IBIMA Publishing
Journal of Information Assurance & Cybersecurity
http://www.ibimapublishing.com/journals/JIACS/jiacs.html
Vol. 2011 (2011), Article ID 726196, 12 pages
DOI: 10.5171/2011.726196

A Framework for the Governance of Information Security in Banking System

Munirul Ula[1], Zuraini bt Ismail[2] and Zailani Mohamed Sidek[2]

[1]Engineering Faculty, Universitas Malikussaleh, Reuleut, Indonesia

[2]Advanced Informatics School, Universiti Teknologi Malaysia International Campus, Kuala Lumpur, Malaysia

Abstract

As modern banking increasingly relies on the internet and computer technologies to operate their businesses and market interactions, the threats and security breaches are highly increase in recent years. Insider and outsider attacks have caused global businesses lost trillions of Dollars a year. Therefore, that is a need for a proper framework to govern the information security in banking system. This paper highlights the information assets and potential threats for banking system. It further examines and compares the elements from the commonly used information security governance frameworks, standards and best practices. Their strength and weakness are considered in its approaches. This paper further proposes the initial framework for governing the information security in banking system. The framework is categorized into three levels which are strategic level, tactical, operational level, and technical level. This proposed framework will be implemented in real banking environment.

Keywords: Information Security Governance, Banking Corporate Governance, Information Security Governance Framework

Introduction

The growth of information technology has been so explosive in the recent decade. Computer has been widely applied in every aspect of our life from business, government, education, finance, health-care, and aerospace to defense system. With society's increasing dependency on information technology (IT), the consequences of computer crime can be extremely grave (Mahncke et al, 2009). Security breach and computer viruses cost global businesses $1.6 trillion a year and 39,363 human years of productivity. In 2009, Symantec has detected 59,526 phishing hosts around the globe, that number is increased by 7 percent compared to phishing hosts detected in 2008. The percentage of threats to confidential information is increased to 98 percent in 2009 compared to 83 percent in 2008, 89 percent of the threats have the ability to export user data and 86 percent of them have keystroke-logging component (Symantec, 2010).

Information system has become the heart of modern banking in our world today, and information has become the most valuable asset to protect from insiders, outsiders and competitors. Customers are very concerned about privacy and identity theft. Business partners, suppliers, and vendors are seeing security as the top requirement, particularly when providing mutual network and information access. Banks ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network services. Having a good reputation for safeguarding information will increase market share and profit. Banks are clearly responsible for compromised data in their possession that results in fraud. Therefore, banks have to be responsible for fraudulent activity perpetrated via the internet channel. Banks have to reimburse most customers for losses, although the customer clearly compromised their account credentials.

Most common technology risk or threat to banking and financial institution is phishing attack (Tubin, 2005). The typical phishing attack is based on social engineering, a tactic used by computer criminals to trick customers and employees into giving up confidential information like their account user names and passwords. With these credentials, the fraudster can penetrate networks, skim funds, and take over accounts. The other forms of attack, like spyware, trojan horses, and key-loggers, can cause a user to unwittingly download malware developed for the malicious intention of collecting various user information. The stolen information can be used for identity theft, which is a much more insidious prospect than the account skimming or account takeover associated with the more common phishing attacks. In an another incident in the year 2007, police of North Carolina, charged three cyber thieves for stealing US$ 450,000 from city's bank account at the City National Bank. The alleged thieves used valid login credentials to access the city's bank account and initiate the money transfers. Forensics investigation of the incident found that the city's login credentials were stolen via spyware installed on company-issued laptop computer (Vijayan, 2010). More recent accounted in New Jersey, a massive scheme to steal 500,000 bank accounts and personal information by a bank employee with the intention to sell it to bill collectors (MSNBC, 2010).

Empirical researches in Information Security Governance is noted to be lacking, and the majority of computer security methods and policies have evolved from case studies, anecdotal evidence, and the prescription of industry "leaders" (Qingxiong Ma, 2004). However, management of information security based on such anecdotes is not realistic. It must be based on sound scientific research and theory. To date, there are some information security governance frameworks, have been developed and widely practiced in developed countries such as United State and Europe, but each of them has its own advantages and weaknesses (Council III, 2006). Commonly, it must be customized to fit with organization structure and environment (Akhmad Syakhroza, 2003). Hence, this paper seeks to fill this research gap.

