An Architectural and Process Model Approach to Information Security Management

Anene L. Nnolim
anene.nnolim@infotsg.com
Lawrence Technological University
Southfield, Michigan 48075, USA

Dr. Annette L. Steenkamp
steenkamp@ltu.edu
Lawrence Technological University
Southfield, Michigan 48075, USA

ABSTRACT

This paper reports on part of a doctoral dissertation research project in information security management. One of the aims of the project is to develop an architectural framework and a process model, with supporting methodology that could enable integration of information security management with enterprise life cycle processes. Over the years, the focus of information security evolved from physical security of computer centers to securing information technology systems and networks, to securing business information systems. With the Internet, computers can communicate and share information with other computers outside organization's networks. This meant that the existing security model was inadequate to meet the threats and challenges inherent in this new technology infrastructure. A new approach to information security management is needed to meet these security challenges. A meta model for the information security management viewpoint, developed in this research, includes various meta primitives, namely; business strategy and mission, security management goals and objectives, security management system, security management program, information security framework, security process improvement model with supporting methodology, and enterprise business systems. The elements of the architecture framework in this research are stakeholder, principles, purpose, level of abstraction, organization layer, context, representation scheme, modeling scheme, standards, and the required technology. An information security management process model in this research consists of four major phases, namely; planning, analysis and design, implementation, and operations and a process improvement sub-phase. Dissertation research results so far indicate a conceptual model that includes other security management models that are beyond the scope of this paper.

Keywords: information security management, architecture framework, security process model, security viewpoint, enterprise security, process improvement

INTRODUCTION

Before computer security evolved into its various dimensions of today, the primary security focus of most organizations was in physical protection of their assets. For organizations with early computers, this included securing and protecting data from natural disasters or malicious activities. With the advent of the personal computer and the internet, security objectives would eventually include computer security. This evolution of computer security strategies is shown in Table 1.

Table 1 Evolution of Computer Security Strategies

Time Frame	State of Affairs	General Location of Computers	Security Objective	Security/Strategy Methodology
Up to early 1980s	Computers used simply as business tools to automate business processes	Computers located in computer centers	Securing compute r centers	Accomplished through physical security
Up to early 1990s	Computers used throughout the enterprise (Distributed use of computers)	Computers located throughout the organization	Securing IT systems and networks	Through software residing on IT systems
Early 2000s to Present	IT systems supporting information as business assets	Computers located within and outside the enterprise	Securing business information systems	Through information security management

** (Developed from Vermeulen and von Solms, 2002)

Background Theory and Application

Information security issues affect every aspect of an organization's operations, and this is the case for both private and public sector organizations. Some of the prevailing security issues facing organizations include identity thefts, security of transactions over the Internet, viruses, Spyware, security breaches of confidential information, securing networks and databases, corporate accountability through Sarbanes-Oxley Act, internal controls through COSO (Committee of Sponsoring Organizations), information technology (IT) governance through COBIT (Control Objectives for Information and related Technologies), etc. In the enterprise, security architectures exist at the operational levels for networks, data, databases, applications, infrastructure, and web services. However, there is limited or non-existence of information security architecture for enterprise security governance.

Over the years, the focus of information security has evolved from the physical security of computer centers to securing information technology systems and networks, to securing business information systems. Computer centers have since evolved into data centers that house several servers and databases. These databases contain data and information that is critical to the enterprise economic survival and profitability. Over time, computer architecture evolved from stand-alone environments to networked systems. Prior to this, communication between computers was practically non-existent. The advent of networked computer systems ushered in a new era in computer communications.

The proliferation of computer networks and the advent of the Internet added another dimension to information security. With the Internet, computers can communicate and share information with other computers outside an organization's networks and beyond their computer center. This new mode of communication meant that the existing security model was inadequate to meet the threats and challenges inherent in this new technology infrastructure. A new model of information security management is needed to meet the security challenges presented in this new environment. The objective of the new model would be the protection of business information systems in the enterprise, and securing the business operations environment. Part of meeting this new challenge would also include the resurrection of risk management as an important component of information security management.

What is information security? A broad definition of information security is given in ISO/IEC 17799 standard as:

> The preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods), and availability (ensuring that authorized users have access to information and associated assets when required (ISO/IEC 17799, 2000, p. viii).

Some authors, like Hong, Chi, Chao, and Tang (2003), see information security as the "application of any technical methods and managerial processes on the information resources (hardware, software, and data) in order to keep organizational assets and personal privacy protected" (Hong et al, 2003, p. 243). Information security is concerned with protecting and securing enterprise information resources.

What is information security management in the enterprise context? Vermeulen and Von Solms (2002) define information security management in terms of an architectural framework. They contend, "information security management refers to the structured process for implementation and ongoing management of information security in an organization" (Vermeulen and Von Solms, 2002, p. 120). To put their definition in context, architectural framework may be looked at as "…a set of tools, methods, processes, and vocabulary that can be used for devel-

oping a broad range of different IT (information technology) architectures…" (Perks and Beveridge, 2003, p. 437). Of course, the range of architectures would include information security management. On the other hand, Perks and Beveridge (2003) consider framework as "…a reasoned, cohesive, adaptable, vendor-independent, domain-neutral, and scalable conceptual foundation for detailed architecture representation" (Perks and Beveridge, 2003, p. 77 and p. 437). An architectural framework then, is an important mechanism in developing architectural descriptions.

Rungta, Raman, Kohlenberger, Li, Dave, and Kime (2004) argued in favor of a new approach to managing information security in the enterprise. As IT security evolved over the years, enterprise security strategies tended to focus on the perimeter of controls and risk reduction within the enterprise network system. But, with the increased interaction between multiple computers within the enterprise, across organizations, and across several geographical boundaries, the study concluded that it was necessary to develop security management strategies to reflect the new technology infrastructure, and that existing policies and management framework for enterprise security management are inadequate (Rungta et al, 2004, p. 304).

As these events unfolded, it seemed that most of the efforts to manage information security were focused on the technical and operational levels. Even at these levels, there seemed to be an absence of a formal framework or methodology for managing information security. Some authors have attempted to provide some reasons for the absence of a methodology. Hong et al (2003) suggested that one of the reasons might be a lack of a theoretical framework for the management of information security in the enterprise. Specifically, they observed that,

> Because of the lack of an information security management theory, there are few empirical studies conducted to examine the effectiveness of management strategies and tools (Hong et al, 2003, p. 243).

By implication, this also means an absence of guiding principles for information security management. Hong et al (2003) suggested that one of the reasons for a lack of theoretical framework in information security management could be due to inconsistent security policy theories. They observed, "…there is no consistent security policy theory so far…" (Hong et al, 2003, p. 244). To support this observation, the authors pointed to three different perspectives on information security policy theory. In the first example, Hong et al (2003) referred to Kabay's (1996) policy theory perspective that:

> … the establishment of information security policy should include five procedures, which are to assess and persuade top management, to analyze information security requirements, to form and draft policy, to implement the policy, and to maintain the policy (Hong et al, 2003, p. 244).

In the second example, Hong et al (2003) referred to Rees, Bandyopadhyay, and Spafford (2003) perspective on information security policy framework theory.

