

TESTIMONY OF

Jody R. Westby, Esq.
Managing Director, PricewaterhouseCoopers LLP

Before the House Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the
Census

September 22, 2004

INFORMATION SECURITY: RESPONSIBILITIES OF BOARDS OF DIRECTORS AND SENIOR MANAGEMENT

Introduction

Good afternoon, Mr. Chairman and Members of the Subcommittee. My name is Jody Westby. I am a Managing Director of PricewaterhouseCoopers LLP, and I currently chair the American Bar Association's Privacy & Computer Crime Committee, Section of Science & Technology Law. I would like to state at the outset, for clarification of the Subcommittee, that I am here today testifying in my individual capacity and that my testimony is based on my own background and experience, and does not necessarily reflect the position of the American Bar Association or PricewaterhouseCoopers.

It is an honor to participate in this important discussion on the ramifications of identity theft. Thank you for including me among these distinguished panelists. I have been working in the field of information technology (IT) security since 1996, with an emphasis upon the role of boards of directors and senior executives in protecting their corporate information infrastructure since 1998. The perspective I bring to the Subcommittee today is based on more than twenty years of technical, legal, policy, and business experience, enabling me to bring a multidisciplinary perspective to the many issues facing businesses and governments in the areas of information security, IT business risk management, outsourcing/offshoring risks, cybercrime, and Homeland Security, including cyberterrorism and infowar. I am a member of the World Federation of Scientists' Permanent Monitoring Panel on Information Security and serve on the board of the National Conference of Lawyers and Scientists. In my professional capacity, I regularly consult with governments, private sector executives, and operational personnel on the development of enterprise security programs that dovetail the technical, legal, operational, and managerial considerations.

Today, our national security, economic security, and public safety are intertwined due to the risks flowing from a global network connecting over 730 million users in nearly 200 countries. Identity theft is but one vulnerability. Security breaches that result in unauthorized access to personally identifiable information provide the data needed for identity theft. In addition, these breaches can feed organized crime, terrorist organizations, and other bad actors information that enables them to exploit others for their benefit or launch asymmetric attacks that jeopardize public safety and our national and economic security. Our ability to control these risks is largely

dependent upon the security of private sector networks. My testimony will focus on the root-cause of electronic identity theft: the lack of enterprise security safeguards that are governed by boards of directors and senior management, including the implementation of best practices and standards and regular risk assessments.

Although the financial sector is ahead of other industries in this area, overall, there remains a disturbing lack of understanding at the officer and director levels regarding their oversight and governance responsibilities for the security of corporate data, applications, and networks. These responsibilities include:

- Regularly assessing information technology (IT) risks to corporate operations and managing identified threats and vulnerabilities;
- Establishing corporate policies governing IT usage, cyber security, and employee conduct;
- Incorporating cyber security best practices and standards into business operations;
- Ensuring sufficient funding is allocated to develop and maintain an enterprise security program with adequate internal controls;
- Implementing the security program through training and measuring compliance through meaningful metrics; and
- Conducting regular reviews and audits of the security program.

Unfortunately, the good work of many to move corporate America in this direction is being undercut by the notion that risk assessments – the critical input necessary for any enterprise security program – can establish knowledge of system vulnerabilities and weaknesses that later could be used against a corporation in the event of a cyber attack or security breach that caused harm to others or resulted in economic losses. Indeed, that could be true if serious weaknesses were identified and no corrective measures were taken. This, however, is no different than the consequences of ignoring structural or mechanical weaknesses after a review process.

My testimony rebuts this notion by asserting that corporations – including their officers and directors – actually *increase* their risk to liability if they fail to (1) conduct assessments, (2) meet security and privacy compliance requirements and legal obligations, and (3) develop and implement an enterprise security program that mitigates identified risks and adheres to best practices and standards. Today, cyber incidents are in the daily news and their general impact upon corporations operations is well known. Moreover, a plethora of standards, best practices, and guidance exists to assist companies of all sizes in protecting their systems. In addition, a sizeable percentage of private sector companies are now subject to numerous security compliance responsibilities. This heightened level of awareness, combined with new legal security requirements and industry acceptance of security standards and best practices, make risk assessments a corporate responsibility to be accepted, not ignored.

This testimony steps through director and officer responsibilities for cyber security, including the major compliance requirements; it discusses the current situation and threats; and suggests possible steps toward advancing cyber security at the corporate level and around the globe.

The starting point is to determine the *responsibility* that boards and officers have to protect their digital assets, which includes information, applications, and networks. In the U.S., this responsibility flows from two sources:

1. Case law surrounding the fiduciary duty of care directors and officers owe their shareholders and the protections afforded by the “Business Judgment Rule;” and
2. Compliance with statutes, regulations, Executive Orders and Presidential Directives, administrative consent decrees, contractual agreements, and public expectations.