This paper is organized into five sections. This section introduces the background of the study and research concern. Section two portrays the literature review of information security governance in banking. Section three discusses commonly used information security governance frameworks and its comparison. The section four discusses the proposed ISG framework for banking system. Finally, the paper ends with conclusion.

Information Security Governance in Banking

There are several definitions on information security governance in the literatures. Academicians and practitioners have lack of consensus in the definition of Information Security governance (Rastogi and Von Solms, 2006). Moulton and Cole (2003) defined that information security governance is the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems. Harris (2006) summarized that information security governance is all of the tools, personnel and business processes that ensure that security is carried out to meet an organization's specific needs. It requires organizational structure, roles and responsibilities, performance measurement, defined tasks and oversight mechanisms. IT Governance Institute (2006) concluded that “information security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly". Rastogi and Von Solms (2006) define that "information security governance consists of the frameworks for decision-making and performance measurement that Board of Directors and Executive Management implement to fulfill their responsibilities of providing oversight, as part of their overall responsibilities for protecting stakeholder value". This definition of information security governance term will be used as reference in this paper because more comprehensive and suitable for this research work.

The main purpose of information security governance implementation is to protect the most valuable asset of an organization. The identification of the information assets of the company is a critical success factor for the efficient and effective implementation of information security in companies (IT Governance Institute, 2001; Deloitte Touche Tohmatsu, 2003). Kurt and Tentra (2004) categorize the information assets to be protected in the banking industry into four items which are:

- Insider information: Information which gives its possessors an unlawful market advantage and is suitable for the carrying out of insider operations (for example: board of directors' meeting minutes, capital market information, and internal company financial data).

- Client information: information which makes the inference of the identity of the client possible (for example: name, address, date of birth) including the designation of his bank contact information (account number, deposit number).

- Numbered account client information: Client information of an economic beneficiary or assignee of numbered or imaginary accounts. Balance information: Information which represents the commercial claims between the bank and its clients or business partners (for example: account balances, deposit balances, nostro balances).

- Transaction information: Information which cause or represent a change in the commercial claims between the bank, clients or business partners (for example: account and deposit movements, business events in trade).

The primary threats to banking system caused by lack of information security governance practice can be classified as: 1) Physical destruction of premises, infrastructure and data by natural elements. A lack of preparation for an emergency can indeed mean the definitive end for a bank in the event of the possible occurrence of the event (Kurt and Tentra, 2004). 2) The unintentional destruction or damage of systems and data due to human failure caused by many factors, such as the suitability of tools, employee training, workload, work ethic and company culture (Kurt and Tentra, 2004; Siregar, 2008). 3) Abuse of confidence by employees or agents of the bank in the handling of sensitive information, such as through the misappropriation of client information or business secrets or through the fraudulent acquisition of insider-relevant information about the bank and clients (Kurt and Tentra, 2004; MSNBC, 2010). 4) Enrichment of employees or agents of the bank at the expense of the bank or clients through the fraudulent manipulation or falsification of balance, transaction or exchange rate information, caused by lack of the employment policy, business processes, the system clearances, social controls, the company culture and ethics. (Kurt and Tentra, 2004; Siregar, 2008; MSNBC, 2010). 5) External attack to the information system of the bank such as hacker and virus lead to information losses, false information, a loss of the confidentiality of information, and breakdowns of business processes (Kurt and Tentra, 2004; Vijayan, 2010). 6) The systematic collection of information by foreign intelligence services through the analysis of data and telecommunications activities and stolen equipment. This kind of threat activities resulted in released confidentiality of client information (Kurt and Tentra, 2004; Business Management, 2010). 7) Social Engineering approach thought the internet to pursue victim to give their identity information or directly calls the bank's help desk impersonating an authorized user to gain information about the system including changing passwords (Business Management, 2010).

Having classified the information assets and potential threats in banking, the next section discusses the commonly used information security governance frameworks, standard, best practice and guideline.

