Information Security Governance Of Enterprise Information Systems: An Approach To Legislative Compliant

Benjamin Khoo, New York Institute of Technology, USA
Peter Harris, New York Institute of Technology, USA
Stephen Hartman, New York Institute of Technology, USA

ABSTRACT

Enterprises are now operating in the network economy. The network economy is dependent on the information infrastructure via the Internet. Organizations of all types (business, academia, government, etc.) are facing risks resulting from their ever-increasing reliance on the information infrastructure. Because of this, the US government implemented a number of legislations to secure cyberspace. This paper will examine the issue of Information Security Governance (ISG) of an enterprise information system, it will elaborate on the ISG framework, discuss the legislations and finally, assess how ISG can be framed to meet legislations to show due diligence and continuous process monitoring.

Keywords: Information Security, Governance, Enterprise Information Systems

INTRODUCTION

The technological explosion of the Internet in the late 1980s and early 1990s has resulted in a paradigm shift that has affected all aspects of our lives; an emerging trend is a movement toward network centric computing. The term Enterprise Information Systems (EIS) is used to refer to the enterprise-wide computer-based systems that gather and store data, process information and generate reports for management. EIS are now operating in the network economy with expansion to the external stakeholders. The network economy is dependent on the information infrastructure. Each day millions of dollars of business transactions and many communication channels flow through the information infrastructure via the Internet. Organizations of all types (business, academia, government, etc.) are facing risks resulting from their ever-increasing reliance on the information infrastructure. Businesses, government, and non-profit institutions have been found wanting in information security. The high risks in cyberspace needs to be mitigated and managed. Because of this, the USA government implemented a number of National Security Presidential Directives (NSPD) and legislations to secure cyberspace. Information Security Governance (ISG) is a pro-active way of mitigating these risks. This paper will examine the issue of Information Security Governance of an enterprise information system, it will elaborate on the ISG framework, discuss the legislations and finally, assess how ISG can be framed to meet legislations to show due diligence and continuous process monitoring.

CURRENT INFORMATION SECURITY GOVERNANCE LANDSCAPE

Businesses and organizations in the US have come to the realization that security is more than just a technical issue (Allen, 2006). Adapting the definition from (Whitman & Mattord, 2004), information security is the protection of the confidentiality, integrity and availability of information and its critical elements, including the software and hardware that use, store, process and transmit that information through the application of policy, technology, education and awareness. Leaders at the highest level of businesses, organizations and governments are coming to realize that effective security in today's network economy requires securing the confidentiality, integrity and availability of information assets in four dimensions – the technical (hardware and software), physical (media, building, equipment, etc), organizational (IT alignment, structure, corporate governance, legal, etc) and managerial (policies, procedures, etc) aspects of the asset.

This paradigm shift has elevated information security to the upper echelon of corporate management as an enterprise-wide issue. Information security is now a business problem. The enterprise will have to utilize all the available resources to manage the security risks and make information security a core part of business operations by integrating it into the existing internal controls and policies that constitute corporate governance.

Quoting F. William Conner, Chairman, CEO and President, Entrust Inc. (Entrust, 2004), "By integrating information security into our corporate governance processes, we can allow for the deep integration with customers, suppliers, partners and other stakeholders that is so important to the extended enterprise, while protecting the critical infrastructure that is a cornerstone of our homeland security."

According to (IT Governance Institute, 2003), information security governance consists of the organizational structures, processes and leadership that safeguard information. Effective communication amongst all parties based on constructive relationships, a common language and shared commitment to addressing the issues are critical to the success of these structures and processes. The five basic outcomes of information security governance include: value delivery by optimizing information security investments in support of organizational objectives; strategic alignment of information security with business strategy to support organizational objectives; resource management by utilizing information security knowledge and infrastructure efficiently and effectively; risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level; and performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved.

Information Security Governance (ISG) is a subset of corporate governance that relates to the security of information systems. (Allen, 2005) defined "governing for enterprise security" as "directing and controlling an organization to establish and sustain a culture of security in the organization's conduct (beliefs, behaviors, capabilities and actions) …treating adequate security as a non-negotiable requirement of being in business."