From an international perspective, the Council of Europe Convention on Cybercrime¹ (CoE Convention) and the European Union’s (EU) Council Framework Decision on attacks against information systems² both specify administrative, civil, and criminal penalties for cybercrimes that were made possible due to the lack of supervision or control by someone in a senior management position, such as an officer or director.³

Duty of Care and Business Judgment Rule⁴

Director and officer governance of corporate digital security is embedded within the fiduciary duty of care owed to company shareholders to:

- Govern the operations of the company and protect its critical assets;
- Protect the company’s market share and stock price;
- Govern the conduct of employees;
- Protect the reputation of the company; and
- Ensure compliance requirements are met.

¹ 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> (hereinafter referred to as “CoE Convention”).

² *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 (hereinafter referred to as EU Council Framework Decision”).

³ CoE Convention, Article 12; EU Council Framework Decision, Article 9. The U.S. is a signatory of the CoE Convention and on November 17, 2003, President Bush sent the Convention to the U.S. Senate for ratification, but action has not been taken. See George W. Bush, “Message to the Senate of the United States,” The White House, Nov. 17, 2003, <http://www.whitehouse.gov/news/releases/2003/11/print/20031117-11.html>.

⁴ Significant portions of the text in this section are taken from the following two sources, of which I own the copyright to the text: Jody R. Westby, ed., *International Guide to Cyber Security*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, ABA Publishing, 2004 at 191-93 (hereinafter “Westby - Cyber Security”); *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, Report & Recommendations, World Federation of Scientists, Permanent Monitoring Panel on Information Security, Nov. 19, 2003, World Summit on the Information Society Document WSIS-03/GENEVA/CONTR/6-E, http://www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf (hereinafter “Toward a Universal Order of Cyberspace”).

Duty of Care

Directors and officers are responsible for governing the operations of a company. This includes the protection of critical assets. Since an estimated 80 percent of corporate assets today are digital,⁵ it logically follows that the oversight of information security falls within this duty. Just as directors and officers have a responsibility to ensure that the research and development lab door is locked and intellectual property is properly secured, today, it is increasingly clear that the same corporate governance responsibility exists with respect to security of company data, systems, and networks. The consequences of IT security breaches can be severe. It is now well substantiated that the theft of proprietary data and other cyber security breaches can result in a loss of market share, significant financial losses, or drop in market capitalization.⁶

Hacking, denial of service attacks, economic espionage, and insider incidents are commonplace and threaten the profitability of every business, leaving officers and directors vulnerable to lawsuits and civil and criminal penalties. Today, insider misuse of data and systems remains one of the top causes of security breaches, providing clear evidence that an area under the direct control of senior management and the board presents one of the highest risks to corporations. Indeed, last month, the U.S. Secret Service and Carnegie Mellon's CERT Coordination Center released an important study on insider threats in the banking and finance sector, noting that, "Management attention on financial performance, to the exclusion of good risk management practices, seems to be a recurrent theme in some of the cases in this study."⁷

Attacks coming from the outside – even those that do not involve theft, disclosure, or sabotage – present grave financial risks to corporations. An examination of the distributed denial of service attacks on Yahoo!, Amazon, and others in 2000 concluded that these attacks can result in a lack of confidence in the company and a drop in stock price.⁸

Any attack, whether from inside or outside the system, can damage the reputation of the company. The protection of a company's good name or brand is linked to a company's bottom line. Corporations have been reluctant to report cyber security breaches out of fear of damaging public relations and harming corporate reputation.⁹ California has curbed this trend by enacting the Security Breach Information Act (SB 1386), a law that requires any state agency, person, or business that conducts business in California to notify the owner or licensee of information of any security breach of unencrypted personal information of any resident of California.¹⁰

⁵ "Cybercrime," *Business Week*, Feb. 21, 2000.

⁶ See, e.g., "Companies urged to prepare for cyber attacks," *globalcontinuity.com*, Aug. 21, 2002, <http://www.globalcontinuity.com/article/articleview/987/1/30/>.

⁷ *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, United States Secret Service and Carnegie Mellon CERT Coordination Center of the Software Engineering Institute, Aug. 2004 at 21, http://www.secretservice.gov/ntac/its_report_040820.pdf.

⁸ 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>.

⁹ *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, National Research Council, Computer Science and Telecommunications Board, 2002, http://www7.nationalacademies.org/cstb/pub_cybersecurity.html.