Information Security Governance Framework

In reference, Rastogi and von Solms (2006) describe that information security governance consists of structures, relationships and processes; the existing guidance that provides frameworks for implementing information security governance. The implementation proceeds mainly by mapping Information Security Governance responsibilities to the organizational hierarchy. Holmquist (2008) suggests that there are several choices of information security governance frameworks applicable to banking industry such as FFIEC, COBIT, ISO 27002, and PCI data security standard. Based on this suggestion, we further look into the mentioned information security governance framework and others are widely used. There are various information security governance frameworks which have been widely used which are:

FFIEC

The Federal Financial Institutions Examination Council (FFIEC) was established in 1979. It was given the authority to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. The FFIEC publication: "Information Security IT Examination Handbook" is used by federal examiners auditing the operations of financial institutions for compliance with their obligations. FFIEC's October 2005 "Authentication in an Internet Banking Environment" guidance will be part of that handbook (RSA, 2010).

COBIT

Control Objectives for Information and related Technology (COBIT) is developed by The Information Systems Audit and Control Association & Foundation (ISACAF) to provide management and business process owners with an IT governance model to help understand and manage the risks associated with IT. COBIT consists of four main components namely, plan and organize, acquire and implement, deliver and support, and finally monitor and evaluate (IT Governance Institute, 2007).

ISO 27002

The International Organization for Standarization (ISO) is ''the world's largest developer and publisher of international standards in a wide area of subjects including information security management systems and practices. The ISO 27002 (2006) standard, formally The ISO 17799 (2005) standard, is an industry benchmark code of practice for information security practice" (ISO, 2009). IT outlines 11 control mechanisms and 130 security controls. The standard establishes guidelines and general principles for ''initiating, implementing, maintaining, and improving information security management within an organization" (ISO, 2006).

PCI

PCI Data Security Standard (PCI DSS), a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures (PCI, 2010).

CGTF

The Corporate Governance Task Force (CGTF) developed an objective, standards-based, scale able, and collaborative framework to aid organizations in the creation of an ISG structure. The framework can be adapted to a wide variety of entities, including corporations of all sizes in different industry sectors, as well as education and non-profit institutions. To facilitate the use of the framework, the task force has developed other additional tools which are The ISG functions and responsibilities guide and the information security governance assessment tool (Corporate Governance Task Force, 2004).

IISA

Information Systems Security Association (ISSA) published The Generally Accepted Information Security Principles (GAISP). The primary goal of the ISSA is to promote practices, from the boardroom to the information security professional that will ensure the confidentiality, integrity, and availability of organizational information assets. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.

CISWG

The Corporate Information Security Working Group (CISWG) has produced guidance on the development of information security metrics and created a definitive summary of information security management references. CISWG is a program formed by Adam H. Putnam, chairman of the Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census of the Government Reform Committee, of the U.S. House of Representatives (Swanson, (2008).

Various researchers have defined the components of information security and how an organization should do about implementing them (International Standards Organization, 2005; Tudor, 2000; McCarthy and Campbell, 2001). Information security components can be described as the principles that enable the implementation and maintenance of information security such as an information security policy, risk assessments, technical controls, and information security awareness. These components could be considered in an information security governance framework to provide organizations with an understanding of the requirements for a holistic plan for information security. It also combines technical, procedural, and people-orientated components for the purpose of cultivating an appropriate level of information security culture and minimizing risks posed to information assets.

