https://doi.org/10.48009/2_iis_2009_650-659

AN INFORMATION SECURITY MANAGEMENT SYSTEM MODEL FOR SMALL AND MEDIUM-SIZED FINANCIAL INSTITUTIONS

Kevin Streff, Dakota State University, Kevin.Streff@dsu.edu

==

ABSTRACT

Information security breaches continue to rise at disturbing rates. Financial institutions are required to have a documented information security program commensurate with their size, complexity and use of technology. However, small and medium-sized financial institutions struggle to complete this task as no information security management system model exists that meets their unique needs. This paper outlines the existing information security management program models in the marketplace, develops an innovative information security program model honed to the specific needs of small and medium-sized financial institutions, and discusses the feedback from rolling out this model in several pilot small and medium-sized financial institutions.

INTRODUCTION

With 85 percent of the critical infrastructure owned by the private sector and not the federal government (Dan, 2003), security experts are concerned that the financial markets could plummet if a cybersecurity attack occurred against the banking and financial infrastructure ("Financial Services Industry Launches New Critical Infrastructure Protection Initiatives," 2003). The President's Information Technology Advisory Committee recently suggested that the financial sector is very vulnerable to attack from terrorists and criminals. To this point, In 1998 President Clinton declared the banking and financial infrastructure critical infrastructure (Clinton, 1998).

Financial institutions desire good security for a couple of reasons. First, customers trust banks to safeguard their financial assets and when banks can not protect consumers' sensitive information, it erodes their confidence in the banks' ability to protect their financial assets (Colin, 2000). Second, there are financial ramifications of poor security (Karen, 2006). For example, following the TJX data breach in which 4.6 million data records were reported compromised (Robin, 2007), TJX's profit fell 57% ("TJX Profit Falls 57% on Costs Tied to Data Breach," 2007). Further, the banks are shouldering much of the cost of these data breaches that occur up and down the supply chain. For example, the TJX data breach impacted many banks financially as the credit card company and merchant seem to be able to pass the buck to the financial institution (Brian, 2007). Most recently, Heartland reported a data breach affecting 10 million data records (McGlasson, 2009). This data breach affects many small and medium sized financial institutions who leverage the Heartland core banking platform (Worthen, 2009).
Further, information security breaches continue to rise at alarming rates (*Symantec Internet Security Threat Report*, January-June, 2007). Scarcely a day goes by when a data breach is not reported ("PrivacyRights," 2007). Financial institutions are often the target of information security attacks because of their large cash flows, large transaction volumes, and extensive use of electronic media, financial institutions are a prime target for this type of "white-collar" crime (Price, Cotner, & Dickson, 1989).

A recent survey on data breaches by America's Community Bankers found that the vast majority of our member banks have been affected, with 72 percent of the respondents having to reissue cards three times or more in the past two years. It costs us $10 to $15 to replace just one card (Michael, 2007). With the Heartland and TJX breach affecting as many as 40 million cards, well over 300,000 cards have had to be replaced so far (Michael, 2007). In fact, financial institutions are beginning to fight back and attempt to push these costs back on the retailer (Jaikumar, 2007; Jenn, 2007; Jonathan, 2007). Further, GLB requires small-entity financial institutions develop an information security program to mitigate information security threats; therefore, small-entity financial institution desire good security controls to be in compliance with the law. This paper outlines a model small-entity financial institutions can use to guide the design and implementation of an information security management program to promote good security and be in legal compliance.

LITERATURE REVIEW

The Gramm-Leach-Bliley Act of 1999 applies to the following types of financial institutions: National banks, Federal branches and Federal agencies of foreign banks and any subsidiaries of these entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OCC); member banks (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, Edge and Agreement Act Corporations, bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (Board); state non-member banks, insured state branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (FDIC); and insured savings associations and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OTS) (*Interagency Guidelines Establishing Information Security Standards: Small Entity Compliance Guide*, 2005). The information security responsibilities for financial institutions are highlighted in Table 1.

Table 1: Information Security Responsibilities

Availability	Processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.
Integrity	Processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
Confidentiality	Processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use.
Accountability	Processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.
Assurance	Processes, policies, and controls used to develop confidence that technical and operational security measures work as intended. assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions.

Source: (*Information Security IT Examination Handbook*, 2006; Steven, 2003).