¹⁰ Security Breach Information Act (SB 1386), Feb. 12, 2002, http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html; Devon Hewitt, "New California privacy law has nationwide ripple,"

Although California is ahead of the curve, the trend is clearly toward legislation requiring mandatory reporting of computer security breaches. At the federal level, Senator Dianne Feinstein has introduced Senate Bill 1350, “The Notification of Risk to Personal Data Act,” modeled after the California reporting law.

Based on the foregoing, it is reasonable to conclude that directors and officers have a duty of care to protect a corporation’s digital assets from a wide range of inside and outside security threats, to protect its market share and stock price from fluctuations as a consequence of these breaches, to guard its reputation, and to govern the conduct of employees. The degree of attention that is required to be given to these issues, however, falls within the Business Judgment Rule.

Business Judgment Rule

The majority of U.S. jurisdictions follow the business judgment rule that the standard of care is that which a reasonably prudent director of a similar corporation would have used. The business judgment rule “operate[s] as a shield to protect directors from liability for their decisions.”¹¹ The ruling in one recent Delaware case turned attention to information systems and internal controls. The 1996 case, *Caremark International Inc. Derivative Litigation*, held that, “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 certain circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards.”¹² To date, no shareholder suit has been brought against officers or directors for failure to take necessary steps to protect corporate systems and data, however, shareholders may have a valid basis for such derivative suits.¹³

The *Caremark* court noted that officer/director liability can arise in two contexts: (1) from losses arising out of ill-advised or negligent board decisions (which are broadly protected by the business judgment rule so long as the decision was reached out of a process that was rational or employed in a good faith effort) and (2) from circumstances where the board failed to act in circumstances where “due attention” would have prevented the loss. In the latter situation, the *Caremark* court noted that:

[I]t would, in my opinion, be a mistake to conclude that . . . corporate boards may satisfy their obligation to be reasonably informed concerning the corporation, without assuring themselves that information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation’s compliance with law and its business performance. . . .

Washington Technology, July 7, 2003 at 12; Keith Poulsen, “California disclosure law has national reach,” *SecurityFocus Online*, Jan. 6, 2003, <http://online.securityfocus.com/news/1984>.

¹¹ *Gries Sports Enterprises, Inc. v. Cleveland Browns Football Co.*, 26 Ohio St.3d 15, 496 N.E. 2d 959 (1986).

¹² *In re Caremark Int’l Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

¹³ Jody R. Westby, “Protection of Trade Secrets and Confidential Information: How to Guard Against Security Breaches and Economic Espionage,” *Intellectual Property Counselor*, (Jan. 2000) at 4-5.

Obviously the level of detail that is appropriate for such an information system is a question of business judgment. . . . But it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility.¹⁴

The *Caremark* case could provide the basis for a shareholder suit against officers and directors for failure to implement an information and reporting system on the security of corporate networks and data such that the officers and directors could:

- Determine whether the organization was adequately meeting statutory, regulatory, or contractual obligations to protect certain data from theft, disclosure or inappropriate use; and
- Ascertain that the data critical to normal business operations, share price, and market share was protected.¹⁵

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."¹⁶

Securities laws and regulations require public corporations to adequately disclose in public filings and public communications relevant risks 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.¹⁷

Thus, the duty of officers and directors to make informed, good-faith decisions to protect the corporation's assets and financial stability is directly dependent upon the board ensuring that an

¹⁴ *Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

¹⁵ See, e.g., *id.*; For a general discussion on corporate liability related to board and officer responsibilities to ensure adequate information and control systems are in place, see Steven G. Schulman and U. Seth Ottensoser, "Duties and Liabilities of Outside Directors to Ensure That Adequate Information and Control Systems are in Place – A Study in Delaware Law and The Private Securities Litigation Reform Act of 1995," Professional Liability Underwriting Society, 2002 D&O Symposium, Feb. 6-7, 2002, <http://www.plusweb.org/Events/Do/materials/2002/Source/Duties%20and%20Liabilities.pdf>.

¹⁶ 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.

¹⁷ *Id.* (citing Dr. Andrew Rathmell, Chairman of the Information Assurance Advisory Council, "Information Assurance: Protecting your Key Asset," <http://www.iaac.ac.uk>).

enterprise security program is in place that manages risks, sets policies and procedures for the conduct of employees and the operations of the corporation, and protects critical digital assets. Clearly, this duty cannot be met and informed decisions cannot be made if risk assessments are not performed.