The information security policy life cycle proposed by Rees addressed four parts, namely policy assessment, risk assessment, policy development, and requirements definition, and review trends and operations management (Hong et al, 2003, p. 244).

In the third example, Hong et al (2003) presented yet another policy theory perspective by Flynn (2001) stating that:

> The e-policy proposed by Flynn (2001) covers comprehensive e-audit, e-risk management policy, computer security policy, cyber insurance policy, e-mail policy, Internet policy, and software policy (Hong et al, 2003, p. 244).

It would seem then that information security management has not reached the maturity level in the enterprise, which could make it a repeatable management process. This lack of repeatability as a management process, plus the need to meet security challenges presented in the evolving technology environment, has motivated the focal area of this research in information security management.

Focal Theory and Application

Information security management could also be looked at in terms of architectural viewpoint. The Open Group (2006) defines a viewpoint, also known as a metaview, as:

> A specification of the conventions for constructing and using a view. A metaview acts as a pattern or template of the view, from which to develop individual views. A metaview establishes the purpose and audience for a view, the ways in which the view is documented (e.g., for visual modeling), and the ways in which it is used (e.g., for analysis) (The Open Group, 2006, p. 438).

A view is defined as "…a representation of a whole system from the perspective of a related set of concerns" (The Open Group, 2006, p. 438). The various security viewpoints in the enterprise are physical security, data security, information security, application security, and infrastructure security. Enterprise refers to the highest level in an organization, and includes organizational goals and objectives, mission, vision, business strategies, and all organization functions and activities.

Information security management in the enterprise may be viewed at three main levels, namely strategic, tactical, and operational. These three levels correspond to the types of security issues that are of concern to senior management, including the general nature of expertise required to manage security, at that level (Belsis, Kokolakis, and Kiountouzis, 2005, p. 193). The motivators or information requirement, for security management are that it should be policy-driven (strategic level), guideline-driven (tactical level), and measures-driven (operational level).

Other distinguishing factors between the different organizational levels of security management are that strategic level affects corporate strategy, tactical level relates to processes and methodologies used to manage security, and at the operational level, the installation, and operation of security tools and measures are prominent (Belsis et al, 2005, p. 193). It would seem that the focus of information security management activities in the past have been at the operational level. Slewe and Hoogenboom (2004) alluded to this when they noted "...for security measures the focus is often on logical and technical measures…" (Slewe and Hoogenboom, 2004, p. 60). This concept of organization level of security management is shown in Figure 1.

Figure 1 Organizational Levels of Information Security Management

Information security could be managed effectively, in the enterprise, using an architectural approach. Using this approach would require that information security be managed along side other architectures in the enterprise, such as business, information, application, and infrastructure architectures. Others, like IEEE 1471 (2000), define architecture as,

> The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution (IEEE 1471-2000).

The Open Group (2006) defines architecture as:

1. A formal description of a system or detailed plan of a system at component level to guide its implementation, and
2. The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time (The Open Group, 2006, p. 430).

Perks and Beveridge (2003) define architecture as,

> …a pragmatic, coherent structuring of a collection of components that through these factors supports the vision of the full user in an elegant way (Perks and Beveridge, 2003, p. 435).

In addition, Schekkerman (2004) defines architecture as,

> …the structure of elements, their interrelationships and the principles and guidelines governing their design and evolution over time (Schekkerman, 2004, p. 22).

On the other hand, Morrogh (2003) defines information architecture as,

> …primarily about the design of information environments and the management of an information environment design process (Morrogh, 2003, p. 6).

Information security architecture, involves the pragmatic and structured design of information environments, which enable the management of information security in a coherent manner.

Purpose of Research

The intent of this research is to examine information security management in the enterprise. It will attempt to determine how information security management could be enhanced as a structured and repeatable management process. The research also aims to develop an appropriate framework and methodology, which could enable integration of information security management with other enterprise business processes.

The results of the research would be important to any organization with a need for a secure business environment. The research results will also be important to individuals responsible for managing information security in their organizations, as wells as to senior executives and members of corporate boards of directors, because of their increased statutory responsibilities to secure various types of information in their organizations (Nnolim and Steenkamp, 2007).

Research Problem

There is a lack of a comprehensive framework, supporting process model, and methodology that can enable an enterprise to implement and effectively manage information security.

Scope of Research

This research project is limited to examining information security viewpoint in the context of enterprise security domain shown in Figure 2. A cursory review of the composite enterprise security viewpoint shown in Figure 3, was undertaken, the purpose of which was to present the research findings in the appropriate context.

Figure 2 Enterprise Security Domain

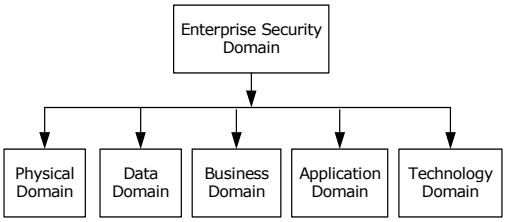
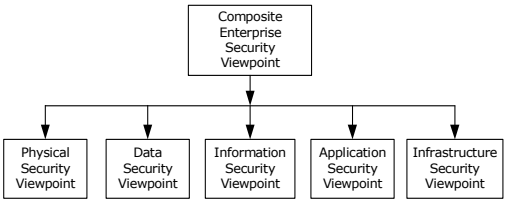


Figure 3 Composite Enterprise Security Viewpoint



Research Questions

Related to the research problem statement are the following research questions. These questions cover important aspects of information security management, i.e. principles, policy framework, integration with management processes, and its significance to enterprise planning process.

> Question 1:
>
> What are the underlining principles influencing the transition of information security, from a traditional IT environment of managing data and application security, to managing information security as an integrated component of the enterprise business strategy and management process?

Question 2:

How can an enterprise security framework facilitate the effective management of information security?

Question 3:

How can information security management become a significant element of the enterprise strategic planning model?

Research Proposition

This research is based on the following propositions:

1. Enterprise information security can be managed effectively using a framework-based approach and supporting methodology.
2. Information security management could be a structured and repeatable management process if a systematic approach is followed to its implementation.

2. LITERATURE REVIEW

The literature review for the main doctoral dissertation research project is extensive. However, due to page limitations for this paper, an abbreviated version of the literature review is reported here.

Background Theory and Application

Security Control Model

In any security environment, one of the main concerns of security professionals is awareness of all possible security loopholes that may exist. The intent, generally, is to implement adequate controls to cover such loopholes. van der Haar and von Solms (2003) propose a model, Information Security Control Attribute Profile (ISCAP), which could provide this solution. The rationale of this model is that organizational properties tend to determine an organization's security goals/levels (van der Haar and von Solms, 2003, p. 235). In other words, the information security goals of an enterprise should be aligned with enterprise business strategies. Examples of organizational properties are industry type, business culture, purpose of the business, etc. These properties would necessitate the security goals and level of security required in the organization. Examples of security goals could be high level of system reliability, medium level of confidentiality, etc.

In the security control model, control attributes are first determined using prescribed standards, for example ISO/IEC 17799, BS 7799, etc. as inputs to the process. Next, organizational properties are aligned to the security goals/levels. Security goals/levels are then aligned with the stated control attributes. Finally, organizational properties are used to identify the applicable required control attributes. The difference between ISCAP and risk management models, as tools for information security management, is that ISCAP uses a top-down approach, while risk management models use a bottom-up approach. Overall, it is important to have a formal process for determining security goals and objectives.

