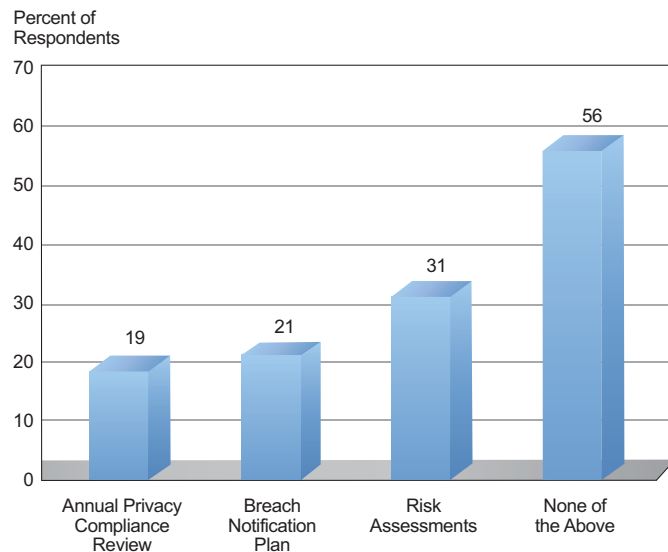
*Out of the pool of respondents, 36% of them indicated that their board had direct involvement with oversight of information security.*

There are a number of best practices for board involvement with respect to IT governance. When asked whether boards receive information or are involved in activities related to these best practices, respondents indicated that boards are only occasionally or rarely engaged:



- 38% of respondents said they only occasionally or rarely reviewed and approved annual budgets for privacy and security risk management; an additional 40% said they never did.
- 55% of respondents indicated they only occasionally or rarely reviewed and approved roles and responsibilities of personnel responsible for privacy and security risks; an additional 28% said they never did.
- 56% of respondents said they only occasionally or rarely reviewed and approved top-level policies regarding privacy and security risks; an additional 23% said they never did.
- 62% of respondents said they only occasionally or rarely received reports from senior management regarding privacy and security risks; an additional 15% said they never got such reports.

**Most Boards Not Engaged in Key Oversight Activities**



*Respondents also indicated that the vast majority of boards that are reviewing privacy and security issues are not focusing on important activities that would help protect the organization from one of its highest risks: the reputational and financial losses flowing from security breaches or the disclosure of personally identifiable information (“PII”).* There are several key actions that help protect companies against these risks and in which board oversight is helpful and can strengthen the security posture of the company.

Respondents indicated, however, that most boards generally are not involved in these activities. Respondents indicated that boards are involved in oversight of annual privacy compliance reviews only 19% of the time; security breach notification plans only 21% of the time, and assessments of risks related to the handling/use of PII or other protected data only 31% of the time.

### Board Committee Structure

The manner in which boards deal with risk management and enterprise security is reflected in how they are organized and how they assign committee responsibilities. On the whole, boards do not separate risk management from audit responsibilities, i.e., there are not separate risk and audit committees.

**Respondents indicated that only 8% have a Risk Committee that is separate from an Audit Committee – but of this 8%, only 53% of them oversee privacy and security.**

When polled about the types of committees their boards have, respondents indicated that only 2.4% of boards have a Technology Committee. *The respondents indicated that their boards are overly reliant upon Audit Committees to manage risk issues.* The survey results revealed that boards assign the majority of tasks directly related to the oversight of risk to the Audit Committee 65% of the time; 23% of the time risk issues are handled by the full board. Risk Committees are assigned the majority of tasks directly related to risk only 4% of the time.