Compliance with Legal Obligations

In addition to foregoing, officers and directors have a responsibility to ensure the company complies with legal obligations and requirements. Unlike the EU and Canada, which have omnibus privacy laws protecting personal information, the U.S. has a complex patchwork of privacy and security laws and regulations that apply to various industry sectors and types of information. Personal information can be protected by constitutions, laws, regulations, case law, and contracts between parties. At the state level, laws commonly protect arrest records and criminal justice data, bank records, cable television subscriber data, credit information, employment data, insurance information, mailing lists, medical and health data, polygraph results, school records, social security numbers, tax records, and telephone service and solicitation records. Federal laws protect all of the foregoing (except arrest records) plus Government data banks and wiretap information.¹⁸

In addition to compliance with non-disclosure agreements and other contractual or legal agreements, several recent laws enacted by Congress impose considerable privacy and security requirements on health information, financial information, and Government information and systems. They *each* require an enterprise approach to security, involving the senior management of the organization. Cumulatively, they impact a large portion of private sector systems. The three major laws directly impacting corporate security programs are:

- The Health Insurance Portability and Accountability Act (HIPAA);
- The Gramm-Leach-Bliley Act (GLBA); and
- The Federal Information Security Management Act (FISMA).

While not specifically mandating security measures, the Sarbanes-Oxley Act of 2002 is also drawing attention to information security programs. Critical infrastructure (CI) industries also live under a veiled threat of regulation due to inadequate security programs.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) protects “Individually Identifiable Health Information” and imposes extensive privacy and security regulations on health care providers, claims processors, insurance companies, and businesses.¹⁹ By extension, HIPAA also applies to “business associates” of covered entities.²⁰ HIPAA’s privacy and security requirements are quite broad. Section 1320d-2(d)(2) of HIPAA states:

¹⁸ *Privacy Laws by State* (excerpted from *Compilation of State and Federal Privacy Laws*, 1997 ed., by Robert Ellis Smith and *Privacy Journal*), <http://www.epic.org/privacy/consumer/states.html>.

¹⁹ Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191, 42 U.S.C. § 1320d, <http://www.hipaadvisory.com/regs/law/index.htm> (hereinafter “HIPAA”); Information on HIPAA privacy, security, and electronic transaction regulations can be found at <http://www.hipaadvisory.com/regs/index.htm>.

²⁰ 45 C.F.R. § 160.103 (definition).

Each [covered entity] who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards –

- (A) to ensure the integrity and confidentiality of the information;
- (B) to protect against any reasonably anticipated –
 - (i) threats or hazards to the security or integrity of the information; and
 - (ii) unauthorized uses or disclosures of the information; and
- (C) otherwise to *ensure compliance with this part by the officers and employees of such persons.*²¹

The regulations, however, can be quite granular. HIPAA’s Security Regulation covers data while both in storage and transit and has 28 “standards” and 41 “implementation specifications.” There are administrative, physical, and technical aspects to the rule. The rule requires that an enterprise approach be taken with policies, procedures, change control mechanisms, risk analysis, review, and training.²² The Security Regulation takes into account technical capabilities of record systems, costs of security measures, the need for personnel training, and the value of audit trails in computerized record systems.

HIPAA compliance concerns are backed up by criminal penalties. Wrongful disclosure of individually identifiable health information carries up to a year in prison and up to a \$50,000 penalty. If the wrongful disclosure is under false pretenses, the maximum term rises to five years, and the monetary penalty to \$100,000; add an intent to sell, transfer, or use for commercial advantage, personal gain, or to inflict malicious harm, and the prison term increases to a maximum of 10 years, with a monetary penalty of up to \$250,000.²³

Gramm-Leach-Bliley Act (GLBA) and Financial Guidance

The Gramm-Leach-Bliley Act (GLBA),²⁴ states that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."²⁵ The GLBA definition of “financial institutions” encompasses banks, securities firms, insurance companies, and other companies providing many types of financial products and services to consumers. This includes lending, brokering or servicing any type of consumer loan; transferring and safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; providing residential real estate settlement services; collecting consumer debts; and other types of financial

²¹ HIPAA, 42 U.S.C. § 1320d-2(d)(2) (emphasis added).

²² Linda A. Malek and Brian R. Krex, “HIPAA’s security rule becomes effective 2005,” *The National Law Journal*, Mar. 31, 2003 at B14; *see also* Chapter Five, Security Plans, Policies & Procedures.

²³ HIPAA, 42 U.S.C. § 1177(b).

²⁴ Gramm-Leach-Bliley Act of 1999, Pub. Law 106-102, 113 *Stat.* 1338 (1999), http://www.ffiec.gov/ffiecinfobase/resources/management/con-15usc_6801_6805-gramm_leach_bliley_act.pdf (hereinafter “GLBA”).

