An Approach to Information Security Management

Anene L. Nnolim, Annette L. Steenkamp

College of Management
Lawrence Technological University

Abstract

This paper reports on part of a doctoral dissertation research project in information security management. The intent of this research is to attempt to determine how information security management could be enhanced as a structured and repeatable management process, and to develop an appropriate architectural framework and methodology that could enable integration of information security management with enterprise life cycle processes.

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. 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. This has motivated the focal area of this research in information security management. Part of meeting this new challenge could also include the resurrection of risk as an important component of information security management.

The results of this 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 well 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.

From the results of the research so far, the information security management viewpoint calls for a phased approach with iterative process models that include several elements, supporting methods and specific outputs. The viewpoint should also include an integrated process improvement model, with supporting methodology.

Currently, the main doctoral research is in the "demonstration of concept" stage. In this stage, the conceptual model will be validated in terms of the stated research problem. Potential outcomes and value of validation of the research proposition could be an approach to implementing an information security management system. This would include an

information security policy framework, a methodology, and a supporting process model that is regarded as essential to managing information security in the enterprise.

Key words: *Information security management, information security architecture, security policy, security process improvement, information security viewpoint, risk management.*

Evolution of Computer Security Strategies

Before computer security evolved into the many dimensional fields of today, the primary security focus of most organizations was in providing physical security to 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, it was inevitable that security objectives would eventually include computer security.

Up to the early 1980's when computers were used simply as business tools to automate business processes, the focus of computer security objective was securing computer centers since most computers were located in computer centers. The security strategy was mainly accomplished through physical security (Vermeulen and Von Solms, 2002). Up to the early 1990's as computers began to be used throughout the enterprise, the focus of security objective shifted to securing information technology (IT) systems and computer networks. The security strategy this time was accomplished through software that resided on IT systems (Vermeulen and Von Solms, 2002). From the early 2000's to the present, computers became components of IT systems that supported information as business assets. The focus of security objective was on securing business information systems, and this was accomplished through information security management (Vermeulen and Von Solms, 2002).

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. Securing business information systems also involves some risk. As a result, meeting this new challenge for security management would require that risk management be an important element in information security management. Achieving the objective of this new model requires comprehensive information security management strategies.

Purpose and Scope of the 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 architectural framework and methodology that could enable integration of information security management with enterprise life cycle processes.

The results of this 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 well 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.

This dissertation research project will be limited to examining the information security management viewpoint and related views. This includes the process and method for architectural descriptions for the information security management viewpoint, in the context of enterprise security domain. A review of other enterprise security viewpoints may be undertaken, to enable the presentation of research findings in the appropriate context.

Problem Statement and Research Question

The problem statement for this research is a lack of a comprehensive framework, supporting process model, and methodology that can enable the implementation and management of information security.

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

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

Research Design

The research approach followed is mixed methods. The strategy of inquiry 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 would allow for both text and statistical analyses of data, and would permit more flexibility when designing questions for possible interviews, i.e. both open- and close-ended questions (Creswell, 2003, p.17).

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

The proposed methods of investigation for this research are:

a) Continue the literature survey and perform a comprehensive analysis of literature on information security management.
b) Develop a conceptual model of a solution to the problems of inadequate information security management.
c) Demonstrate the conceptual model by means of an appropriate method, such as an example of how to apply the approach to developing an information security system for the organization.
d) Conduct in-depth structured interviews with senior executives in different industries, using a set of questions derived from the conceptual model. The interviews would be limited to senior executives responsible for information security management in their organization. This may include interviews with information security professionals.

Research Process

In the process model used for this research, the various activities, timelines, and expected deliverables are outlined. The major phases of the research process model are Research Planning (Problem identification, Proposal development), Research (Literature review, Conceptualization of solution), and Research Experiment (Demonstration of concept, Interpretation of findings, Presentation and defense of dissertation)

Research Validation Methodology

To validate the propositions for this research, it will be necessary to design a demonstration of the concept in the form of an example of how the approach might be implemented within an organization. Validation of the proposition will be done by means of criteria for evaluating validity, reliability, and generalizability of the approach. The results of the research project will be evaluated in terms of:

a) Whether they support or refute the research propositions,
b) Whether they provide the basis to confirm or reject the conceptual solution, and
c) Applicability of the demonstration-of-concept example to the conceptual solution.