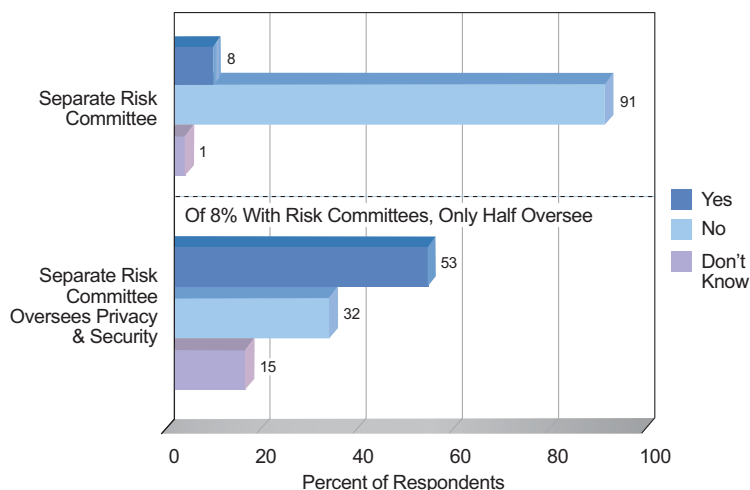
**Assigning both oversight of risk and audits of how the risks are being managed to the same committee – the Audit Committee – creates segregation of duties (“SOD”) issues at the board level** because the same committee that exercises oversight of operational aspects of privacy and security also oversee audits in these areas. Best practices and industry standards separate the audit and risk functions. Enterprise security programs should be developed and sustained by operational personnel, with oversight by a Board Risk Committee. Audit Committees should conduct annual reviews of the organization’s enterprise security program to confirm that best practices are being followed, compliance requirements are being met, controls are effective, and privacy and security risks are being managed. In addition, internal audit plays a valuable role in conducting targeted reviews of particular areas of the security program and testing controls.<sup>15</sup>

### Internal Organizational Roles & Responsibilities

**Officers and senior management are not establishing key positions for privacy and security or appropriately assigning responsibilities.**

Best practices call for clear roles and responsibilities with respect to privacy and security. The delineation of responsibilities should serve as a check and balance and protect the company against SOD issues that could increase risk.

**Few Have Risk Committees Separate from Audit Committees**



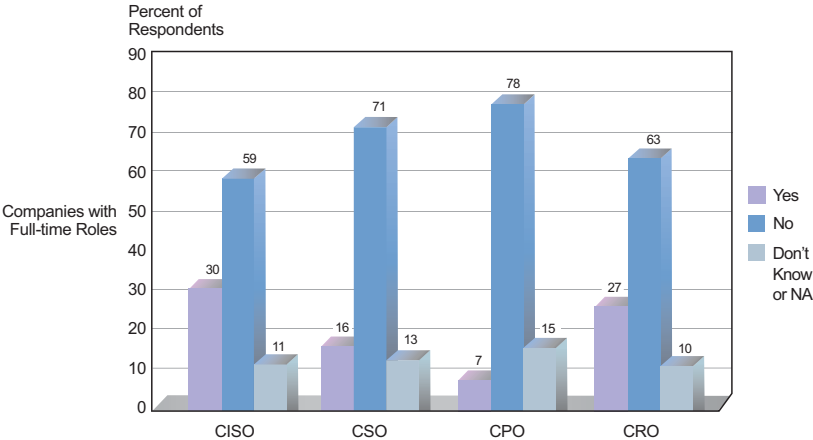
There is a general belief that most companies do not understand this and either are not creating the needed roles or are combining responsibilities. So disparate are the approaches to IT security, that titles for personnel responsible for privacy and security span four possibilities: chief privacy officer (“CPO”), chief information security officer (“CISO”), chief security officer (“CSO”), and chief risk officer (“CRO”).

*The majority of survey respondents indicated that their organizations did not have personnel in these roles:*

*59% of the respondents said their organizations did not have a CISO and 71% said they did not have a CSO. A whopping 78% of the respondents said they did not have a CPO. It was not surprising that 63% said their organizations did not have a CRO, as that is a relatively new title that is being used by security savvy companies who understand the need to integrate IT, physical, and*

*personnel security and manage it through one position. It is possible, however, that some respondents indicated they did not have someone in a particular position because the person in their organization did not have that specific title. Nevertheless, the percentages are high and indicate that this is an area that needs more board attention*