²⁵ GLBA, 15 U.S.C. § 6801, <http://www4.law.cornell.edu/uscode/15/6801.html>.

services.²⁶ GLBA's definition of financial institutions has even swept up colleges and universities.²⁷

Pursuant to the GLBA, the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and Federal financial regulatory bodies²⁸ have issued regulations requiring administrative, technical and physical safeguards for financial information. The statute specifies that the regulations are intended:

- 1) To ensure the security and confidentiality of customer records and information;
- 2) To protect against any anticipated threats or hazards to the security or integrity of such records; and
- 3) To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.²⁹

The regulations set forth the required steps that must be taken, but they do not specify what the technical components of a safeguards program must be. For example, the Federal Trade Commission requires that financial institutions under its purview must develop a plan in which the institution must: (1) designate one or more employees to coordinate the safeguards, (2) identify and assess the risks to customers' information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks, (3) design and implement a safeguards program, and regularly monitor and test it, (4) select appropriate service providers and contract with them to implement safeguards, and (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firms business arrangements or operations, or the results of testing and monitoring of safeguards.³⁰

In addition to GLBA, there are also standards and guidance for financial system security. The Federal Financial Institutions Examination Council's (FFIEC) *IT Examination Handbook* sets forth an enterprise and process approach to information security. This follows the same approach the FFIEC took in its "Guidelines to Establishing Standards to Safeguard Customer Information" regarding implementation of the GLBA.³¹ In addition, the Office of the Comptroller of the Currency (OCC), which regulates and supervises national banks, has formally advised banks to safeguard against the threats and vulnerabilities of cyber terrorist attacks.³²

²⁶ "Financial Privacy: The Gramm-Leach Bliley Act," <http://www.ftc.gov/privacy/glbact/>.

²⁷ "Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information," *NACUBO Advisory Report 2003-01*, National Association of College and University Business Officers, Jan. 13, 2003, http://info-center.ccit.arizona.edu/~security/GLBA_Summary.pdf.

²⁸ The Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Board of Directors of the Federal Deposit Insurance Corporation, the Director of the Office of Thrift Supervision, and the National Credit Union Administration.

²⁹ GLBA, 15 U.S.C. § 6801, <http://www4.law.cornell.edu/uscode/15/6805.html>.

³⁰ See "Financial Institutions and Customer Data: Complying with the Safeguards Rule," <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>.

³¹ FFIEC Examination Handbook at 1.

³² See "Infrastructure Threats from Cyber-Terrorists," Office of Comptroller of the Currency, OCC 99-9, Message to Bankers and Examiners, Mar. 5, 1999, <http://www.occ.treas.gov/ftp/bulletin/99%2D9.txt>.

The World Bank also has been a leader in the area of financial security of electronic transactions. Through a series of papers, reports, presentations, and events, The World Bank has made a global contribution toward “connecting the dots” in the security of financial transactions.³³ The Bank’s *Electronic Security: Risk Mitigation in Financial Transactions—Public Policy Issues* sets forth “The 12 Layers of Security,”³⁴ which has been implemented by The World Bank Treasury, incorporated in the Monetary Authority of Singapore’s Risk Management Guidelines, and added to the latest ISO Information Security Banking Standard 13569.³⁵

*Federal Information Security Management Act (FISMA)*³⁶

Title III of the E-Government Act of 2002, also known as The Federal Information Security Management Act (FISMA), added several requirements for the security of Government systems.³⁷ FISMA also applies (1) to private sector contractors who process Government information or operate systems on behalf of the Government, and (2) when Federal information is used within equipment that is acquired by a Federal contractor incidental to a Federal contract.

Under FISMA, the term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability of information.³⁸ FISMA requires the head of each Federal agency to provide certain information security protections for agency information and systems and to ensure that information management security processes are integrated with agency strategic and operational planning processes.

Taking an enterprise approach, consistent with security best practices, FISMA requires the head of each agency to develop, document, and implement an agency-wide information security program to provide security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or entity. This includes:

³³ See, e.g., Thomas Glaessner, Tom Kellermann, and Valerie McNevin, *Electronic Security: Risk Mitigation in Financial Transactions—Public Policy Issues*, The World Bank, June 2002, [http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/\(attachmentweb\)/E-security-RiskMitigationversion3/\\$FILE/E-security-Risk+Mitigation+version+3.pdf](http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/E-security-RiskMitigationversion3/$FILE/E-security-Risk+Mitigation+version+3.pdf) (hereinafter “Glaessner, Kellermann, and McNevin”); Thomas Glaessner, Tom Kellermann, and Valerie McNevin, *Electronic Security: Risk Mitigation in Financial Transactions—Summary of Recent Research and Global Dialogues*, The World Bank, May 2003, http://www.worldbank.org/wbi/B-SPAN/sub_e-security.htm (hereinafter “World Bank Financial Security Summary”).