The huge volume of business transactions that are processed through the information infrastructure via the Internet makes it a prime target for online criminals. The confidentiality, integrity and availability of information assets, the privacy of individuals, the accountability and integrity of the transactions are threatened. As a result, the USA government implemented a number of National Security Presidential Directives (NSPD) and legislations to secure cyberspace.

As the 21st century gets more competitive, businesses, governments and organizations continue to push the envelope of the extended enterprise by extending deeper access to their information assets and services while at the same time balancing their compliance with the myriad legislations around information privacy and corporate governance. Secure information systems provide the support for maintaining the balance (Entrust, 2004). See Figure 1.

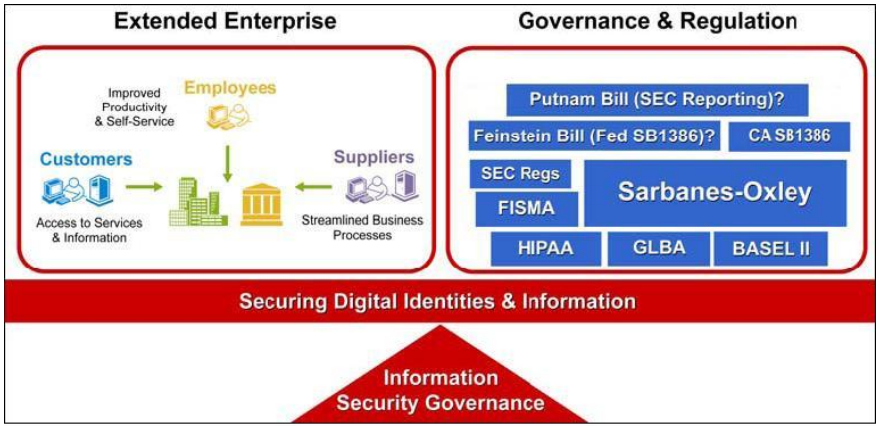

Figure 1. Balancing the Extended Enterprise with Governance and Regulation (Entrust, 2004).

Cyberspace cannot be secured just by depending on government officials or CIOs. Organizations must elevate the issue to a corporate governance priority in order to systematically strengthen information security at all levels of the organization. Boards and CEOs who treat it as corporate governance issue best address US information security; this resulted in the formation of the Corporate Governance Task Force in December 2003. Its goal is to develop and promote a coherent governance framework to drive implementation of effective information security programs. Information security is a governance challenge that involves risk management, reporting and accountability from top-level executive management. This private sector Corporate Governance Task Force subsequently developed a framework for organizations to improve ISG on a voluntary basis. The ISG framework was documented in the report (CGTF, 2004), "Information Security Governance: A Call to Action", released in April 2004 and is available online at http://www.cyberpartnership.org. This report recommended an ISG framework that facilitates organizational self-evaluation and mitigation of information security issues while complying with various legislations.

ISG FRAMEWORK

The ISG framework includes recommendations and tools that will enable organizations to create or improve their ISG. This framework will enable organizations to enhance the process of securing information systems, complying with regulations, increasing business process efficiency and strengthening homeland security. (CGTF, 2004) The ISG framework provides guidelines to ensure "the effectiveness of information security controls over information resources; to provide effective management and oversight of the related information security risks; to provide for development and maintenance of minimum controls required to protect an organization's information and information systems, and; to provide a mechanism for oversight of the information security program." (CGTF, 2004, p. 12). The major elements of the ISG framework include (CGTF, 2004):

1. **Organizational Responsibilities and Authority**: Describes the significant role each member of an organization plays in ISG, from the Board of Directors/Trustees to the employees.
2. **Information Security Program Components**: Describes the essential components of an information security program, with detailed guidance specified in the security practices based on accepted international standards like ISO/IEC 27001/BS17799, Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Controls-Integrated Framework and Control Objectives for Information and Related Technology (COBIT®). This includes assessment, policies and procedures, training, testing, remediation of risks, detection and response to incidents and business continuity planning.
3. **Reporting and Independent Evaluation Recommendations**: Describes how each independent organizational unit should assess, remediate and report on its information security program including the contents, frequency and audience for reporting to satisfy governance oversight requirements. In addition, if appropriate, each year an independent information security program evaluation should be completed in accordance with generally accepted auditing standards and the results reported to the Board of Directors/Trustees.