Process Model Theory

Although the issues of enterprise modeling techniques mentioned in the study by Dalal, Kamath, Kolarik, and Sivaraman, (2004) is focused on enterprise resource planning (ERP) systems, most of the issues are applicable to information security management. For example, a need for a theory base, a need for new process modeling semantics that are explicit enough to reflect the concept of cost and time, and a need to link business and technical processes (Dalal et al, 2004, p. 85) are all applicable to information security management. Similarly, it is necessary to link information security program to overall business strategy. It is generally understood that a theoretical base usually creates good foundations for formal analysis, whether it is ERP systems or information security management. By implication, there is the need for a comprehensive theoretical foundation for the design and development of information security management models. This is part of the motivation for the research problem.

Socio-ethical Framework

In their study, Trompeter and Eloff (2001) discuss ethics in IT and argue that it is a fundamental component of information security management. It makes the point that, in the past, most security management efforts were focused on technical solutions. However, as information security manage-

ment becomes increasingly seen as a business issue, managing ethics also has become just as important. It is in this context that a framework to implement socio-ethical controls in information security management is being proposed. The proposed framework would link security policy to socio-ethical issues.

Socio-ethical information security awareness is defined as the "conforming of an organization to recognized information security ethical principles" (Trompeter and Eloff, 2001, p. 386). Employees would therefore be required to conform to a standardized and recognized code of ethical behavior in the organizational environment. The model, as described by the study, would represent layers of building blocks, namely e-business (foundation block), technical services, baseline standards, adherence to law, socio-ethical information security awareness, and security policies and procedures. These would culminate eventually to information security management. It is possible that using a framework to implement socio-ethical controls will increase the level of information security awareness among employees.

Focal Theory and Application

Process Model

Enterprise architecture could be used to integrate the various processes within the organization. As generally understood, business processes tend to focus on individual processes with no enterprise perspective. Anaya and Ortiz (2005) define enterprise architecture as "a set of descriptive representations (i.e. models) that are relevant for describing an enterprise such that it can be produced to management's requirements and maintained over the period of its useful life" (Anaya and Ortiz, 2005, p. 25). If this definition of architecture is applied to information security management, it is possible then to develop a set of process models for information security management that are adaptable to different management's requirements.

To achieve this goal, organizations may have to make the transition from their present organizational structures to a different one that would utilize a value-chain approach to business processes. The conclusion that can be derived from their study is that enterprise architecture could be used to identify organizational integration problem, and at the same time use it to manage enterprise processes. In this respect, enterprise architecture will be a useful tool for information security management process.

Multi-level Architecture

In this study, Duflos (2002) describes the use of multi-level architecture to manage security for distributed multimedia services using policies. The three levels of architecture described are network management, middleware management, and service management (Duflos, 2002, p. 654). This reiterates the point made earlier by Anaya and Ortiz (2005) regarding the use of enterprise architectures as management tools. These three levels of security architecture described in the study could be analogous to the three organizational levels of information security management i.e. strategic, tactical, and operational. Therefore, in developing any enterprise architecture, the three organizational levels of information security management would have to be prominent.

Process-centric Approach

As more organizations adapt from department structures to a process-centric approach to business process, the need to align IT strategies, including information security management, with the business strategies becomes important. Brown and Ross (2003) discuss the need to design IT organizations that could support these process-centric entities. Some organizational initiatives often result in implementation of common enterprise level process. At other times, organizations integrate various processes by cross-function, or globalization, or through business restructuring (Brown and Ross 2003, p. 36). This cross-function integration often presents opportunities to integrate information security management with new processes. For example, in a cross-function integration, information security enterprise architecture can act as an enabler for better management of a new process, as information security management becomes an integral part of overall enterprise business strategy.

Organizational Factors

Chang and Ho (2006) developed four null hypotheses in an attempt to determine the impact of organizational factors on the effectiveness of implementing an information security management standard. The hypotheses used four organizational factors as positive determinants of information security management, namely IT competence of business managers (H1), environmental factors (H2), industry type (H3), and organization size (H4). Using quantitative techniques, the study was able to provide evidence to accept all four hypotheses, i.e. the four organizational factors had significant impact on the effectiveness of implementation of information security management standard (Chang and Ho, 2006, p. 356).

Other issues that came out of their study were that security problems are caused by human errors, and that training and managing individuals on security matters is an important part of information security management (Chang and Ho, 2006, p. 346). This seems to echo the point made by Campbell (2006), regarding the role of human behavior in information security management. The study also points out that information security is not only a technical issue, but a management and business issue as well. The study also argued that in addition to standards, methodology is also an important aspect of information security management (Chang and Ho, 2006, p. 347).

3. RESEARCH DESIGN AND PROCEDURES

The research design was impacted by the findings of the literature review. As noted earlier, due to page limitations for this paper, the literature review reported in Section 2 is an abbreviated version of the comprehensive literature review conducted for this research.

Research Methodology

The research approach followed in this research is mixed methods since this is a problem-centered research. The strategy of inquiry for this approach is concurrent procedures. Concurrent procedures strategy is defined as situations "… in which the researcher converges quantitative and qualitative data in order to provide a comprehensive analysis of the research problem" (Creswell, 2003, p. 16). The rationale for selecting mixed methods design is to get a better understanding of the problem identified in this research. The mixed methods approach would allow for both text and statistical analyses of data, and would permit more flexibility when designing questions for survey interviews, i.e. both open- and close-ended questions (Creswell, 2003, p. 17). In this research, the survey design for the interview included both open- and close-ended questions.

The knowledge claim position for this research is pragmatism. Creswell (2003) noted that some of the characteristics of pragmatism knowledge claims are problem-centered, consequences of actions, real-world practice oriented, and pluralistic (Creswell, 2003, p. 6). These characteristics fit within the scope of this research.

In summary, the methods adopted for this research includes the following:

1. Conducted a review of literature in enterprise security, that includes an in-depth review of literature in information security management viewpoint, and perform a comprehensive analysis of literature on information security management.
2. Developed a conceptual model of a solution to the information security management problem stated in the research proposal, i.e. the lack of a comprehensive framework, supporting process model, and methodology that can enable an enterprise to implement and effectively manage information security.
3. Demonstrated the conceptual model of the solution to the research problem by the following means:
    a. Conducted in-depth structured interviews of senior executives, with decision-making responsibilities for security management in their organizations, using a set of interview questions that were derived from the draft conceptual model.
    b. Presented summary of a draft conceptual model, at national and international professional and academic

conferences, for review by group of peers, academics, security management professionals, managers, and senior executives from various industries.

c. Outlined how the conceptual model of the solution could be implemented in an organization.

The research process model used for this research is shown in Appendix A, and it outlines the various activities, timelines, and expected deliverables.

Technologies and Management Concepts Used in this Research

Various office, application, and communication technologies were used throughout this research project. These tools and technologies were used effectively in this research project because of the knowledge and skills gained from several years experience using the tools and technologies. Some of the tools and technologies include:

- Microsoft office tools and technologies, e.g. picture manager, document scanner, document imaging, graphics, etc.
- Microsoft Office Suite of applications, i.e. Word, Excel, PowerPoint, Visio, Project, Outlook, Publisher, etc.
- ProVision by Metastorm for process design, process modeling, information architecture, meta modeling, etc.
- Internet technologies, i.e. browsers, search engines, multi-media tools, etc.