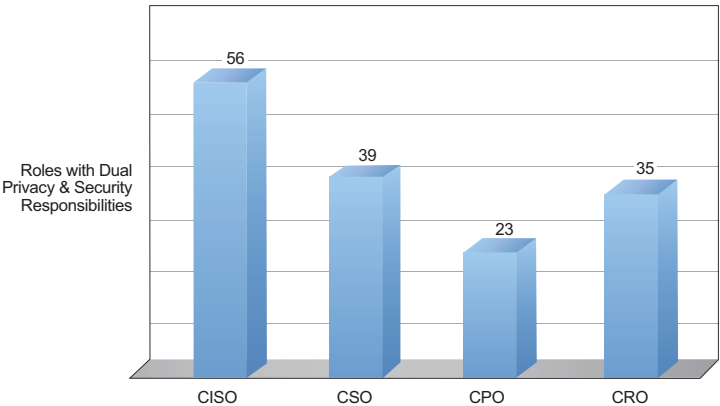
**Majority of Companies Do Not Have Privacy & Security Executives**



*Organizations tend to overlap privacy and security responsibilities, not understanding the inherent SOD issues.*

More than half of the respondents who have a CISO (56%) indicated that the CISO in their organization is responsible for both privacy and information security; 39% of CSOs also handle privacy issues. Interestingly, organizations were less likely to assign security responsibilities to privacy officers. Respondents indicated that only 23% of CPOs are also responsible for information security issues. CROs are responsible for both privacy and security in 35% of the respondents’ organizations.

**Overlapping Privacy & Security Roles Create SOD Issues**

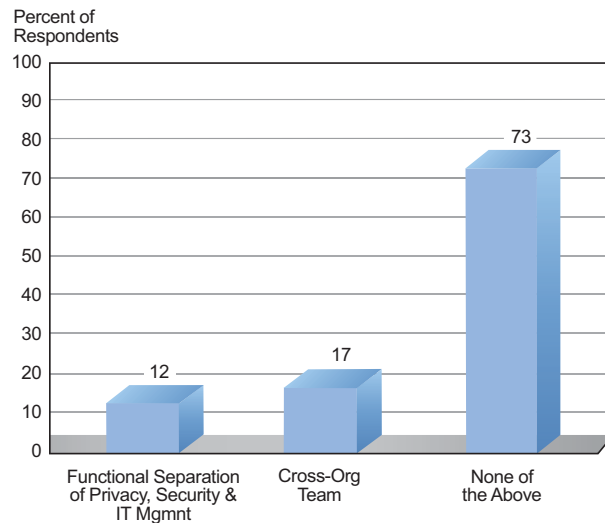


It is important that privacy and security responsibilities be separated to prevent a single point of failure, which can occur (a) when security personnel do not understand compliance requirements or needed privacy controls, or (b) when privacy personnel do not understand the technical security configuration or technical controls.<sup>16</sup>

***Organizations lack functional separation of privacy and security and cross-organizational communication***, leaving them more

vulnerable to insider threats, external attacks, governance gaps, and legal liability. When asked if their board reviewed the roles of personnel for information security, only 12% of the respondents indicated that their organization had a functional separation of privacy, security, and information technology management. Only 17% of the respondents said their organizations had a cross-organizational or inter-departmental team (“X-Team”) that meets regularly to manage privacy and security issues. A stunning 73% of respondents stated their organizations had neither functional separation nor cross-organizational communication on privacy and security.

### Most Lack Functional Separation & Cross-Org Communication



## CONCLUSIONS

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

- Boards – especially those of critical infrastructure companies – need to better understand the risks associated with IT, especially privacy and security risks.
- Few boards have Risk Committees; they tend to be overly reliant upon their Audit Committee for both overseeing and auditing privacy and security.
- There is little board oversight or governance on privacy and security issues.
- There is little value placed on corporate social responsibility as a governance issue, which could include organizations being good cyber citizens.
- Many organizations do not have executives in key roles for privacy and security, and few have functional separation of privacy and security responsibilities or cross-organizational teams.
- Many organizations have major gaps or areas in their enterprise security programs that are not in compliance with internationally accepted best practices and standards, leaving them legally and technically vulnerable.