The threats to the information infrastructure have resulted in the US government implementing new legislations to address those threats. Legislations can be logically separated into criminal laws and laws implementing security requirements for critical infrastructure.

LEGISLATIONS

The advent of the Internet has blurred the traditional borders between states and nations. People of every nation are now able to interact on a daily basis. The use of the Internet to facilitate trans-border commerce provides Congress with the power to establish Federal legislation defining legally acceptable behavior involving computers and information technology (United States Constitution, Article I). The use of the Internet for interstate and international communication requires that information security professionals are aware of legislation affecting network security (Robinson, 2003a). The US government's legislation regulates either criminal activity or national defense in information security. There are two definitions of the term "computer crime": (1) the use of a computer by a criminal to conduct illegal activity or (2) a computer as the target of illegal activity (Robinson, 2003c). Congress has instituted Federal legislations regulating criminal activity involving information technology in an

attempt to address these two facets of computer crime including the Computer Fraud and Abuse Act (CFAA) and Electronic Communications Protection Act (ECPA). Two important national defense in information security legislations implemented include Gramm-Leach-Bailey (GLB) Act and Sarbanes-Oxley Act (SOX) for the financial industry.

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA") is the primary computer crime statute in the United States. According to (Robinson, 2003c), the CFAA imposes criminal liability for:

1. Knowingly accessing a computer without authorization, or in excess of authorization, and obtaining classified information;
2. Intentionally accessing a computer without authority and obtaining consumer financial information, information from any department or agency of the federal government, or information from any protected computer where access involves an interstate or foreign communication;
3. Intentionally accessing, without authorization, a non-public computer of any department or agency of the federal government that is either used exclusively for governmental purposes, or with respect to a computer that is not used exclusively for government purposes, where the conduct affects the use of that computer by or for the federal government;
4. Knowingly, and with wrongful intent, accessing a protected computer, without authorization or in excess of authorization, and by doing so, obtaining anything of value, other than the use of the computer itself (if the value of the computer use is less than $5,000 in any one year);
5. Knowingly causing the transmission of a program, information, code, or command, and by doing so, intentionally causing unauthorized damage to a protected computer; or recklessly or negligently causing damage to a protected computer by intentionally accessing that computer without authorization or in excess of authorization;
6. Knowingly, and with wrongful intent, trafficking in user names, passwords or other access credentials through which a computer may be accessed without authorization, if that conduct affects interstate or foreign commerce or if the computer is used by or for the federal government; or
7. With the intent to extort money or anything of value from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, transmitting in interstate or foreign commerce any communication containing a threat to damage a protected computer [18 U.S.C. §§ 1030 (a)(1)-(7)].

Sentencing for computer crimes is different from that taken under pre-information age criminal law. A breach of security with respect to only a small amount of data can be a very serious computer crime compromising government or industry secrets. Accordingly, sentences under the CFAA are graduated in terms of the state of mind of the perpetrator and the type of information taken. See Table 1 below.

Table 1. Table of CFAA Offense and Punishment (Robinson, 2003c)

Offense	Punishment
Whoever **intentionally** accesses a protected computer without authorization, and **because of such conduct, causes damage**. 18 U.S.C. § 1030 (a)(5)(c)(emphasis supplied).	**1st Offense or Attempt**: Imprisonment for not more than one year, fine or both. 18 U.S.C. §1030 (c)(2)(A). **Subsequent Offense or Attempt**: Imprisonment for not more than ten years, fine or both. 18 U.S.C. §1030 (c)(3)(B).
Offense: Whoever having **knowingly** accesses a computer without authorization or exceeding authorized access, and by means of such conduct having **obtained information that has been determined by the United States Government ... to require protection against unauthorized disclosure for reasons of national defense or foreign relations, ... with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it."** 18 U.S.C. § 1030(a)(1)(emphasis supplied).	**1st Offense or Attempt**: Imprisonment for up to 10 yrs., fine or both. **Subsequent Offense or Attempt**: Imprisonment for up to 20 yrs., fine or both. 18 U.S.C. §1030 (c)(1).