These objectives are accomplished through designing and implementing an integrated, documented information security program that accounts for the use of technology and complexity of operations. For example, Streff, Rajagopalan and Fu (2007) outlined the key components of the international banking system is the payment system and recommended transaction camouflaging for funds-transfer activities (Streff, Rajagopalan, & Fu, 2007). However, community bankers generally struggle to understand how to develop an information security program, partially because no model exits to facilitate the program's development. Streff (2008) outlines that bank regulators are in fact looking for management at the bank to have a management program to manage information security risk of customer information (Streff, 2008). However, understanding what framework to use is typically problematic for small and medium-sized financial institutions.

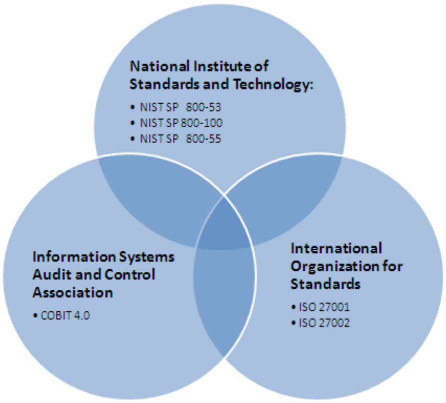
Because of this fact, financial institutions are required to have a documented information security program commensurate with their size, complexity and use of technology (*Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 2001). The Security Guidelines primarily implement two statutes, Section 216 of the Fair and Accurate Credit Transactions Act of 2003 ("Fair and Accurate Credit Transactions Act of 2003," 2003) and Section 501(b) of the Gramm-Leach-Bliley Act ("Gramm-Leach-Bliley Act," 1999a). The Fair and Accurate Credit Transactions Act of 2003 was passed to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes ("Fair and Accurate Credit Transactions Act of 2003," 2003). The Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) requires financial institutions to safeguard customer information ("Gramm-Leach-Bliley Act," 1999a). The Gramm-Leach-Bliley Act of 1999 (GLB) is federal law that addresses consumer concerns related to online banking, electronic commerce, and electronic records storage. Private information, including bank balances, social security numbers, and account information, is routinely bought and sold by banks, credit card companies, and other financial institutions. The Gramm-Leach-Bliley Act provided privacy protections against the sale of this private financial information, legislating that banks, credit card companies, and other financial institutions protect customer privacy. The GLB's privacy protections only applied to financial institutions, businesses engaged in banking, stocks and bonds, insuring, financial advice, and investing ("Gramm-Leach-Bliley Act," 1999a; "Gramm-Leach-Bliley Act," 1999b; O'Neal, 2000). Practitioners and researchers are mixed in their opinions of GLB. Some have suggested that GLB has had positive impacts on the banking industry (Alexander, Jones, & Nigro, 2001), while others have called GLB necessary but insufficient (Cuaresma, 2002).

The Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) set forth standards pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (*Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 2001). The Guidelines apply to customer information maintained by or on behalf of state member banks and bank holding companies and their nonbank subsidiaries, except for brokers, dealers, persons providing insurance, investment companies, and investment advisors. These Guidelines also apply to customer information maintained by or on behalf of Edge corporations, agreement corporations, and uninsured state-licensed branches or agencies of foreign banks (*Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 2001). The Guidelines require each financial institution to implement a management-approved, documented Information Security Program (ISP) that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. The program must be designed to ensure the security of customer information, protect against unanticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. Each institution must assess risks to customer information and implement appropriate policies, procedures, training, and testing to manage and control these risks. Institutions must also report annually to the board of directors or a committee of the board of directors.

This Small-Entity Compliance Guide is intended to help financial institutions comply with the *Interagency Guidelines Establishing Information Security Standards* (Security Guidelines). The guide summarizes the obligations of financial institutions to protect customer information and illustrates how certain provisions of the Security Guidelines apply to specific situations. The appendix lists resources that may be helpful in assessing risks and designing and implementing information security programs (*Interagency Guidelines Establishing Information Security Standards: Small Entity Compliance Guide*, 2005).

The Information Security IT Examination Handbook published by the Federal Financial Institutions Examination Council outlines three models for developing an information security program for a financial institution: NIST, ISO, and CobiT. Each standard has some unique features and some common features as depicted in Figure 1:

Figure 1: Relationship of Information Security Standards


National Institute of Standards and Technology:
• NIST SP 800-53
• NIST SP 800-100
• NIST SP 800-55
Information Systems Audit and Control Association
• COBIT 4.0
International Organization for Standards
• ISO 27001
• ISO 27002

Each information security standard mentioned in the Information Security IT Examination Handbook is further discussed next.