³⁴ Glaessner, Kellermann, and McNevin at 51-52.

³⁵ An updated version of ISO/TR 13569 which incorporates the 12 Layers of Security will be released mid-2003, see <http://www.iso.org/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=13569>.

³⁶ This portion of the testimony is taken from a section of Westby – Cyber Security (pp. 49-54) of which I own the copyright.

³⁷ Federal Information Security Management Act, Title III of E-Government Act of 2002, Pub. Law 107-347, <http://csrc.nist.gov/policies/FISMA-final.pdf> (hereinafter “FISMA”).

³⁸ 44 U.S.C. § 3542.

- Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or systems;
- Policies and procedures that are based on the risk assessments and ensure compliance with security guidance and standards;
- Security awareness training to inform personnel, contractors, and other users of information systems that support the operations and assets of the agency of:
 - (a) information security risks associated with their activities; and
 - (b) their responsibilities in complying with agency policies and procedures designed to reduce these risks;
- Periodic testing and evaluation (not less than annually) of the effectiveness of information security policies, procedures, and practices, which includes testing of management, operational, and technical controls;
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Sarbanes-Oxley Act of 2002

Although the Sarbanes-Oxley Act of 2002³⁹ does not specify information security measures, it does require officers of public companies to attest to the appropriateness and integrity of the financial data reported in SEC filings⁴⁰ and to assess and report on the effectiveness of the internal control structure and procedures for financial reporting.⁴¹ In today's business environment, financial data is digital and processed and stored in a variety of ways. Therefore, the legal requirements of Sarbanes-Oxley are directly dependent upon the integrity of the IT systems processing the data.

Critical Infrastructure

Section 2 of the U.S. Homeland Security Act defines "critical infrastructure" (CI) as having the same meaning as that used in the USA PATRIOT Act:

³⁹ Sarbanes-Oxley Act of 2002, Pub. Law 107-204, § 302, <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf> (hereinafter "SOX").

⁴⁰ SOX, § 302.

⁴¹ SOX, § 404.

[T]he term “critical infrastructure” means systems and assets, whether physical or virtual, so vital to the ... [nation] that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

The National Strategy for Homeland Security, released by the White House on July 16, 2002, lists the following as critical infrastructure:

- ◆ Agriculture
- ◆ Food
- ◆ Water
- ◆ Public health
- ◆ Emergency services
- ◆ Government
- ◆ Defense industrial base
- ◆ Information and telecommunications
- ◆ Energy
- ◆ Transportation
- ◆ Banking and finance
- ◆ Chemical industry and hazardous materials
- ◆ Postal and shipping.

The Administration has grown increasingly nervous about the fragility of our nation’s critical infrastructure and the lack of attention from boards and senior management to fully engage on the security of these infrastructures, including their supervisory control and data acquisition (SCADA) and supporting IT systems. To that end, the Administration issued the *National Strategy for the Protection of Critical Infrastructure and Key Assets*⁴² and the *National Strategy to Secure Cyberspace*⁴³ identifying the key measures that need to be taken to ensure these assets are available when needed and secure from attack. Subsequently, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7), which establishes a national policy for Federal departments and agencies to identify and prioritize CI and key resources and protect them from terrorist attacks.⁴⁴ Although there are no mandated requirements for the security of critical infrastructure, there have been repeated warnings that the Administration would ask Congress to enact legislation requiring comprehensive security programs if senior management did not step up to the plate.⁴⁵ HSPD-7 makes regulation that much easier and provides a

⁴² *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Mar. 4, 2003, <http://www.whitehouse.gov/pcipb/physical.html>.

⁴³ *The National Strategy to Secure Cyberspace*, Feb. 14, 2003, http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

⁴⁴ Homeland Security Presidential Directive / HSPD-7, “Critical Infrastructure Identification, Prioritization, and Protection,” Dec. 17, 2003, <http://www.fas.org/irp/offdocs/nspd/hspd-7.html>.

⁴⁵ See, e.g., Martin Edwin Anderson and Tim Starks, “Government and Industry Struggle to Build a Post-9-11 Partnership,” *Congressional Quarterly Homeland Security*, 2004, <http://www.ewa-iit.com/content.asp?sectionID=6&contentID=137>; Michael Singer, “National Cyber Security Initiative Still Stalling,” *eSecurityPlanet.com*, Dec. 3, 2003, <http://www.ewa-iit.com/content.asp?sectionID=6&contentID=137>.

legitimate justification for doing so in the name of national and economic security and public safety.