Table 1 provides the components and compares the commonly used approaches to information security governance frameworks in order to define and construct a new information security governance framework for banking. These components were selected from each approach where a component was depicted as a key principle, or as an information security control. Where components overlapped between approaches such as "policies," a combined component category was defined. Table 1 shows that corporate governance, ethical conduct, trust, and auditor security program are not included in many other frameworks, although all four components are considered as important components by various researchers (International Standards Organization, 2005; Flowerday and Von Solms, 2006; Allen and Westby, 2007) when governing information security in an organization. It is notable that not one of the framework cover all information security governance components, some of the framework such as PCI Security standard is very specific to operational level. Some other frameworks, such as ISO 27002 or the COBIT, also detailed technical practice security standards, which have the character of basic configuration and operation of IT systems and only indirectly affect information security (Kurt and Tentra, 2004). Kurt and Tentra (2004) also state that "although it is often speak of "best practice" in connection with data security, in practice there is no standard that completely regulates all of the aspects of information security and can fulfill the needs of individual companies to the same degree. The reasons why there cannot be universally correct information security, because of the significant differences between various economic operators, even within the same industry. Different companies have different sizes, financial strengths, cultures, values, core competencies, visions, business strategies, business models, target customer segments, and also different risk policies. Thus, companies have disparate conceptions about the importance and value of information security for the achievement of particular business objectives and a correspondingly different willingness to pay for it.

Table 1: Information Security Governance Approach Comparison

ISG components	ISO 27002	IISA	COBIT	CGTF	CISWG	FFIEC	PCI
Information security strategy	x	x	✓	✓	x	x	x
Leadership and sponsorships	✓	✓	✓	✓	✓	✓	x
Security return on investment	x	✓	✓	✓	✓	x	✓
Security metric and measurement	x	✓	✓	✓	✓	x	✓
Corporate governance	x	x	x	x	✓	✓	x
Internal and External Auditor Information Security Program	x	x	x	x	✓	x	x
Security program organization	✓	✓	✓	✓	✓	✓	x
Security policies, procedure, best practice, standards, and guidelines	✓	✓	✓	✓	✓	✓	✓
Compliance	✓	✓	✓	✓	✓	✓	x
Monitoring and auditing	✓	✓	✓	✓	✓	✓	x
Legal and regulatory	✓	✓	✓	✓	✓	✓	x
User awareness, education and training	✓	✓	✓	✓	x	x	✓
Ethical values and conduct	x	✓	x	x	x	x	x
Privacy	x	x	x	x	x	x	x
Trust	x	x	x	x	x	x	x
Certification against a standard	✓	✓	✓	x	x	x	x
Risk management and assessment process	✓	✓	✓	✓	✓	✓	✓
Best practice and baseline consideration	✓	✓	✓	✓	✓	x	x
Asset management	✓	✓	✓	x	✓	x	✓
Physical and environmental controls	✓	✓	✓	x	✓	x	✓
Technical operations	✓	✓	✓	✓	x	x	✓
System acquisition, development, and maintenance	✓	✓	✓	x	✓	x	✓
Incident management	✓	x	x	✓	x	x	x
Business continuity planning	✓	x	✓	✓	✓	x	x
Disaster recovery planning	x	x	✓	✓	x	x	x
User management	✓		✓		✓	✓	✓

Legend: x = Not included ✓ = Included

It is found that the design of business-oriented information security can only emanate from an information strategy that is in agreement with the business strategy. Corporate information security governance should have its own place within the framework of corporate governance, beside IT governance and risk management (Kurt and Tentra, 2004). Hoekstra & Conradie (2002) and Spafford (2003) too agreed that there are some frameworks that have been developed and widely practiced in corporate governance, but each of them has its own strengths and weaknesses. Therefore, customization is pertinent to appropriately fit with the organization's environment.

The Initial Design of the Proposed ISG Framework for Banking System

The initial design of the proposed ISG framework can be used as a starting point by banking sector to govern information security by developing guidelines and implementing controls to protect banking information assets from the threats identified in literature reviews. This framework is an integration of all available framework components discussed and derived from literature review. Nevertheless, the suggested framework is still a general approach to information security governance program, it needs to be reviewed by professionals and tested in the real banking environment. As each organization's environment is different and subject to different national and international legislation and regulations, additional components might be required, while others may not be relevant. Based on the definition of information security governance given by Rastogi and Von Solm (2006), the initial design of information security governance framework constructs by mapping information security components into corporate hierarchy which are strategic level, tactical and operational level and operational level (CGTF, 2004; Rastogi and Von Solm, 2006). Each level of information security components and the composition thereof are discussed below.