National Institute of Standards and Technology (NIST) Information Security Model

Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies the minimum security requirements for federal information and information systems in seventeen security-related areas (Gutierrez & Jeffrey, 2006). NIST has established over 100 publications to help organizations with information security ("NIST Website," 2007). It began in 1995 when NIST published a documented entitled “An Introduction to Computer Security: The NIST Handbook” (Courtney et al., 1995).

Four other notable NIST documents include:

- NIST Special Publication 800-100 – Information Security Handbook: A Guide for Managers (Bowen, Hash, & Wilson, 2006).
- NIST Special Publication 800-53 – Recommended Security Controls for Federal Information Systems (Ross et al., 2005).
- NIST Special Publication 800-18 – Guide for Developing Security Plans for Federal Information Systems (Swanson, Hash, & Bowen, 2006).
- NIST Special Publication 800-155 – Performance Measurement Guide for Information Security (Chew et al., 2007).

These documents are designed to be used in combination to secure an enterprise. However, these NIST documents are too complex for small and medium-sized financial institutions that often do not have a technology individual on staff (and rarely or never has an information security professional on staff). For example, NIST Special Publication 800-100 is 178 pages. This suite of documents is simply too long and complex for the needs of small-entity financial organizations. These documents are intended for large federal government agencies which have sufficient resources to read, understand and operationalize. Further, the requirements to secure a federal government agency far exceed the requirements of a typical small-entity financial organization. The same is true for resources; meaning, that the financial and human resources of a federal government agency far exceed the financial and human resources of a typical small-entity financial organization.

International Standards Organization (ISO) Information Security Model

The International Standards Organization (ISO) 27001 information security standard is a management standard originally documented by the British Standards Institute and ultimately refined and adopted by ISO (*27001 Information Security Standard*, 2005). ISO 27001 is an information security standard designed to give organizations a means for providing clients, partners and regulators with proof that they adhere to an internationally recognized set of information security controls (Brenner, 2007). However, companies in the United States have been slow to adopt this internationally recognized standard (Greenemeier, 2006). The standard is difficult to understand and adhere to (Bruno-Britz, 2006), so much so that ISO 27001 Certification Guides are available ("World's First ISO 27001 Certification Guides Launched," 2005). Further, awareness of the standard is lacking (Violino, 2006) and small-entity financial institutions have not adopted the standard. In fact, as of the writing of this journal article, not a single small-entity financial institution is registered to the standard. While the standard includes a “Statement of Applicability”, the reality is that the standard is not directly relevant to a small-entity financial institution. For example, most small-entity financial institutions don’t write software, making vendor selection and vendor management an important component of their information security program; however, the ISO standard emphasizes software development and maintenance. Table II outlines the domains in the ISO 27001 information security standard.

Table II: ISO 27001 Information Security Domains

1. Security Policy
2. Organization of Information Security
3. Asset Management
4. Human Resources Security
5. Physical & Environmental Security
6. Communications & Operations Management
7. Access Control
8. Information Systems Acquisition, Development & Maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

The most important problem with the ISO standard is that federal regulators have not recognized its importance. When querying federal bank regulators about the standard, most are unaware of its existence. Therefore, basing your information security program on this standard is problematic.

CobiT Information Security Model

Control Objectives for Information and related Technology (CobiT) provides good practices across a domain and process framework and presents activities in a manageable and logical structure ("COBIT 4.1," 2007). CobiT is based on the broader quality, fiduciary and security requirements, seven distinct, certainly overlapping, information criteria are defined in Table III.

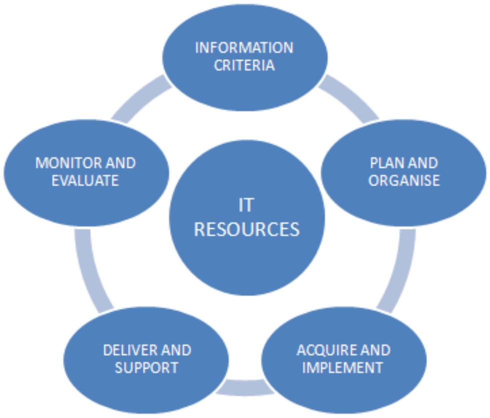
Table III: CobiT Information Criteria

Criteria	**Description**
Effectiveness	Information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner
Efficiency	Information through the optimal use of resources
Confidentiality	The protection of sensitive information from unauthorized disclosure
Integrity	relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations
Availability	Information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities
Compliance	Complying with the laws, regulations and contractual arrangements
Reliability	Appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities

These information criteria go beyond the fundamental requirements of confidentiality, integrity and availability as defined by the federal bank regulators. Therefore, these criteria are confusing to bankers who are desperately trying to gain compliance with federal requirements. For example, community bankers do not talk about information reliability; rather, small and medium sized financial institutions typically deal with confidentiality, integrity and availability. Without a dedicated, educated information security officer, these institutions have their hands full with the basic CIA triad.

Further, CobiT is a codes-based model that requires a very deep understanding to implement. Figure II outlines the four major areas of CobiT and introduces several of the codes used in the standard:

Figure II: CobiT Information Security Process



The reality is that CobiT is far too complex for small-entity financial institutions. Von Solms (2005) confirms that CobiT is large and complex (B. von Solms, 2005). For organizations with dedicated IT auditors, the standard may hold value; however, for small-entity financial institutions without such a resource, a simpler, easier-to-understand standard that is honed to the unique needs of the small-entity financial organization is required.

As mentioned previously, the NIST, CobiT and ISO models are not tailored to small financial entities; therefore, this is not a practical blueprint from which small-entity financial institutions can develop an information security program. The next section outlines such a model that small-entity financial institutions can use for information security program compliance.

SMALL-ENTITY INFORMATION SECURITY PROGRAM COMPLIANCE MODEL (SMEISP)

The small-entity information security framework developed included the following considerations as identified through previous research:

Peltier (2005) emphasized the inclusion of I.T. Risk Assessment in the design of an information security program. Peltier suggested that the ISP components be determined based upon the results of a thorough risk assessment (Peltier, 2005).

Thomson and von Solms (1998) recognized the importance of security awareness and education as a layer in the defense-in-depth model. Thomson emphasized that security awareness and education be included in any information security program to compliment both the policy and technology components (Thomson & von Solms, 1998).

Von Solms (2005) investigated utilizing two information security standards (CobiT and ISO 17799) and provided a level of 'synchronization' between these two frameworks (B. von Solms, 2005). This is desired because these standards don't seem to really hit the mark alone and reflects industries desire to develop a better, more complete information security standard.

Cooper et al (2007) highlighted the disconnected nature of security activities in organizations and challenges leaders to move out of the reactive mode of information protection into a proactive mode where the culture promote coordinated information protection (Cooper, Lipinski, Cook, & Orndorff, 2007).

Tipton (2004) outlined organizations should adopt a information security management system that enables organizations to clarify their vision and strategy and translate them into action (Tipton & Krause, 2004).

Su, Bolzoni and van Eck (2006) emphasized tying an organization's information security program to the business and technology strategy. The researchers emphasized outlining business requirements so that maximum return on investment is achieved for each information security decision (Su, Bolzoni, & van Eck, 2006).

Rycroft and Tully (2007) explained in a recently published journal paper an approach for rationalizing commonly used information security standards and collating them into a single, accessible, 'Meta Standard' (Rycroft & Tully, 2007).

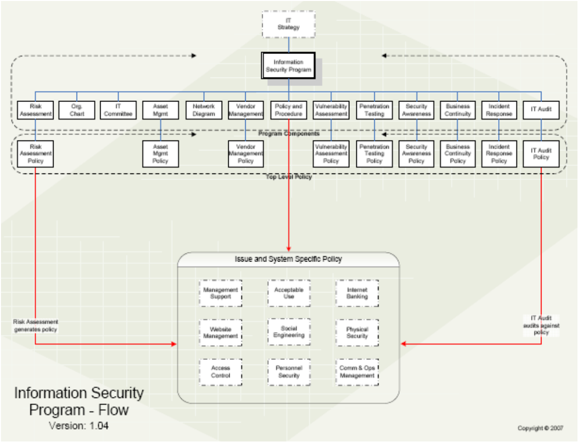
It is generally accepted that Information Security Governance is an integral part of Corporate Governance. It is therefore essential for any company to have a proper Information Security Governance program which reflects this integration with Corporate Governance (R. von Solms & von Solms, 2006).