Situation Today

Senior executives of an organization should regard cyber security as a management opportunity rather than a technical problem. The good news is that a number of factors are moving companies toward the development of robust security programs. Two of the most obvious are increasing connectivity and raised awareness regarding (1) vulnerabilities and threats and (2) the availability of best practices, standards, and guidance.

In addition, some excellent reference materials have been developed that guide directors and officers through the digital governance process. The *International Guide to Cyber Security* sets forth a comprehensive list of non-technical, *management* questions in the areas of assessment, security program, internal controls, implementation, and compliance and enforcement.⁴⁶ Of course, the heightened emphasis on corporate governance and the responsibilities of executives to take action to protect market share, stock price, and corporate reputation is also helping.

Now the bad news. There is a growing knowledge base and evidence of:

- Collaboration between terrorist organizations and organized crime in the areas of drug trafficking, money laundering and other forms of financial crime, and weapons trafficking, among others. Identify theft can play a significant role in all of these crimes.⁴⁷
- Terrorists' use of IT to communicate and conspire on attacks against critical infrastructure. In fall 2001, the Mountain View, California, police department requested FBI assistance in investigating suspicious surveillance of computer systems controlling utilities and government offices in the San Francisco Bay Area. The digital snooping was being done by Middle Eastern and South Asian browsers. The FBI found "multiple casings of sites" through telecommunications switches in Saudi Arabia, Indonesia, and Pakistan that focused on emergency telephone systems, electrical generation and transmission equipment, water storage and distribution systems, nuclear power plants, and gas facilities across the U.S. Some of the electronic surveillance focused on the remote control of fire dispatch services and pipeline equipment. Subsequently, information about those devices, including details on how to program them, was found on Al Qaeda computers seized this year.

The U.S. Government has expressed concern that terrorists are targeting the junctures between physical and virtual infrastructures, such as electrical substations handling hundreds of thousands of volts of power or panels controlling dam floodgates. According to a recent *Washington Post* report, one Al Qaeda laptop found in Afghanistan had frequented a French website that contained a two-volume online

⁴⁶ Westby – Cyber Security at 194-96.

⁴⁷ See, e.g., "The Fusion Task Force," Interpol, Sept. 20, 2004, <http://www.interpol.com/Public/FusionTaskForce/default.asp>.

“Sabotage Handbook” on tools of the trade, planning a hit, switch gear and instrumentation, anti-surveillance methods, and advanced attack techniques. An Al Qaeda computer seized in January 2002 in Afghanistan contained models of a dam, complete with structural architecture and engineering software that enabled the simulation of a catastrophic failure of dam controls. Other computers linked to Al Qaeda visited Islamic chat rooms and had access to “cracking” tools to search networked computers and find and exploit security holes to gain entry or full command. Additionally, evidence obtained from browser logs indicate Al Qaeda operatives spent time on sites that offer software and programming instructions for digital switches that run power, water, and transport and communications grids. Al Qaeda prisoners have reportedly admitted to planning to use such tools. These systems are especially vulnerable because many of the distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems that control critical infrastructure are connected to the Internet but lack even rudimentary security. In addition, the technical details regarding how to penetrate these systems are widely discussed in technical fora, and experts consider the security flaws to be widely known.⁴⁸

- Cyber incidents that cascade and domino through systems, affecting, and possibly endangering, millions of people.⁴⁹
- The inability or difficulty to track and trace cyber incidents. The original engineering of the Internet did not anticipate that it would support the global economy and link businesses and process transactions. The Internet was designed for a trustworthy population of scientists and researchers and, therefore, did not originally incorporate the ability to track and trace user behavior. For example, Internet Protocol (IP) addresses can be readily “spoofed” by attackers to hide their true source of attack. Due to the poor state of security throughout the Internet, computers are easily taken over by attackers and used as “stepping stones” to hide their tracks or amplify their attacks. Also, a large number of IP addresses are dynamically assigned, requiring extensive cooperation among Internet Service Providers (ISPs) and law enforcement when trying to track and trace incidents to actual individuals. Even when tracing is possible, if a packet has been routed through a foreign country or if the perpetrator is located overseas, jurisdictional issues are burdensome and time consuming, international cooperation of law enforcement may be difficult or impossible, and any search and seizure of evidence may be performed in a manner that renders it inadmissible in a U.S. court.⁵⁰

In light of the foregoing, it is hard to conceive that conducting risk assessments and following best practices would increase a company’s risk of liability. In fact, the contrary conclusion is

⁴⁸ Toward a Universal Order of Cyberspace at 10 (citing " Barton Gellman, “Cyber-Attacks by Al Qaeda Feared,” *Washington Post*, June 26, 2002, <http://www.washingtonpost.com/wp-dyn/articles/A50765-2002Jun26.html>).