Strategic Level

Strategic level refers to board of directors and senior executive management (CGTF, 2004). Most of the framework, standard and practices reviewed in the literature propose at this level, the leadership and governance component involves the compilation of an information security strategy to address a successful information security program. The information security strategy should be linked to the organizational and IT strategy to ensure that the organization's objectives are met both in the short and in the long term. This level requires executive sponsorship for information security program as well as commitment from the board and management to protect information assets. This is due to the fact that information security governance is accepted as an integral part of Corporate Governance (Von Solms, 2005). Corporate governance relates to the responsibility of the board to effectively direct and control an organization through sound leadership efforts (Donaldson, 2005). This is associated with IT governance, which is concerned about the policies and procedures that define how an organization will direct and control the use of its technology and protect its information. At this level also, the framework includes the concepts of metrics and measurement to identify the effectiveness of current information security governance program. Many organizations are turning to metrics to evaluate the overall effectiveness of their information security programs and whether it contributes in achieving the organization's strategy (Witty and Hallawell, 2003).

Tactical and Operational Level

Tactical and operational level refers to senior managers and operation managers (CGTF, 2004). Most of the reviewed frameworks suggest that, this level addresses user awareness; education and training as key component. But not many researchers suggest ethical conduct, trust and privacy to be included in this level. The researcher includes ethical conduct; trust and privacy as key component at this level because OECD states that one of the principles in creating a security culture is ethical conduct where both management and the board develop and communicate corporate codes of conduct (OECD, 2004). As part of the information security governance framework, ethical conduct must be addressed by the organization to minimize the risk of, for instance, invasion of privacy, selling of customer information and unauthorized altering of data. These ethical conducts preserve to employees as part of the security awareness program.

The other key component proposed in this level is "trust". When implementing the information security governance framework components, management must be able to trust employees to adhere to information security policies, while employees must be able to trust management in keeping the commitment for implementing information security program. A trusting relationship should also be established between trading partners and clients who could contribute to the organization's reputation. And privacy as key component in this level also an essential issue of trust when it comes to good relationships with customers, suppliers and other business partners (Tipton and Krause, 2004). Program organization and legal and regulatory considerations are key components in this level. Program organization refers to the information security organizational design, composition and reporting structures. It also defines the roles and responsibilities, skills and experiences, and resource levels committed to the enterprise security architecture. Legal and regulatory consideration proposed as key component because different countries have different laws and regulation, therefore, it should be considered for information security governance program.

Most of reviewed frameworks suggest security policies, procedures, standards, and guidelines as the key components to implement information security in order to provide management and employees with direction and support and they should clearly state what is expected of employees and guidelines for their behavior. The security policies should be implemented in the organization through effective processes and compliance monitoring. Examples of information security policies are an access control policy, e-mail, and Internet policy and a physical and environmental policy. A procedure is an interpretation of the security policy and is the steps that need to be taken to accomplish the policy (Von Solm and Von Solm, 2006). Procedures are underpinned by standards such as a password standard and guidelines such as the procedures to configure a firewall to meet the requirements of the security policy.