The knowledge and skills gained from own experience in various management concepts, were applied throughout this research project. Some of these skills and knowledge are in the following areas:

- Project management.
- Process analysis; process design; process modeling.
- Information architecture; process architecture.
- Business ethics; conflict management.
- Strategic planning.

Data Collection and Analysis Methodology

Interviews were conducted in this research. The intent was to gather data through in-depth structured interviews, with five information security decision makers from different organizations in different industries. Thirteen organizations were solicited for participation in the interview, but only five accepted. Of those that declined to participate, the most cited reason was an unwillingness to discuss their organization's security matters with a researcher.

The population for the research interview is potentially infinite, because it includes all public and private organizations of all sizes that have a need for a secure operating environment. Because of the potential population size, the sampling method used for the interview is purposive sampling and as such, it is a non-probability sampling. Purposive sampling refers to situations where participants are selected based on their "… specialized insight or special perspective, experience, characteristic, or condition that we wish to understand" (Yegidis and Weinbach, 1996, p. 122). Participants for the research interviews are individuals with specialized insight on security management issues. They possess the experience and perspective in information security management that this research wishes to understand. Given the security management experience and background of potential interviewees, purposive sampling method seems the most logical choice for data collection in this research.

Using a statistically significant sample for this survey interview would not be feasible or practical. The nature of the research subject matter, i.e. information security, could cause potential organizations included in a statistically significant sample to be unwilling to participate in the survey. This action alone has the potential to distort any results derived from using such a statistically significant sample. In addition, those organizations that would participate, because they are included in the statistically significant sample, may not be willing to discuss their security issues with a researcher in a candid manner. These potential actions were evident from the reasons given by majority of the eight organizations that were solicited

but declined to participate in the structured interviews.

The interview document, shown in Appendix E, includes 59 questions, classified into eight groups, as follows:

A. Security Management Program (9 questions).

B. Security Governance (8 questions).

C. Risk Management (7 questions)

D. Security Policy (8 questions).

E. Security Management System (9 questions).

F. Infrastructure (6 questions).

G. Technology (8 questions).

H. Outcomes (4 questions).

These groups were identified based on insights gained from own professional experience, analysis of the literature on the background and focal theories, and their application in the field of information security management. A draft conceptual model of the solution to the research problem, developed as a result of all of the above experiences, formed the basis for developing interview questions.

The scale of measurement for the interviews was explicit answers, and some "yes" or "no" answers. The questions were electronically mailed to interviewees approximately one week before their scheduled interview date. The average time for the interviews was 75 minutes. All interviews were conducted face-to-face, in person, at the interviewees' site of business.

Generally, one of the data analysis methodologies for concurrent procedures strategy is data transformation. That means quantifying qualitative data, i.e. creating themes qualitatively from collected interviews data, tallying the number of occurrences of the themes in the collected data, and using the themes to report analysis of the data. Creswell (2003) noted that quantification of qualitative data enables a researcher to compare quantitative results with qualitative data (Creswell, 2003, p. 221). This research used the data transformation methodology to analyze interview data. One of the eight primary strategies suggested by Creswell (2003) for checking the accuracy and validity of findings is the use of rich, thick descriptions to convey the findings (Creswell, 2003, p. 196). In this research, the strategy was to develop a detailed description of interview findings, and feedback from peer reviews.

Limitations of Research Design

Because of the nature of the subject matter of information security, and based on own experience most organizations are unwilling to discuss their security issues with a researcher in a candid manner. In fact some organizations declined to participate in the interviews.

It is neither feasible nor practical to use an actual organization to demonstrate the conceptual model of the solution, for a number of reasons. One is that even if an organization were to volunteer and participate, it would be several years before accurate data for analysis may be obtained. This could be an area for a future research project. Most organizations would not be prepared to invest resources to test theoretical concepts. In addition, the researcher would not have any input or control on the learning curves for all that would be involved.

4. RESEARCH FINDINGS

The doctoral dissertation research findings are classified into two major areas, namely; findings from the interviews, and findings from other research activities. Interview findings provided insight into how information security is managed in those organizations that participated in the research. Findings from other research activities clarified current issues in information security management.

Interview findings are described in terms of tables and charts, and are structured similar to the interview question groups, as follows:

- Information Security Management Program.
- Security Governance.
- Security Risk Management.

- Security Policy and Planning.
- Security Management System.
- Infrastructure.
- Technology.
- Outcomes (Security Environment).
- Miscellaneous.

Details of the interview findings will be presented at the conference.

During the interviews, it was observed that there were several variables in the management of information security in the enterprise. On further discussions with interviewees, additional insight was gained on how these variables affected information security management in the enterprise. Using this insight and own professional experience, these variables were classified according to how they affect security management, namely: dependent, independent, and intervening or mediating variables. These variables are shown in Table 2.

Table 2 Dependent, Independent, and Intervening Variables

Dependent Variables	Independent Variables	Intervening or Mediating Variables
Security management strategy.	Organization's industry.	Organization's existing governance model.
Security management framework.	Existing infrastructure.	Compliance strategy.
Security management system.	Organization hierarchical structure.	Enterprise life cycle process models.
Security management process methodology.	Enterprise strategic plan.	Existing security tools.
Security plan.	Organization's goals and objectives.	Business systems architecture.
Security policy.	Business strategy/ mission.	
Security training and awareness.	Stakeholder.	
Security management program.	Existing technology.	
Security architecture.	Available resources.	
Security management capability.	Regulatory requirements.	

Additional research findings emanated from an analysis of current trends and issues in security management; review of legislative and regulatory issues pertaining to information security; and peer reviews feedback at the three conference presentations.

One of these findings relate to security breaches. In the past two years, there have been a series of widely publicized security breaches in various organizations, including the government. During this period, the total number of records containing sensitive personal information involved in reported security breaches is 158,051,696 (Privacy Rights Clearinghouse, 2007). Privacy Rights Clearing House (2007) maintains a complete list of all reported security breaches for the period 2005 to 2007 (Privacy Rights Clearing House, 2007).

Also, a study, named "The State of Information Security 2006" conducted by CIO, CSO, and PricewaterhouseCoopers, was reviewed because of its relevance to this research. Some of the findings in the study are similar to those in this research interviews, and are referenced in the detail interview findings reported in the main dissertation report. Some of these will be presented at the conference. The state of information security study was a survey of 7,791 executives, senior managers, IT, and security professionals from more than 50 countries. It has a margin of error of 1% (CIO, CSO, and PricewaterhouseCoopers, 2006, p. 3).

The draft conceptual model was later refined based on own professional experience, the insights gained from analysis of literature on the background and focal theories, and their application in information security management, analysis of interview findings, and from research activities at this stage of the research. The outcome is a proposed conceptual model of the solution, which is a comprehensive information security management approach that comprises various components. Components of the conceptual model of the solution that are within the scope of this paper are:

- Information security management meta model.
- Information security framework.
- Information security management process model.