### III. Recommendations

The survey revealed that governance of enterprise security is lacking, with gaps in critical areas. If boards and senior management take the following actions, they could significantly improve their organizations' security posture and reduce the risk of privacy breaches:

- Establish a board Risk Committee separate from the Audit Committee and assign it responsibility for enterprise risks, including IT risks.
- Ensure that privacy and security roles within the organization are separated and responsibilities are appropriately assigned.
- 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 and legal, the chief financial officer (“CFO”), the chief information officer (“CIO”), chief security or risk officer, privacy officer, and business line executives.
- Develop or review existing top-level policies to ensure that a culture of security and respect for privacy are established. Organizations can enhance their reputation by valuing cyber security and the protection of privacy and viewing them as corporate social responsibilities.
- Review the organization's security program and ensure that it comports with best practices and standards and addresses identified gaps or weaknesses.
- Include IT risks in enterprise risk management planning.
- Conduct an annual review of the enterprise security program, to be reviewed by the board Risk Committee.
- Conduct an annual audit of the organization's enterprise security program, to be reviewed by the Audit Committee.
- Require regular reports from senior management on privacy and security risks and review annual budgets for IT risk management.
- Conduct annual privacy compliance audits and require security breach notification plans.

## Endnotes

- <sup>1</sup> 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 and Allen”).
- <sup>2</sup> *Board Briefing on IT Governance*, 2nd ed., IT Governance Institute, 2003 at 10, [http://www.itgi.org/Template\\_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm](http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm) (emphasis added).
- <sup>3</sup> *Convergence of Enterprise Security Organizations*, American Society for industrial Security, Information Systems Security Association, and Information Systems Audit and Control Association, 2003 at 2, [http://www.issa.org/Downloads/Convergence\\_StudyNov05.pdf](http://www.issa.org/Downloads/Convergence_StudyNov05.pdf).
- <sup>4</sup> 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, <http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450036>.
- <sup>5</sup> Sarbanes-Oxley Act of 2002, Pub. Law 107-204, Sections 302, 404, <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>. The SEC has taken a narrow interpretation of Sarbanes-Oxley to the point that information security and risk management pertain only to the financial statements of a company. The Federal Reserve has countered this by saying a broader interpretation is needed to include all of the operational risks since there are many aspects that can impact the financial standing of an organization that can affect the integrity and accuracy of the financials.
- <sup>6</sup> Thomas J. Smedinghoff, “Where We’re Headed – New Developments and Trends in the Law of Information Security,” Nov. 12, 2006, <http://www.wildman.com/index.cfm?fa=news.pubArticle&aid=5072F372-BDB9-4A10-554DF441B19981D7>.
- <sup>7</sup> “Legal Resources,” Critical Energy Infrastructure Information (CEII) Regulations, Federal Energy Regulatory Commission, <http://www.ferc.gov/legal/maj-ord-reg/land-docs/ceii-rule.asp>.
- <sup>8</sup> Council of Europe *Convention on Cybercrime* – Budapest, 23.XI.2001 (ETS No. 185) (2002), <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm>, Council of Europe *Convention on Cybercrime Explanatory Report*, Nov. 8, 2001, <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.
- <sup>9</sup> *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://europa.eu.int/eur-lex/en/com/pdf/2002/com2002\\_0173en01.pdf](http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf).
- <sup>10</sup> “EU Ministers Agree on Legislation To Harmonize Laws to Combat Crimes,” *Privacy & Security Law Report*, Vol. 2, No. 14, Apr. 7, 2003 at 352.

<sup>11</sup> John H. Nugent, “Corporate Officer and Director Information Assurance (IA) Liability Issues: A Layman’s Perspective,” Dec. 15, 2002, [http://gsmweb.udallas.edu/info\\_assurance](http://gsmweb.udallas.edu/info_assurance).

<sup>12</sup> *Id.* (citing Dr. Andrew Rathmell, Chairman of the Information Assurance Advisory Council, “Information Assurance: Protecting your Key Asset,” <http://www.iaac.ac.uk>).

<sup>13</sup> A. Marshall Acuff, Jr., “Information Security Impacting Securities Valuations: Information Technology and the Internet Changing the Face of Business,” Salomon Smith Barney, 2000, at 3-4, <http://www.ciao.gov/industry/SummitLibrary/InformationSecurityImpactingSecuritiesValuations.pdf>.