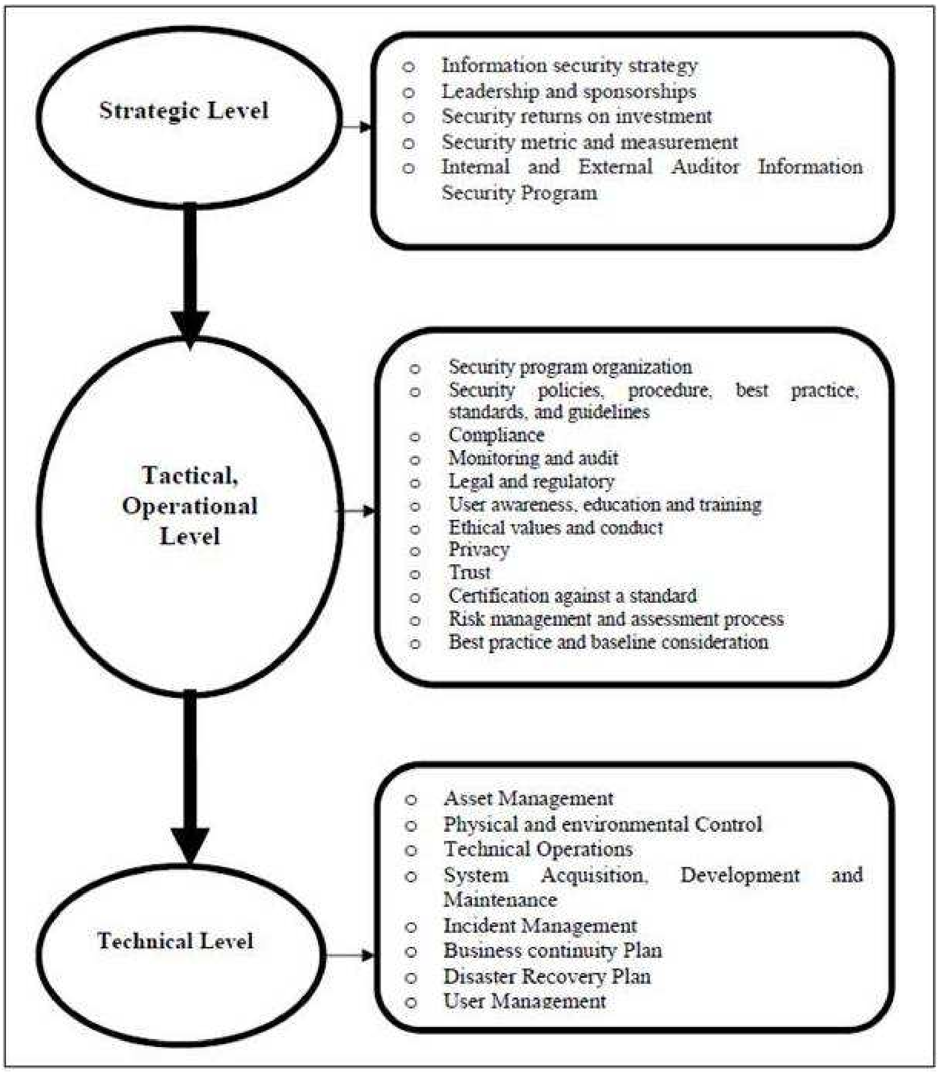
Strategic Level
Information security strategy
Leadership and sponsorships
Security returns on investment
Security metric and measurement
Internal and External Auditor Information Security Program
Tactical, Operational Level
Security program organization
Security policies, procedure, best practice, standards, and guidelines
Compliance
Monitoring and audit
Legal and regulatory
User awareness, education and training
Ethical values and conduct
Privacy
Trust
Certification against a standard
Risk management and assessment process
Best practice and baseline consideration
Technical Level
Asset Management
Physical and environmental Control
Technical Operations
System Acquisition, Development and Maintenance
Incident Management
Business continuity Plan
Disaster Recovery Plan
User Management

Figure 1: The Initial Design of the Proposed ISG Framework

At this level of the framework, monitoring, compliance, and auditing are also proposed as key components to manage the information security program. It is essential to measure and enforce compliance (Von Solms, 2005), and both technology and employee behavior should be monitored to ensure compliance with information security policies and to respond effectively and timely to incidents detected (Vroom and Von Solms, 2004). Monitoring of employee behavior could include monitoring the installation of unauthorized software, the use of strong passwords or Internet sites visited. Technology monitoring could relate to capacity and network traffic monitoring. Information security auditing is necessary to ensure that the policies, processes, procedures and controls are in line with the objectives, goals and vision of the organization.

Technical Level

Technical level refers to all employees (CGTF, 2004). Some of reviews framework proposed the technology protection and operations as the key components of information security governance program. It involves the technical and physical mechanisms implemented to secure an IT environment Von Solm (2000). When implementing the security governance framework, the technology controls applicable to the organization's environment and identified risks must be implemented. These include asset management, system development requirements, incident management, technical operations such as network security, and physical, environment, business continuity controls and user management. It is essential that the technology environment be monitored on a constant basis and that the risks of technology changes in the market be addressed e. g., the use of personal digital assistants and teleworking technology.