Information Security Management Meta Model

A meta model, developed in this research, for the information security management

viewpoint includes various components. Details of the meta model will be presented at the conference. Some elements (the meta primitives) of the meta model are business strategy and mission, security management goals and objectives, security management system, security management program, information security framework, process improvement model with supporting methodology, and enterprise business systems (Nnolim and Steenkamp, 2007). A partial meta model of the information security management meta model is shown in Appendix B.

Information Security Framework

Based on own professional experience, insights gained from the analysis of literature on various architecture frameworks such as DMIT framework, TOGAF, Zachman, The Index Model, etc., and discussions with Dissertation Committee Supervisor, an information security framework was developed in this research.

As with architecture definitions, there are various but similar definitions of architecture framework. Perks and Beveridge (2003) views architecture framework as,

> …a reasoned, cohesive, adaptable, vendor-independent, technology-independent, domain-neutral, and scalable conceptual foundation for detailed architecture representation (Perks and Beveridge, 2003, p. 77).

The Open Group proposes the following expectations that an architecture framework should be able to meet, i.e.

1. It (architecture framework) should describe a method for designing an information system in terms of a set of building blocks, and for showing how the building blocks fit together.
2. It should contain a set of tools and provide a common vocabulary.
3. It should also include a list of recommended standards and compliant products that can be used to implement the building blocks (The Open Group, 2006, p. 4).

In adopting an architecture framework in this research, for the information security viewpoint, some of the above issues were taken into consideration. While there are several architecture frameworks in use today, some like Boar (1999) and The Open Group (2000) have a focus on technical IT architectures. At Lawrence Technological University's Doctoral program, some earlier work on enterprise architectures adopted the Index Model. Based on that experience, an architecture framework for information security viewpoint that was adopted for this research is the DMIT framework (Steenkamp, 2006).

An architecture framework is an important mechanism in developing architectural descriptions, and The Open Group (2006) views an architectural framework as a tool that may be used for developing a broad range of different architectures (The Open Group, 2006, p.4). Details of the information security framework will be presented at the conference. The important elements of this framework are stakeholder, principles, purpose, level of abstraction, organization layer, context, representation scheme, modeling scheme, standards, and required technology (Nnolim, 2007)

Information Security Management Process Model

The information security management process model, shown in Appendix C, consists of four major phases, namely; planning, analysis and design, implementation, and operations, and a process improvement sub-phase. The sub-phase occurs if the objective of the security management initiative is only to improve a specific security management process or activity.

In Appendix C, the security management process starts in the planning phase. In this phase, if the aim of the project is security process improvement then the next step would be the process improvement sub-phase. If additional analysis is required before proceeding with the process improvement, then the next step would be the analysis and design phase. On the other hand, if no security process improvement is required, the next stage, from the planning phase, would be analysis and design.

In the analysis and design phase, new security processes are introduced, existing ones are refined, and those needing improve-

ments are enhanced. If the aim of the project is process improvement, the next step would be the process improvement sub-phase. Otherwise, the next step is implementation. New or enhanced security processes are implemented in this phase. It is important that implementation plans are integrated with other business processes, and consistent with organization's business strategies. From the implementation phase, there is transition to the operations phase. The operations phase consists of maintenance activities with feedback and links to other phases of the process model as well as other enterprise life cycle processes.

The information security management process model has a supporting methodology. This methodology shows how the security management process model could be implemented in an organization. The process methodology consists of 13 elements for each phase of the security management process model, except for the process improvement sub-phase. Appendix D shows the different phase elements of the process methodology. The process improvement sub-phase would use the appropriate methodology from any of the four phases depending on specific process improvement objectives. The elements may differ in each phase, but each has supporting methods, models or tools, and outputs or deliverables are produced for each phase element.

Details of the how the information security management process model, with the supporting process methodology, could be implemented in an organization are discussed in the main doctoral dissertation. Some of these details will be presented at the conference.

5. CONCLUSION

The findings of the research interviews show that current information security management in some of the participating organizations, generally lack a formalized comprehensive framework-based approach. This seemed to have an adverse effect on the effective management of information security in those organizations. Results of the State of Information Security Study 2006 (CIO, CSO, and PricewaterhouseCoopers, 2006), provides support that information security management in organizations still lacks a formalized approach.

Discussion on the conceptual model of the solution to the research problem is beyond the scope of this paper. However, in the main dissertation research it was shown how enterprise security framework can facilitate effective management of information security. Information security architecture framework, developed as part of the conceptual model, is the tool used to develop architectural descriptions of security management viewpoint.

Information security is still a maturing discipline, and the management of information security is still evolving as a process. Further more, research findings seem to show that there is a need for a formal and systematic approach to managing information security in the enterprise. For example, in the interview findings, four out of five of the interviewees indicated that they would prefer a formal security management program in their organizations. Part of this formal approach to information security management includes:

- Information security management meta model.
- Information security framework.
- Information security management process model, with supporting methodology.

6. AREAS FOR FUTURE RESEARCH

Some aspects of information security management that are beyond the scope of the main dissertation research project are recommended for future research. These are:

- Determine whether there is a link between lack of formalized approach to information security management and a high probability of security breach in an organization.
- Look into how to measure security management effectiveness in the context of organization security strategy, and develop metrics to be used against security goals, and objectives.
- Determine a process and methodology to integrate information security govern-

ance architecture with existing corporate governance structures.

7. REFERENCES

Anaya, V., & Ortiz, A. (2005), How enterprise architecture can support integration, *Proceedings of the first international workshop on inter-operability of heterogeneous information systems*, Bremen, Germany, 25-30.

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005), Information systems security from a knowledge management perspective, *Information Management and Computer Security*, Volume 13, November 3, 189-202.

Boar, B. H. (1999), *Constructing Blueprints for Enterprise Architectures*, John Wiley and Sons, New York.

Brown, C. V, & Ross, J. W. (2003), Designing a process-based IT organization, *Information Strategy: The Executive's Journal*, Summer, Volume 19, Issue 4, 35-41.

Campbell, S. (2006), How to think about security failures, *Communications of the ACM*, January, Volume 49, Number 1, 37-39.

Chang, S. E., & Ho, C. B. (2006), Organizational factors to the effectiveness of implementing information security management, *Industrial Management and Data Systems*, Volume 106, Number 3, 345-361.

COBIT (2000), *Control Objectives for Information and Related Technologies*, 4th. Edition, IT Governance Institute.

COSO, Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org.

Creswell, J. W. (2003), *Research Design – Qualitative, Quantitative, and Mixed Methods Approaches*, 2nd Edition, Sage Publications, Thousand Oaks, California.

Dalal, N. P., Kamath, M., Kolarik, W. J., & Sivaraman, E. (2004), Toward an integrated framework for modeling enterprise processes, *Communications of the ACM*, March, Volume 47, Number 3, 83-87.

Duflos, S. (2002), An architecture for policy-based security management for distributed multimedia services, *Proceedings of the tenth ACM international conference on multimedia*, Juan-les-Pins, France, 653-655.

Flynn, N. L., (2001), *The Epolicy Handbook: Designing and Implementing Effective E-mail, Internet and Software Policies*, American Management Association, New York.

Hong, K., Chi, Y., Chao, L.R., & Tang, J. (2003), An integrated system theory of information security management, *Information Management and Computer Security*, Volume 11, Number 5, 243–248.