<sup>14</sup> Sharon Gaudin, “Estimates Put T.J. Maxx Security Fiasco at \$4.5 Billion,” *Information Week*, May 2, 2007, <http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199203277>.

<sup>15</sup> Westby and Allen at 57-58.

<sup>16</sup> 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.

## Bibliography & Additional References

### BIBLIOGRAPHY

A. Marshall Acuff, Jr., "Information Security Impacting Securities Valuations: Information Technology and the Internet Changing the Face of Business," Salomon Smith Barney, 2000, <http://www.ciao.gov/industry/SummitLibrary/InformationSecurityImpactingSecuritiesValuations.pdf>.

*Board Briefing on IT Governance*, 2nd ed., IT Governance Institute, 2003, [http://www.itgi.org/Template\\_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm](http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm).

*Convergence of Enterprise Security Organizations*, American Society for industrial Security, Information Systems Security Association, and Information Systems Audit and Control Association, 2003, [http://www.aesrm.org/projects\\_and\\_publications.html](http://www.aesrm.org/projects_and_publications.html).

Council of Europe *Convention on Cybercrime* – Budapest, 23.XI.2001 (ETS No. 185) (2002), <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm>, Council of Europe Convention on Cybercrime Explanatory Report, Nov. 8, 2001, <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

"EU Ministers Agree on Legislation To Harmonize Laws to Combat Crimes," *Privacy & Security Law Report*, Vol. 2, No. 14, Apr. 7, 2003 at 352.

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>

Jody R. Westby, ed., *International Guide to Cyber Security*, American Bar Assn., Privacy & Computer Crime Committee, 2004, <http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450036>.

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>

John H. Nugent, "Corporate Officer and Director Information Assurance (IA) Liability Issues: A Layman's Perspective," Dec. 15, 2002, [http://gsmweb.udallas.edu/info\\_assurance](http://gsmweb.udallas.edu/info_assurance).

"Legal Resources," Critical Energy Infrastructure Information (CEII) Regulations, Federal Energy Regulatory Commission, <http://www.ferc.gov/legal/maj-ord-reg/land-docs/ceii-rule.asp>.

*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://europa.eu.int/eur-lex/en/com/pdf/2002/com2002\\_0173en01.pdf](http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf).

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

Sharon Gaudin, "Estimates Put T.J. Maxx Security Fiasco at \$4.5 Billion," *Information Week*, May 2, 2007, <http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199203277>.

Thomas J. Smedinghoff, "Where We're Headed – New Developments and Trends in the Law of Information Security," Nov. 12, 2006, <http://www.wildman.com/index.cfm?fa=news.pubArticle&aid=5072F372-BDB9-4A10-554DF441B19981D7>.

## **ADDITIONAL REFERENCES**

*20 Questions Directors Should Ask About IT*, The Canadian Institute of Chartered Accountants, Information Technology Advisory Committee, Apr. 2004, [http://www.cica.ca/index.cfm/ci\\_id/1000/la\\_id/1.htm](http://www.cica.ca/index.cfm/ci_id/1000/la_id/1.htm).

Alan Calder, *IT Governance Guidelines for Directors*, IT Governance Publishing, 2005, <http://www.isaca.e-symposium.com/guidelines.pdf>.

Board Responsibilities for Managing Risks of eBusiness, American International Group, Inc., 2001.

Common Sense Guide for Senior Managers: Top Ten Information Security Practices, 1st ed., Internet Security Alliance, July 2002.

E. Michael Power and Roland L. Trope, *Sailing in Dangerous Waters: A Director's Guide to Data Governance*, American Bar Association, Business Law Section, 2005, <http://www.abanet.org>.

*Enterprise Governance: Getting the Balance Right*, International Federation of Accountants, Professional Accountants in Business Committee, Feb. 2004, <http://www.ifac.org/MediaCenter/files/EnterpriseGovernance.pdf>.

*Fundamental Information Risk Management: Implementation Guide*, Information Security Forum, March 2000, <http://www.securityforum.org/assests/pdf/firm.pdf>.

*Guide to Information Security and the Law*, American Bar Association, Information Security Committee, 2002, <http://www.abanet.org>.