Hinson (2007) outlined the importance of I.T. audit with regard to information protection (Hinson, 2007). Information Technology auditors best audit against an approved standard; however, small-entity financial institutions have yet to adopt a standard.

Policies and procedures communicate and control access to information assets and other resources. Policies are developed for accomplishing the business objectives and the procedures then support how they will be enforced. Internal control is established through design of sound policies and procedures (Mader & Srinivasan, 2005). Any information security program should include appropriate policies and procedures to carry out effective information security practices.

With these important concepts in mind, the SMEISP framework identified in Figure x was developed:

Figure III: SMEISP Diagram



The two major pillars of the program include the IT Risk Assessment and the IT Audit. The IT Risk Assessment evaluates the use of technology to identify appropriate compensating controls, while the IT Audit evaluates the compliance and adequacy of these controls. In between these important programs are the rest of the programs:

- **Security Awareness** – Involves ensuring that the people working in the bank understand what they can do to protect sensitive bank information.

- **Business Continuity** – Involves ensuring continuity of operation for those systems that the bank cannot live without.

- **Incident Response** – Involves a prevention and detection program on a repeatable way to handle security incidents.

- **Vulnerability Assessment** – Involves an internal scan of a bank's network to find network vulnerabilities.

- **Penetration Test** – Involves an external scan of a bank's network to simulate the activities of an external hacker.

- **Asset Management** – Small-entity financial institutions must inventory their electronic assets to ensure they know what systems are storing, processing and transacted sensitive customer and financial information. Further, small-entity financial institutions must develop procedures to ensure the appropriate disposal of assets.

- **Vendor Management** – Controls how vendors and service providers are selected and managed. Small-entity financial institutions can outsource the development or hosting of a system; however, they remain responsible and accountable for ensuring the confidentiality, integrity and availability of the information stored, processed and transacted on the system.

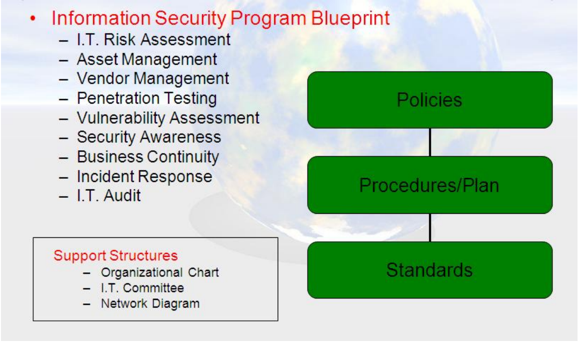
These mandatory programs relate to each other and have many interdependencies. Two examples: the risk assessment will identify the "availability" requirement for each system and the business continuity program will ensure continuity of operation for those assets with high availability needs. A second example is risk assessment will identify which assets have external connectivity and the penetration test will test these assets to understand how they could be compromised by hackers.

The program includes three support structures: an IT Committee to ensure that more than more set of eyes is involved in managing security, a network diagram and an organization chart to ensure all network components and security personnel are documented and accounted for.

Finally, the program includes an optional set of policy depending upon the IT risk assessment. For example, does the bank need an Internet Banking policy? It depends upon the controls identified in the IT risk assessment. The same is true for all other lower-level policies. This is why the IT risk assessment must be completed prior to developing lower-level information security policy.

Another way to look at the SMEISP program is as follows:

Figure IV: SMEISP Diagram II



- Information Security Program Blueprint
  - I.T. Risk Assessment
  - Asset Management
  - Vendor Management
  - Penetration Testing
  - Vulnerability Assessment
  - Security Awareness
  - Business Continuity
  - Incident Response
  - I.T. Audit

Support Structures
- Organizational Chart
- I.T. Committee
- Network Diagram

Policies

Procedures/Plan

Standards

SMEISP includes the mandatory programs required for small and medium sized community banks, support structures to augment these foundational programs and an ISMS represented by a set of policies, procedures, plans and standards. This management framework provides the board of directors and IT committee at small and medium-sized financial institutions with the sheet music to get everyone on the same page with regard to a management framework for information protection at their bank.

SMEISP CASE STUDY

The researcher introduced and implemented the new information security framework in three small-entity financial institutions to test and evaluate the model. The small-entity financial institutions included:

- $150 million community bank with three branches in the Midwest

- $2.0 billion community bank with 30 branches in the Northwest

- $12 million credit union in the Midwest

The researcher worked with the management team of each financial institution to operationalize the framework over three to six months. Table IV outlines the steps.