IEEE Std 1471 (2000), *IEEE Recommended Practice for Architectural Description*, American National Standards Institute/Institute of Electronic and Electronics Engineers (ANSI/IEEE).

ISO/IEC Std. 17799 (2000), *Information Technology – Code of Practice for Information Security Management*, International Standards Organization (ISO).

Kabay, M. E. (1996), *The NCSA Guide to Enterprise Security*, McGraw-Hill, New York

Morrogh, E. (2003), *Information Architecture – An Emerging 21st Century Profession*, Prentice Hall, Upper Saddle River, New Jersey.

Nnolim, A. L. (2007), *A Framework and Methodology for Information Security Management – Conceptualization of the Solution Report*, Dissertation Research, Lawrence Technological University, Southfield, Michigan.

Nnolim, A. L. & Steenkamp, A. L. (2007), Developing an Architectural Description for the Information Security Management Viewpoint, *Conference Paper Presented at The Open Group Enterprise Architecture Practitioners Conference,* Paris, France, April 24.

Perks, C., & Beveridge, T. (2003), *Guide to Enterprise IT Architecture*, Springer-Verlag, New York.

Privacy Rights Clearinghouse, (2007), San Diego, California

http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP, retrieved July 14.

Rees, J., Bandyopadhyay, S. & Spafford, E. H. (2003), PFIRES: A policy framework for information security, *Communications of the ACM*, July, Volume 46, Number 7, 101-106.

Rungta, S., Raman, A., Kohlenberg, T., Li, H., Dave, M., & Kime, G. (2004), Bringing security proactively into the enterprise, *Intel Technology Journal*, Volume 8, Issue 4, 303–311.

Schekkerman, J. (2004*), How to Survive in the Jungle of Enterprise Architecture Frameworks – Creating or Choosing Enterprise Architecture Framework*, Trafford Publishing, Victoria, British Columbia.

Slewe, T., & Hoogenboom, M. (2004), Who will rob you on the digital highway? *Communications of the ACM*, Volume 47, Number 5, May 2004, 56-60.

Steenkamp. A. L. (2006), *Architecture Framework Models,* Private Communications, Lawrence Technological University, Southfield, Michigan.

Steenkamp, A. L., & McCord, S. A. (2006), *Doctoral Research Prospectus*, Lawrence Technological University, Southfield, Michigan.

The Open Group (2000), *The Open Group Architecture Framework (TOGAF), Version 6.0*, The Open Group, San Francisco, California.

The Open Group (2006), *The Open Group Architecture Framework (TOGAF), Version 8.1 Enterprise Edition*, The Open Group, Berkshire, United Kingdom.

Trompeter, C. M., & Eloff, J. H. P. (2001), A framework for the implementation of socio-ethical controls in information security, *Computers and Security*, Volume 20, 384-391.

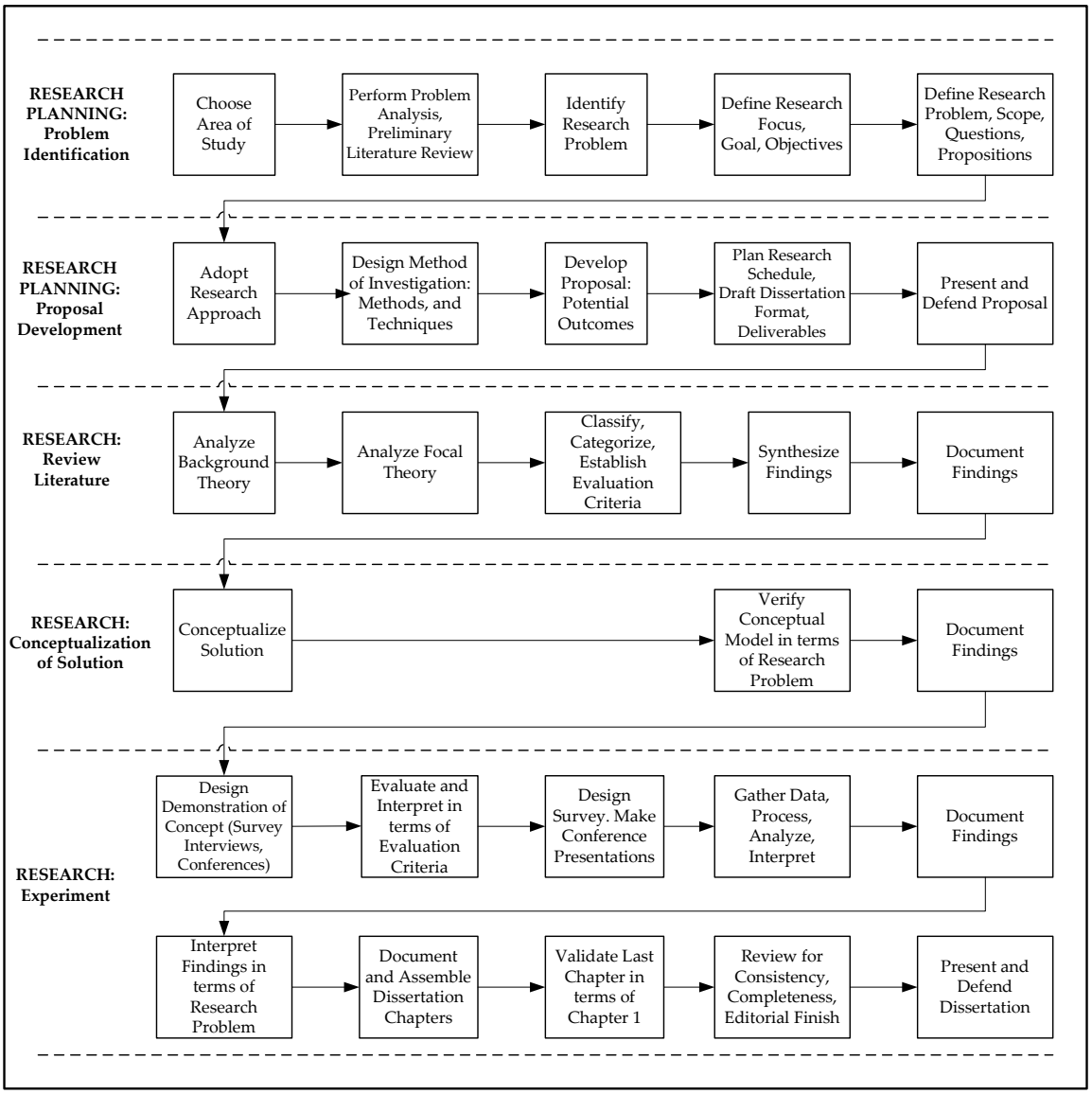
van der Haar, H., & von Solms, R. (2003), A model for deriving information security control attribute profiles, *Computers and Security*, Volume 22, Number 3, 233-244.

Vermeulen, C., & von Solms, R. (2002), The information security management toolbox – taking the pain out of security management, *Information Management and Computer Security*, Volume 10, Number 3, 119-125.

Yegidis, B. L. & Weinbach, R. W. (1996), *Research Methods for Social Workers*, 2nd. Edition, Allyn and Bacon, Boston, Massachusetts.