*Implementing Turnbull: A Boardroom Briefing*, The Institute of Chartered Accountants, Sept. 1999, <http://www.steelhenge.co.uk/knowledgezone/Implementing%20Turnbull-ICA.pdf>.

*Information Risk Management in Corporate Governance*, Workshop Report, Information Security Forum, Dec. 2003, <http://neumann.hec.ca/gestiondesrisques/03-04.pdf>.

*Information Security Governance: A Call to Action*, Corporate Governance Task Force Report, Apr. 2004, [http://www.cyberpartnership.org/InfoSecGov4\\_04.pdf](http://www.cyberpartnership.org/InfoSecGov4_04.pdf).

*Information Security Governance: Guidance for Boards of Directors and Executive Management*, IT Governance Institute, 2006, <http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=34997>.  
*Information Security Governance: Toward A Framework for Action*, Business Software Alliance, <http://www.bsa.org>.

*Information Security Governance: What Directors Need to Know*, The Institute of Internal Auditors, Critical Infrastructure Assurance Project, 2001, <http://www.theiia.org/download.cfm?file=7382>.

*IT Governance Global Status Report---2008*, IT Governance Institute, 2008, <http://www.itgi.org/.../ContentManagement/ContentDisplay.cfm&ContentID=39735>.

*Information Security Oversight: A 2007 Survey Report*, National Association of Corporate Directors, 2007, <http://www.nacdonline.org>.

Jody R. Westby, ed., *Roadmap to an Enterprise Security Program*, American Bar Association, Privacy & Computer Crime Committee, 2005, <http://www.abanet.org/scitech/Roadmapworkshopagenda.doc>.

Jody R. Westby, "Protection of Trade Secrets and Confidential Information: How to Guard Against Security Breaches and Economic Espionage," *Intellectual Property Counselor*, Jan. 2000.

Kenneally, "The Byte Stops Here: Duty and Liability for Negligent Internet Security," *Computer Security Journal*, Vol. XVI, No. 2, 2000, <http://www.stanford.edu/class/msande91si/www-aut04/aut04/slides/erinCSIPresent.ppt>.

*Organizational Governance: Guidance for Internal Auditors*, The Institute of Internal Auditors, July 2006, <http://www.theiia.org/download.cfm?file=76050>.

Pauline Bowen, Joan Hash, and Mark Wilson, *Information Security Handbook: A Guide for Managers*, National Institute of Standards and Technology, Special Pub. 800-100, Oct. 2006, <http://csrc.nist.gov/publications/PubsSPs.html>.

Peter Weill, *Don't Just Lead, Govern: How Top-Performing Firms Govern IT*, Massachusetts Institute of Technology, Center for Information Systems Research, Sloan School of Management, March 2004, <http://dspace.mit.edu/handle/1721.1/1846>.

Peter Weill and Jeanne W. Ross, "Ten Principles of IT Governance," Harvard Business School, Harvard Business School Working Knowledge, July 5, 2004, <http://hbswk.hbs.edu/archive/4241.html>.

*Principles of Corporate Governance 2005*, Business Roundtable, Nov. 2005, <http://www.businessroundtable.org/pdf/CorporateGovPrinciples.pdf>.

*Risk Management: Practical guidance on how to prepare for successful audits*, IT Compliance Institute, IT Audit Checklist Series, 2006, [http://download.101com.com/pub/itci/Files/ITCi\\_ITACL-Risk-Management\\_0610.pdf](http://download.101com.com/pub/itci/Files/ITCi_ITACL-Risk-Management_0610.pdf).

Steven M. Kowal, "The Risk of Director Liability Has Increased," Food & Drug Law Institute, Issue 4, July/Aug. 2001, <http://www.fldi.org>.

"The List of Authority Documents," Unified Compliance Framework Series, IT Compliance Institute, <http://www.itcinstitute.com/>.

*The Struggle to Manage Security Compliance for Multiple Regulations*, White Paper: Enterprise Security, Symantec Corp. 2004, <http://www.symantec.com/index.jsp>.



Carnegie Mellon University  
5000 Forbes Avenue  
Pittsburgh, PA 15213

[www.cylab.cmu.edu](http://www.cylab.cmu.edu)