Step	**Description**
1	Write or update the business and

	technology strategy
2	Establish the IT Committee
3	Write or revise the top level information security policy, including policies for IT risk assessment, asset management, penetration test, vulnerability assessment, business continuity, security awareness, incident response, vendor management and IT audit.
4	Gain Board of Director (Board) approval for the top level information security policies
5	Update asset inventory for information-based assets
6	Conduct an IT risk assessment to evaluate the use of technology and identify appropriate compensating controls
7	Review IT risk assessment results with IT Committee and Board
8	Write or revise the organizational chart
9	Write or revise the network diagram
10	Review organizational chart and network diagram with the IT Committee
11	Identify and write additional lower-level policy based on the IT risk assessment
12	Gain Board approval for the lower-level information security policies
13	Conduct security awareness program with employees and others
14	Review the results of the security awareness training with the Board
15	Develop and test the business continuity plan
16	Review the results of the business continuity test with the Board
17	Write or revise the incident response plan
18	Conduct Penetration Test and review the results with the IT Committee
19	Conduct Vulnerability Assessment and review the results with the IT Committee
20	Conduct IT audit
21	Review the IT audit results with the Board

While more steps were executed, these were the primary tasks to implement this framework.

The feedback from the three institutions was phenomenal. All of the executives appreciated a clear roadmap that they could use to design and implement their information protection program. Further, they liked being able to point to a document that succinctly illustrates the program. This was important so that employees, consultants, business partners, Board members, IT Committee members and the management team were all on the same page, used the same terminology, and had a general plan regarding this emerging and confusing problem called information security. Also, management indicated a liking that the program could be done in phases: top-level policy and lower-level policy. This approach made the framework doable and clearly prioritized the activities.

Two of the three small-entity financial institutions completed their regulatory exam after their new information security program was operationalized. The FDIC was the regulatory body. The feedback from regulators was very positive. While regulators will find improvements, these recommendations were small and the organizations were very happy with their IT examination.

CONCLUSIONS AND FUTURE WORK

Data breaches continue to rise and financial institutions are required to have a documented information security program commensurate with their size, complexity and use of technology. Small and medium-sized financial institutions struggle to complete this task as no model exists that meets their unique needs. This paper outlined an innovative model honed to the specific needs of small and medium-sized financial institutions, and discussed the feedback from rolling out this model in several pilot small and medium-sized financial institutions.

The researchers intend to implement the framework in more small-entity financial institutions. Further, feedback from the OCC, Federal Reserve and NCUA is important to continue to validate and improve the model. Finally, the researcher intends to do more formal model evaluation, including pre and post assessments to determine differences as measured through management, employees and regulators. Finally, there is no reason to believe that the SMEISP management framework has utility beyond the financial services marketplace, and researchers need to test the SMEISP model in other industries to determine merit.

REFERENCES

27001 Information Security Standard. (2005): International Standards Organization.

Bowen, P., Hash, J., & Wilson, M. (2006, October). Information Security Handbook: A Guide for Managers.

Brenner, J. (2007). ISO 27001: RISK MANAGEMENT AND COMPLIANCE. *Risk Management, 54*(1), 24.

Brian, F. (2007). Banks Claim Share of Credit Card Security Costs Is Unfair. *Computerworld, 41*(26), 14.

Bruno-Britz, M. (2006). Corillian Maps to ISO Security Standard -- Company's certification to ISO 27001 standard to provide greater assurance to clients. *Bank Systems & Technology, 43*(8), 19.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2007, September). Performance Measurement Guide for Information Security (DRAFT).

Clinton, W. (1998). *Presidential Decision Directive 63*. Washington, DC: The White House.

COBIT 4.1. (2007). IT Governance Institute.

Colin, W. (2000). Security is an essential ingredient. *The Banker, 150*(896), 132.

Cooper, M., Lipinski, S. A., Cook, C., & Orndorff, C. (2007). Is 3 pace: casting the information security spell for cultural change (pp. 41-45): ACM Press New York, NY, USA.

Courtney, R., Burrows, J., McNulty, L., Katzke, S., Gilbert, I., & Steinauer, D. (1995, October). An Introduction to Computer Security: The NIST Handbook.

Dan, V. (2003). Feds Say IT Security Lacking. *Computerworld, 37*(49), 1.

Financial Services Industry Launches New Critical Infrastructure Protection Initiatives. (2003). *PR Newswire*, 1.