APPENDIX A

RESEARCH PROCESS MODEL

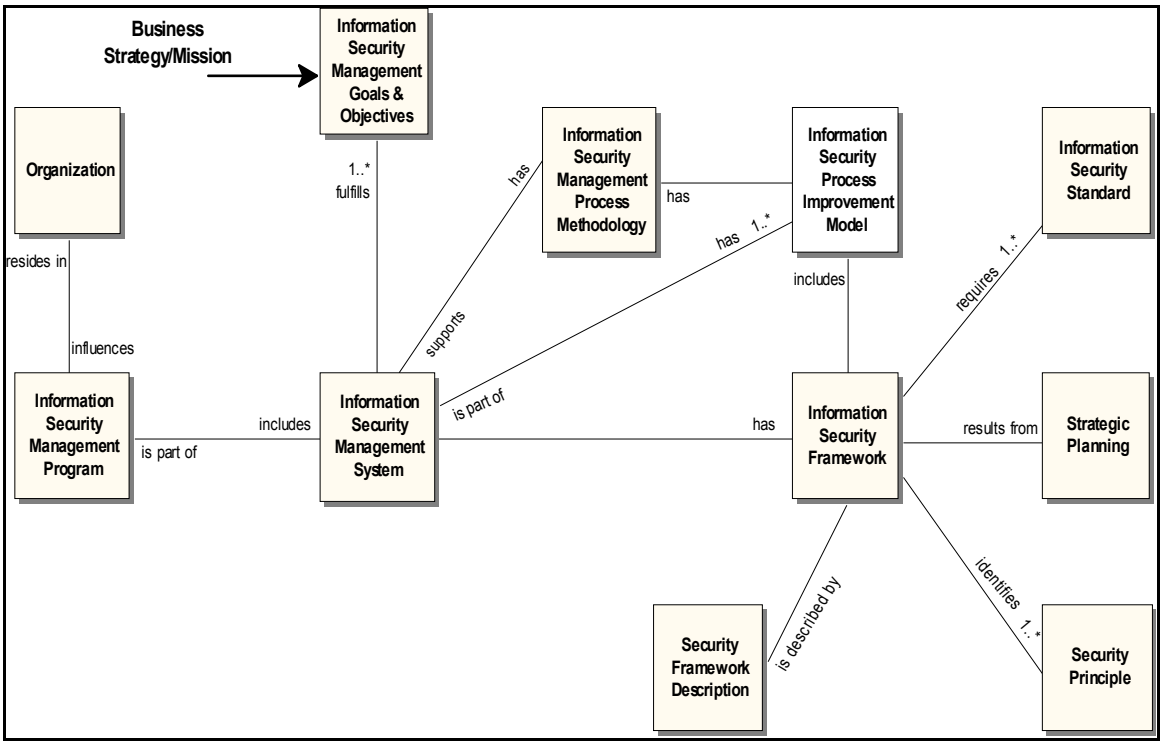


** Adapted from Steenkamp & McCord (2006)

The process model adopted for this research outlines the various activities, timelines, and expected deliverables at every stage of the research project. Deliverables, for each major research stage, are usually in the form of written reports. The final deliverable is the presentation and defense of the dissertation.

APPENDIX B

INFORMATION SECURITY MANAGEMENT PARTIAL META MODEL

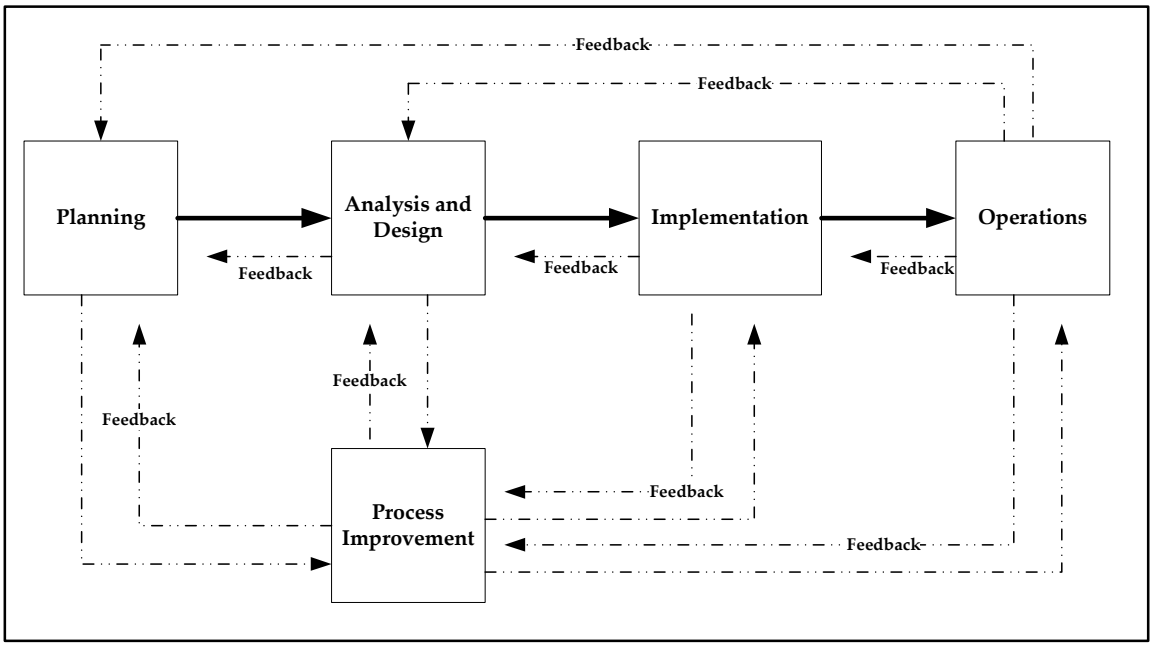


The meta primitives of the partial meta model for information security management are described as follows:

1. Enterprise business strategy and mission are fundamental inputs to the process of determining information security management goals and objectives.
2. The organization influences an information security management program within that organization. An information security management program resides in the organization, and includes an information security management system.
3. An information security management system is part of a security management program, and it fulfils information security management goals and objectives.
4. Information security management system has one or more information security process improvement models, an information security framework, and an information security management process methodology.
5. An information security framework results from strategic planning, requires one or more information security standards, and includes an information security process improvement model. Information security framework is also described by a security framework description, and it identifies one or more security principles.
6. An information security process improvement model is part of an information security management system, and has an information security management process methodology.

APPENDIX C

INFORMATION SECURITY MANAGEMENT PROCESS MODEL



The information security management process model is an iterative process. Feedback from one phase can be transmitted to preceding phase or phases, as necessary. This process iteration ensures that the information security management process model is an ongoing system that does not end with completion of specific information security management projects. The approach to managing information security should not be a point solution, i.e. it should be a continuum of activities, which provides ongoing maintenance and incremental improvements to the information security processes.