Conclusion

In today's technological and social environment, security is a very important part of a banking and financial institution system. Business partners, suppliers, and vendors require high information security from one to another, particularly when providing mutual network and information access. Espionage through the use of networks to gain competitive intelligence and to extort organizations is becoming more prevalent. Banks ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network connectivity and services. Having a reputation for safeguarding information and the environment within which it resides enhances an organization's ability to preserve and increase market share. A comprehensive information security governance framework is highly needed for banking information system. Some general standards and best practices have been developed such as FFIEC, COBIT, ISO 27002 and PCI data security standard, but none of them can fulfill specific and unique needs of an organization. This in-progress research is to develop a specific information security governance framework with banking environment and IT information system in mind. To this end, the framework can be used as a initial effort for bank to govern their information security. This framework is an integration of all framework components available today. Essentially, this framework is still a general approach to information security governance program, it needs to be reviewed by professionals and comprehensively tested in the real banking environment. This study will proceed with a web-based survey to further examine the IT professional perception on information security governance framework in a newly developed country.

References

Akhmad Syakhroza (2003). Best Practice Corporate Governance Dalam Kontek Perbankan Indonesia. Jakarta: Usahawan No. 06 Thn XXXII. 19.

Allen, J. H. & Westby, J. R. (2007). Governing for Enterprise Security (GES), Implementation Guide: Characteristics of Effective Security Governance1. USA: Carnegie Mellon University. 5-7

Biri, K .& Tentra, G.M. (2004). "Corporate Information Security Governance in Swiss Private Banking," Master's Thesis University of Zurich

Business Management (2010). Staying off The Hook. Business management Magazine Issue 4, Security & Data. Retrieved July 2010, from http://www.busmanagementme.com/article/ Middle East Bank - Security Breaches - Phishing Frauds - IT Security/

Corporate Governance Task Force (2004).'Corporate Governance Task Force Report: Information Security Governance A Call To Action,' National Cyber Security Summit April 2004, USA

Council III, C. (2006). 'An Investigation of a COBIT System Security IT Governance Initiative in Higher Education,' PhD Thesis. Nova Southeastern University

Donaldson, W. H. (2005). 'U.S. Capital Markets in The Post-Sarbanes Oxley World: Why our markets should matter to foreign issuers,' U.S: Securities and Exchange Commission. London School of Economics.

Ernst & Young (2003). Global Information Security Survey 2003. US: E&Y

Flowerday, S. & Solms, R. V. (2006). Trust an Element of Information Security *Security* *and Privacy in Dynamic Environments.* IFIP/SEC2005; Boston: Kluwer Academic Publishers, 87–97.

Harris, S. (2006). Information Security Governance Guide [online], [Retrieved 03-04-2008]. www.SearchSecurity.com

Hoekstra, A. & Conradie, N., (2002). CobiT, ITIL and ISO17799, How to Use Them in Conjunction. USA: *Price Water House Copper.*

Holmquist, E. (2008). "Which Security Governance Framework is The Best Fit?," TechTarget ANZ, Australia [Online]. [Retrieved: August 2008], http://searchcio. techtarget.com. au/articles/24787-Which- security-governance-framework-is the-best-fit-.htm,

ISO 27002-2006(2006). International Standard - Information Technology - Security Techniques - Code of Practice for Information Security Management [Online]. [Retrieved May 15, 2009], http://www.iso.org/iso/iso_catalogue/catalogue_tc/

IT Governance Institute (2001). Information Security Governance: Guidance for Board of Directors and Executive Management. IT Governance Institute, Rolling Meadows, 11

IT Governance Institute (2006), Information Security Governance: Guiding for Board of Director and Executive Management 2nd Edition [online], [Retrieved May 15, 2009], www.itgi.org

IT Governance Institute (2007). CobiT 4.1 Excerpt [Online]. [Retrieved March 20, 2009], http://www.itgi.org/Template_ITGI.cfm?Section=Recent_publications&Template=/Content Management/ ContentDisplay.cfm&ContentID=45948

Ma, Q. (2004). 'A Study on Information Security Objectives and Practices,' PHD Dissertation, Southern Illinois University. 17

Mahncke, R. J., McDermid D. C.& Williams P. A. (2009). "Measuring Information Security Governance within General Medical Practice," Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia.