Greenemeier, L. (2006). Follow The ISO Path To Security. *InformationWeek*, 69.

Gutierrez, C. M., & Jeffrey, W. (2006, March). Minimum Security Requirements for Federal Information and Information Systems. *Federal Information Processing Standards Publication*, 17.

Hinson, G. (2007). The State of IT Auditing in 2007 (Vol. 36, pp. 13-31): Taylor & Francis.

Information Security IT Examination Handbook. (2006). Retrieved. from.

Interagency Guidelines Establishing Information Security Standards: Small Entity Compliance Guide. (2005). Retrieved. from.

Jaikumar, V. (2007). Credit Union Bills TJX $590k for Breach Costs. *Computerworld, 41*(24), 10.

Jenn, A. (2007). TJX faces class action lawsuit in data breach. *Knight Ridder Tribune Business News*, 1.

Jonathan, B. (2007). Banks to press retailers on data security FRAUD. *Financial Times*, p. 19.

Karen, K. (2006). As Data-Breach Fears Grow, Banks Need to Inspire Calm. *USBanker, 116*(4), 16.

Mader, A., & Srinivasan, S. (2005). Curriculum development related to information security policies and procedures (pp. 49-53): ACM Press New York, NY, USA.

McGlasson, L. (2009). Heartland Payment Systems, Forcht Bank Discover Data Breaches Both Companies Might be Victims of Larger Fraud Schemes. Retrieved February 5, 2009 from www.bankinfosecurity.com

Michael, T. C., Jr. (2007). Protecting Consumers Is Job No. 1. *Hoosier Banker, 91*(5), 14.

NIST Website. (2007). Retrieved October 27, 2007, from www.csrc.nist.gov/publications/PubsSPs.html

Peltier, T. R. (2005). *Information Security Risk Analysis*: Auerbach Pub.

Price, R. L., Cotner, J. S., & Dickson, W. L. (1989). Computer Fraud In Commercial Banks: Management's Perception. *Journal of Systems Management, 40*(10), 28.

PrivacyRights. (2007). Retrieved October 23, 2007, 2007

Robin, S. (2007). Giant Retailer Reveals Customer Data Breach; Incident Could Affect Millions of Shoppers at T.J. Maxx, Marshalls and Other TJX Stores Dating Back to 2003. *Wall Street Journal*, p. D.1.

Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G., et al. (2005, February). Recommended Security Controls for Federal Information Systems.

Rycroft, S., & Tully, M. (2007). Building an information security Meta Standard (Vol. 25, pp. 37-40): Springer.

Steven, M. (2003). New information security guidelines issued. *Bank Systems & Technology, 40*(3), 10.

Streff, K. (2007). *Information Security in Banking:* IGI Publishing.

Streff, K., Rajagopalan, A., & Fu, X. (2007, March 15-16 2006). *ABC: Adaptive Bank-Transaction Camouflaging Systems.* Paper presented at the International Conference on i-Warfare and Security (ICIW), University of Maryland Eastern Shore, USA.

Su, X., Bolzoni, D., & van Eck, P. (2006). A Business Goal Driven Approach for Understanding and Specifying Information Security Requirements.

Swanson, M., Hash, J., & Bowen, P. (2006, February). Guide for Developing Security Plans for Federal Information Systems.

Symantec Internet Security Threat Report. (January-June, 2007).): Symantec Corporation.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively (Vol. 6, pp. 167-173): Emerald Group Publishing Limited.

Tipton, H. F., & Krause, M. (2004). *Information Security Management Handbook*: Auerbach Pub.

TJX Profit Falls 57% on Costs Tied to Data Breach. (2007). *Wall Street Journal*, p. B.3.

Violino, B. (2006). Sorting The Standards. *Computerworld*, *40*, 46.

von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? (Vol. 24, pp. 99-104): Elsevier.

von Solms, R., & von Solms, S. H. B. (2006). Information Security Governance: A model based on the Direct–Control Cycle (Vol. 25, pp. 408-412): Elsevier.

World's First ISO 27001 Certification Guides Launched [Electronic (2005). Version]. *PR Newswire*, 1 from http://www.ezproxy.dsu.edu:2048/login?url=?did=915699481&Fmt=7&clientId=18865&RQT=309&VName=PQD

Worthen, B. (2009). Card Data Breached, Firm Says. Wall Street Journal, January 20, 2009.