APPENDIX D

INFORMATION SECURITY MANAGEMENT PROCESS METHODOLOGY – PHASE ELEMENTS

PLANNING	ANALYSIS and DESIGN	IMPLEMENTATION	OPERATIONS
Business Systems	Business Systems Analysis	Business Systems	Business Systems Operations
Information Technology Strategic Plan	Information Security Architecture	Information Security Architecture	Information Security Architecture
Current Security Environment	Current Security Environment	Security Environment	Security Operations
Risk Management	Risk Management	Risk Management	Risk Management
Performance Management	Performance Management	Performance Management	Performance Management
Policy Development	Policy Analysis	Policy	Policy Administration
Human Factors	Human Factors	Human Factors	Human Factors Management
Technology	Technology	Technology	Technology Management
Security Education	Security Education	Security Education	Security education
Compliance	Compliance	Compliance	Compliance Management
Resource Management	Resource Management	Resource Management	Resource Management
Security Management Capability	Security Management Capability	Security Management Capability	Capability Maturity Management
Security Plan	Security Plan	Security Plan	Security Plan Administration

The element in each phase represents the step or stage in a particular phase where specific security management activity occurs. A phase element is the "what" security management activity that needs to be done, and "where" in the organizational structure that the activity should be done. Supporting method refers to the actual methodology of "how" things are done for the specific element. Supporting method is the action that must be taken to support accomplishment of stated objectives of the element or stage of the phase. Model is the tool to be used with each of the specified supporting method, towards achieving objectives of the element of the phase. Output is the deliverable from the specified supporting method of the various phase elements of the security management process model.

APPENDIX E

RESEARCH INTERVIEW DOCUMENT

Survey Questions Groups

A. Security Management Program

B. Security Governance

C. Risk Management

D. Security Policy

E. Security Management System

F. Infrastructure

G. Technology

H. Outcomes

Interviewee's Background Information

Position Title: _____

Portfolio Responsibility:

_____ Security _____ IT Planning

_____ IT Operations _____ Other Business Unit

Security Responsibility Level:

_____ Strategic _____ Tactical

_____ Strategic/Tactical _____ Tactical/Operational

Organization's Industry: _____

Major Products: _____

_____

Organization Size:

a). Employees: _____

b). Yearly Revenue: _____

Date of Survey Interview: _____

A. Security Management Program

1. Security and information security management has been evolving over the years in different forms and different industries. How has this evolution influenced your organization's approach to information security management?

2. Do you have a formal security management program in the organization? If so, what are the components of such program?

3. In planning any new security initiatives, what elements are taken into consideration to ensure that stated security goals are achieved, and security objectives are accomplished?

4. To what extent does your existing technology and related infrastructure influence security initiatives in the organization?

5. Is there a separate budget for security management? If there is, what is the approximate percentage of the security budget to your budget (IT, organization)?

6. What approximate percentage of your security budget is planned in advance, at least six months before the money is spent?

7. How is funding for security initiatives determined, and how is the allocation made?

8. What is the level of executive support for information security management?

9. How often does the Board, through a working committee, interact with security professions, or is the interaction strictly through senior management?

B. Security Governance

1. Some reference models and legislation dealing with corporate governance are CoBIT, COSO, Sarbanes-Oxley Act, HIPAA, IEEE Standards, etc. How has any or all of these influenced security management initiatives in your organization?
2. How is organization security strategy, goals and objectives developed?

3. What kinds of process (or processes) do you have for aligning tactical security issues to organization security strategy

4. To what extent do current security threats and vulnerabilities influence the development of organization security strategy?

5. How are security priorities determined?

6. How would you describe your organization's security management capability, using the capability maturity model (CMM) levels below?
   Level I: Initial (few stable processes)
   Level II: Repeatable (documented and stable processes)

Level II: Defined (integrated processes)
Level IV: Managed (stabilized and understood processes)
Level V: Optimized (continuous and systematic process improvements)

7. How do you monitor statutory compliance, i.e. to HIPAA, Sarbanes-Oxley, Graham-Leach-Bliley Act, etc., and security policy/standards compliance both internally and externally with partners and suppliers?

8. What role does corporate culture play in the management of information security in the organization?

C. Risk Management

1. How do you proactively manage risk through a security management strategy?

2. To what extent is risk management integrated with the security management function in the organization?

3. If and when you conduct security audits, what is the frequency and focus of such audits?

4. In developing mitigation strategies for security risk management, what motivators are used? Motivators could include economic incentives/consequences, reward/punishment, technology control, employee security training and awareness, policy enforcement, etc.
5. What processes do you have for identifying, measuring, and reporting security risks in the organization?

6. In identifying risk, how do you evaluate and prioritize security intelligence information?

7. How has the organization integrated security and risk management capabilities?

D. Security Policy

1. Do you have a written security policy that can be referenced by employees in the organization?

2. What are the major components of your security policy?

3. How are new security policies developed?

4. To what extent do relevant stakeholders participate in security management initiatives, at the strategic and tactical levels, e.g. in security policy development and enforcement, developing and delivering user training and awareness programs, etc?

5. What is the process for increasing employee security awareness and responsibility in the organization?

6. How do you manage and measure the impact of security-related incidents on the organization, e.g. security breaches?

7. Security planning:
   a) How is your security plan developed?
   b) What are the major components of the security plan?

8. To what extent is human behavior taken into account as an important factor in security policy development and enforcement?

E. Security Management System

1. What formal process do you use to manage information security?

2. How is the information security management function integrated into other enterprise business processes?

3. How many individuals are dedicated to the function of security management?

4. Of these personnel dedicated to security management, what is the focus of their official job description, i.e. strategic, tactical, and operational?

5. Regarding dedicated security personnel, what is the focus of the actual job tasks and activities performed, i.e. strategic, tactical, or operational tasks?

6. The organization uses various types of information from multiple sources, and provides information used as input to multiple actors and systems.
   a) How do you classify the different sources and uses of information?
   b) How do you manage the different classes of information once they are classified either by type, source, or use?

7. How are employees made to become willing participants in taking security management responsibilities?

8. What is the process for conducting background checks on individuals occupying critical positions in the organization?

9. What do you see as constraints on security management in the organization?

F. Infrastructure

1. In planning for disaster recovery, what is the process and method you use to develop a disaster recovery plan?

2. What mechanisms exist to deal with security threats and vulnerabilities to the infrastructure, i.e. technology, physical, applications, data, etc?

3. How do you identify infrastructure requirements necessary to bridge security gaps?

4. What administrative and technical controls are in place to ensure that infrastructure is adequately maintained for continuous and secure business operations?

5. How are unauthorized hardware, software, or unauthorized configuration changes in the infrastructure detected and removed?

6. What is the process for determining compatibility of infrastructure assets, and their conformity to established security standards?

G. Technology

1. Is using technology the only security management strategy used in the organization?

2. If so, what is the focus of the technology security management activity?

3. What are the most common security tools you use in managing security?

4. To secure data, whether in storage or during transmission, what process or tools do you use to ensure data security and integrity?

5. Have there been any recent security breaches in the last 12 months (no details)?

6. Do you rely more on security-specific technology to manage security? If so, what are the underlying reasons for using such strategy?

7. What roles do IPsec protocol, network firewalls, and security audits play in the overall management of information security in the organization?

8. What is the technology capability for detecting network intrusion and malicious codes?

H. Outcomes

1. In what ways are the deliverables of the security management function meeting the stated security goals and objectives?

2. What would be the characteristics of your desired;
    a. Security management environment?
    b. Security management program?
    c. Security management system?

3. How would you describe your overall satisfaction level of the current security environment?

4. What type of security process improvement model would you like to have that you do not have at present?