⁴⁹ Jody R. Westby, “Cyber Realities: From Worms to Warfare,” NATO Forum on Business & Security, Berlin, Feb. 2004.

⁵⁰ Jody R. Westby, ed., *International Guide to Combating Cybercrime*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, ABA Publishing, 2003, <http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450030>.

apparent: boards and senior management who wish to ignore digital governance and risk management actually *increase* the likelihood of corporate and personal liability in the event of a cyber incident.

Solving the Problem

Some corporations may ask their counsel to conduct any risk assessments performed, hoping to protect it under the cloak of attorney work product.⁵¹ This privilege can provide some degree of protection from disclosure of certain audit or risk assessment information when specific conditions are met. Generally, the attorney work product privilege established in *Hickman v. Taylor*,⁵² protects from disclosure materials prepared by attorneys “in anticipation of litigation.” Such work product includes an attorney’s thoughts, litigation plan or strategy, evaluation of facts and evidence, and legal theories relevant to his client’s case.⁵³ However, the “anticipation of litigation” requirement places a significant limitation on this privilege.⁵⁴ “[A]t the very least, some articulable claim, likely to lead to litigation, must have arisen.”⁵⁵ Thus, it is not likely that this privilege will afford substantial protections.

I tend to favor market solutions over regulation. I believe there are approaches open to Congress that would both motivate the private sector and result in dramatic improvements to our computer systems and networks. The most obvious solution is to provide tax credits to corporations that implement enterprise security programs. Such credits could encompass risk assessments, implementing best practices and standards, establishing internal controls, integrating security into the capital planning and investment process, and training. Another initiative could provide Government grants or funding to academia, private sector entities, and our national laboratories to help advance the development of models to effectively measure return on investment of security programs and other tools that would help boards and senior management through the decision-making processes regarding cyber security.

Lastly, I would like to draw the Subcommittee’s attention to the three books recently published by the American Bar Association’s Privacy & Computer Crime Committee: *The International Guide to Combating Cybercrime* (2003), the *International Guide to Cyber Security* (2004), and the *International Guide to Privacy* (2004). The *Roadmap to an Enterprise Security Program* will be published within the next month. These books dovetail the legal, technical, managerial, and operational aspects of privacy, security, and cybercrime and guide the reader through the development of an enterprise security program.

⁵¹ See generally, Westby Cyber-Security at 244-46.

⁵² *Hickman v. Taylor*, 329 U.S. 495 (1947) (codified as Federal Rules of Civil Proc. P 26(b)(3).

⁵³ *Id.* at 510.

⁵⁴ *Coastal States Gas Corp. v. Dep’t of Energy*, 199 U.S. App. D.C. 272; 617 F.2d 854, 864 (1980). State law, however, may differ on this rule. For example, under California Civ. Proc. Code 2018, there is not mention of the “anticipation of litigation” requirement and California courts have ruled according to this statute that the privilege also applies to the work product of an attorney when he acts as counselor in a nonlitigation capacity. See *Casualty & Surety Co. v. Superior Ct*, 153 Cal. App. 3d 467, 478-479 (1984); *Rumac, Inc. v. Bottomley*, 143 Cal. App. 3d 810, 815-16 (1983).

⁵⁵ *Id.* at 864.

The books were written by an international, multidisciplinary team of technical experts, attorneys, industry representatives, government officials, NGO representatives, and members of academia. We recognize that our national and economic security and the protection of our citizens from an array of threats, ranging from identity theft to terrorist attacks on critical infrastructure, is, in part, dependent upon the security of the networks in the nearly 200 countries connected to the Internet. Our ability to prosecute cybercrimes is dependent upon trained law enforcement and prosecutors and inter-governmental cooperation in those 200 countries. Our ability to protect private information is also dependent upon our ability to guide developing countries toward good cyber security practices, laws, and policies.

To that end, the ABA is making all four of these publications available free of charge to persons in developing countries. The *Cybercrime* book has already been translated into one language, and we hope to obtain funds for the translation of all the publications into Russian, Spanish, and Chinese so they might reach a global audience through workshops and their use as textbooks. Congressional funding for these types of translation and workshop efforts would significantly increase our ability to combat cybercrime and secure our networks against catastrophic or costly attacks.

Mr. Chairman and Members of the Subcommittee, I thank you for your consideration and this opportunity.