McCarthy, M.P. & Campbell, S. (2001). Security Transformation. New York: McGraw-Hill.

Moulton, R & Coles, R. S. (2003). "Applying Information Security Governance," *Elsevier*

MSNBC (2010). Massive Bank Security Breach Uncovered in New Jersey [online]. [Retrieved July 2010], from http://www.msnbc.msn.com/id/3303539

OECD. (2004). OECD Principles of Corporate Governance Organisation for Economic Co-Operation and Development. OECD

PCI. (2010). About the PCI Data Security Standard (PCI DSS) [online], [Retrieved July 2010], https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
Publisher

Power, R. (2002). CSI/FBI Computer Crime and Security Survey (2002), Computer Security Issues & Trends, vol. VIII, No.1.

Rastogi, R & Von Solms, R. (2006). Information Security Governance a Re-definition. IFIP International Federation for Information Processing, Volume 193/2006, Springer Boston.

Rogers, M. (2001). A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: an Exploration Study. Unpublished dissertation.[online], [Retrieved August 2007], http://www.mts.net/mkr/cybercrime-thesis.pdf

RSA (2010). Information Security Glossary: The Federal Financial Institutions Examination Council (FFIEC)[online].[

Retrieved July 2010], www.rsa.com/glossary/default.asp?id=1020

Schmid, G. (2001). 'Report on the Existence of a Global System for The Interception of Private and Commercial Communication,' (ECHELON interception system) (2001/2098(INI)). European Parliament Session document, pp 5-118

Siregar, I., (2008). Tanda Lemahnya Manajemen Keamanan [online]. [Retrieved 28-8-2008], http://irwanesiregar.blogspot.com/2007/10/tanda-lemahnya-manajemen-keamanan.html,

Spafford, G. (2003). "The Benefits of Standard IT Governance Frameworks," [online]. [Retrieved November 2007]

Swanson, D. (2008). Who is Responsible for Information Security? [online][Retrieved July 2010],

Symantec (2010). Symantec Internet Security Threat Report. Trends for 2009, Volume XV, (report) Capertino, CA : Symantec

Tipton H. F. & Krause, M. (ED.) (2004). A Matter of Trust: Information Security Management Handbook fifth Edition. London: AUERBACH PUBLICATIONS

Tohmatsu, D. T. (2003). 2003 Global Security Survey. USA: Deloitte Touche Tohmatsu. 19

Tubin, G. (2005). The Sky IS Falling: The Need for Stronger Consumer Online Banking Authentication. USA: TowerGroups.

Tudor, J. K. (2000). Information Security Architecture: An Integrated Approach to Security in the Organization, Boca Raton, FL: Auerbach.

Vijayan, J. (2010)."Five Indicted in Cybertheft of City's Bank Account," [online].[Retrieved July 2010], http://www.computerworld.com/s/article/9177409/Five_indicted_in_cybertheft_of_city_s_ bank_accounts

Von Solms, B. (2000). "Information Security - The Third Wave?," *Computers and Security*, 19(7). November, 615-620.

Von Solms, R. & Von Solms S. H. (2006). "Information Security Governance: A Model Based on the Direct Control Cycle," Elsevier Ltd: *Computers & Security*, Volume 25, September 2006, Pp 408-412

Von Solms, S. H. (2005). "Information Security Governance: Compliance Management vs. Operational Management," *Computers and Security*, 24 (6), 443–447.

Vroom, C. & Von Solms, R. (2004)."Towards Information Security Behavioural Compliance," *Computers and Security*, 23 (33), 191–198.

Witty, R. J. & Hallawell, A. (2003). "Client Issues for Security Policies and Architecture," Gartner. ID number: K-20-7780.

Zviran, M. & Haga, W. J. (1999)."Password Security: an Empirical Study," *Journal of Management Information Systems*, 5(4) 161-185.

Zwass, V. (1997). Foundations of Information Systems. Boston:Irwin/McGraw-Hill,: The Encyclopedia of Computer Security