According to (Robinson, 2003b), the primary thrust of the CFAA, with respect to private sector systems, is to prohibit access to protected computers without authorization or exceeding authorization, whether to obtain something of value or to damage systems or data. The primary concern of the ECPA is related, but distinct. The ECPA prohibits the unauthorized and unjustified interception, disclosure or use of communications, including "electronic communications." The ECPA has two major parts (Robinson, 2003b): Title I - The Wiretap Act, 18 U.S.C. §§ 2510-22 (the "Wiretap Act"); and Title II, the Stored Communications Act, 18 U.S.C. §§ 2701-12. (the "Stored Communications Act"). Under the Wiretap Act, "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce, but does not include - (A) any wire or oral communication (defined as aural communications in the statute); (B) any communication made through a tone-only paging device; (C) any communication from a tracking device; or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds. 18 U.S.C. § 2510 (12). The Stored Communications Act imposes civil and criminal penalties for the intentional, unauthorized access to an electronic communication service facility to obtain, alter or prevent authorized access to, a stored wire or electronic communication.

The Gramm-Leach-Bailey (GLB) Act requires financial institutions to protect the confidentiality and integrity of the personal information of consumers. The Federal Trade Commission (FTC) because of GLB issued the Safeguards Rule, which requires financial institutions under its jurisdiction to have measures in place to keep customer information secure. Financial institutions include businesses like check-cashing businesses, credit-reporting agencies to courier services. A secure business is one that has effective coordination and oversight, regular risk assessment and prompt response to new developments. The Safeguards Rule requires companies to develop an appropriate information security plan that describes how consumer information is protected. According to (http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus54.shtm), each company must:

1. designate one or more employees to coordinate its information security program;
2. identify and assess the risks to customer 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 service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
5. evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

In addition, businesses will have to address risks to consumer information in all areas of operations in particular 3 areas – Employee Management and Training, Information Systems and, Detecting and Managing System Failures.

The US Congress passed the Sarbanes-Oxley Act (SOX) in 2002 in response to public outcry over the financial scandals that rocked the corporate world such as those at Enron, WorldCom, etc. Top executives of big corporations took advantage of poor internal control and reporting systems to misstate the actual financial results of the corporation for personal gains. The SOX is of particular interest because it focuses on corporate governance, mandates stronger internal controls and institutes personal liability for top executives of companies that are publicly traded in the United States. SOX support a simple premise: good corporate governance and ethical business practices are now required by law! The adoption of IT by businesses has thrust IT controls to the forefront because of SOX. Thus, SOX has a compelling impact on corporate governance and IT governance. SOX specifically mentioned an international control framework for financial reporting from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Internal control is defined by COSO as a process, it is effected by people, it can only provide reasonable assurance and it is geared to achieve objectives in categories. As in the case of COSO, Control Objectives for Information and related Technology (COBIT) provides similar guidance to IT governance. COBIT requires that IT resources be managed by a set of 4 naturally grouped processes—Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. COBIT provides the needed information for management to reasonably assure the IT control structure and the information integrity for reporting purposes to comply with Section 404 of the SOX. It is important to note that the work

required to meet the Sarbanes-Oxley requirements not only ensures compliance but is an opportunity to establish strong governance models that ensure accountability, responsiveness to business needs and competitive advantage (Damianides, 2005).

The ISG framework (CGTF, 2004) can be implemented to meet these legislations passed by Congress. Associated with the ISG implementation is an ISG assessment tool when properly implemented by organizations will facilitate the incorporation of information security into an organization's corporate governance structure.

ISG ASSESSMENT TOOL

The ISG Assessment Tool is developed to support the ISG framework. The tool is intended to help organizations determine the degree to which they have implemented an ISG framework. The ISG assessment tool is divided into four sections (CGTF, 2004):

1. **Business Dependency**: Measures an organization's reliance on information technology for business continuity as well as the degree of sector interdependency and regulation.
2. **Risk Management**: Evaluates the risk management process as it relates to creating information securing strategy and program.
3. **People**: Evaluates the organizational aspects of the information security program.
4. **Processes**: Identify the processes that should be part of an information security program.

Details of the assessment matrix can be found in Appendix D of (CGTF, 2004).

The ISG framework provides a platform to develop metrics to assess an organization's compliance to the legislations and show due diligence and continuous process monitoring.

MOVING FORWARD

Embarking on an enterprise information security governance program (ESP) and acting on the tasks in the ISG framework requires tenacity and perseverance. There will be significant challenges along the way and may occur at all levels of the organization and throughout all phases of the ESP. Some challenges to consider often include: appreciating the enterprise-wide nature of the security problem, establishing the proper organizational structure and segregation of duties, overcoming the lack of a game plan, understanding complex global legal compliance requirements and liability risks, assessing security risks and the magnitude of harm to the organization, determining and justifying appropriate levels of resources and investment, dealing with the intangible nature of security, reconciling inconsistent deployment of security best practices and standards and overcoming difficulties in creating and sustaining a security-aware culture (Allen, 2007). The effectiveness of the ESP is enhanced if enterprises understand, anticipate and response to these challenges.

AUTHOR INFORMATION

Benjamin Khoo completed his Ph.D. (Information Systems) at the University of Maryland, Baltimore County. He is a member of two honor societies and was awarded the Phi Kappa Phi Dissertation Research Grant. He has published regularly in information systems journals. Prior to becoming an academician, he was a member of the Technical Staff (Software Engineer) of a large telecommunication Corporation.

Peter Harris is a professional accountant and is an Associate Professor of Accounting at The New York Institute of Technology. He completed his MBA degree at Columbia University in New York City. He has also worked for Ernst and Young LLP and is a member of several professional organizations.

Stephen Hartman is a Professor of Management at The New York Institute of Technology. He has extensive experience acting as a consultant to business, education, government, and the military.

REFERENCES

1. AESRM (2005) Convergence of Enterprise Security Organizations, The Alliance for Enterprise Security Risk Management, Booz Allen Hamilton, November 8, 2005.
2. Allen, Julia H. (2005) Governing for Enterprise Security, (CMU/SEI-2005-TN-023). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 2005.
3. Allen, Julia H. (2006) Security Is Not Just a Technical Issue, Build Security In Web Site, Department of Homeland Security, October 2006. Retrieved June 27, 2009, https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/management/563.html.
4. Allen, Julia H. (2007) Governing for Enterprise Security, CERT.org, February 2007.
5. Caralli, Richard. (2004) Managing for Enterprise Security, (CMU/SEI-2004-TN-046). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, December 2004.
6. CGTF (2004) Information Security Governance: A Call to Action, Corporate Governance Task Force, April 2004. Retrieved June 20, 2009, from http://www.cyberpartnership.org.
7. Damianides, Marios. (2005) Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance, *Information Systems Management*, Winter 2005.
8. Entrust Inc. (2004) Information Security Governance (ISG): An Essential Element of Corporate Governance, April 2004.
9. Herrmann, Debra S. (2007) *Complete Guide to Security and Privacy Metrics*, Auerbach Publications, 2007.
10. IT Governance Institute (2003) Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition. http://www.itgi.org.
11. Robinson, S. (2003a) (February 2, 2003.) "U.S. Information Security Law, Part 1." Retrieved June 27, 2009, from http://www.securityfocus.com/infocus/1669.
12. Robinson, S. (2003b) Robinson, S. (April 1, 2003.) "U.S. Information Security Law, Part 2." Retrieved June 27, 2009, from http://www.securityfocus.com/infocus/1681.
13. Robinson, S. (2003c) Robinson, S. (May 12, 2003.) "U.S. Information Security Law, Part 3." Retrieved June 27, 2009, from http://www.securityfocus.com/infocus/1693.
14. Robinson, S. (2003d) Robinson, S. (July 9, 2003.) "U.S. Information Security Law, Part Four." Retrieved June 27, 2009, from http://www.securityfocus.com/infocus/1710.
15. Steven, John. (2006) Adopting an Enterprise Software Security Framework, *IEEE Security & Privacy*, IEEE Computer Society, March/April 2006.
16. United States Constitution, Article I Retrieved June 27, 2009, from http://www.law.cornell.edu/constitution/constitution.articlei.html#section8.
17. Michael E. Whitman, Herbert J. Mattord (2008) *Principles of Information Security*, Edition Number: 3, Cengage Learning, January 2008

NOTES