Summary of Focal Theory

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, Glossary, p.8).

Various security viewpoints in the enterprise make up an enterprise composite security viewpoint. These are physical security, data security, information security, application security, and infrastructure security viewpoints. Each viewpoint has various additional views.

The concept of information security management in the enterprise may be viewed at three main levels, namely strategic, tactical, and operational. These levels correspond to the types of security issues that are of concern to management, including the general nature of expertise required to manage security, at that level (Belsis *et al*, 2005, p.193). The distinguishing factors between the domains are strategic (impacts corporate strategy), tactical (regarding the methodologies/practices used to manage security), and operations (installation and operation of security tools and measures) (Belsis *et al*, 2005, p.193). In other words, the motivators for security management are that it should be policy-driven (strategic level), guidelines-driven (tactical level), and measures-driven (operational level).

It would seem that majority of information security management activities in the past have been focused at the operational level, and very little attention was given to information security management as a continuum at all three-enterprise levels. 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).

It can be inferred, then, that information security management has not reached a maturity level that could make it a repeatable management process. This has motivated the focal area of this research, namely information security management in the enterprise.

Sample Literature Review

The literature review for the research was organized into themes. This facilitated the analysis of literature materials. Examples of these themes include architecture framework, governance, risk management, policy, and standards, etc. A sample of the literature review follows.

Eloff and Eloff (2003) proposed that organizations use a holistic approach to information security management, and establish an information security management system. This system would integrate policies, standards, guidelines, code-of-practice, technology, human issues, legal, and ethical issues. This means using a process model approach to manage information security. The authors propose "process security" and "product security" in information security management. In "process security", the focus would be on planning

and implementing management practices, procedures, and processes to establish and maintain information security. In "product security", the focus would be on the use of certified software products in the IT infrastructure in order to establish and maintain information security (Eloff and Eloff, 2003).

Doherty, N. F., and Fulford, H. (2006) discussed the aligning of information security policy with strategic information systems plan (SISP). It would seem that a broader strategy of aligning information security policy with corporate policy strategy might be better in the long run. The argument in support of aligning information security policy with SISP is that it would provide a framework to ensure that systems are developed with security built-in. However, if information security policy is aligned with corporate policy, the same systems development objective could still be accomplished.

To comply with security regulations of the Health Insurance Portability and Accountability Act (HIPAA) organizations are required to secure individual identifiable personal information (HIPAA, sub.F, Sec. 261). The security regulations identifies three safeguard standards that must be met by organizations covered under the Act, namely administrative safeguards, physical safeguards, and technical safeguards. Geffert (2004) observed that in the process of complying with this Act, organizations could end up with an effective enterprise risk management system (Geffert, 2004, p.21). On the other hand, Sarbanes-Oxley Act (2002) does not deal specifically with information security. However, the focus of the act is mostly on corporate governance, i.e. corporate accountability and responsibility of officers of the organization.

Botha, J., and von Solms, R. (2004) presented a theoretical model of business continuity planning methodology that could be generally applied to most businesses, as part of an information security management strategy. Out of the three information security fundamental principles of confidentiality, integrity, and availability, this study maintains that availability tends to assume greater importance than the other two principles in business continuity planning (Botha & von Solms 2004, p.329). Their theoretical model is a seven-phase planning methodology, namely project planning, business impact analysis, business continuity strategies, continuity strategies implementation, continuity training, continuity testing, and continuity plan maintenance (Botha & von Solms 2004, p.331-332). This is similar to that proposed by Heng (1996). However, before most organizations can use this methodology, they would need to first identify their specific organizational properties. These properties become variables in the organization's business continuity plan.

Gerber, M., and von Solms, R. (2001) attempted to determine the importance of risk analysis in identifying security controls, and whether there are other alternative approaches to risk analysis for accomplishing similar goals (Gerber & von Solms 2001, p.577). They identified several factors that influence an organization's security requirements. These are (a) business requirements for confidentiality, integrity, and integrity, (b) legal, statutory, or regulatory requirements, and (c) risks to the infrastructure. They argue that if the security requirements analysis determines the appropriate security controls, then this alternative analysis is called "security requirements analysis" (Gerber & von Solms 2001, p.582-583).

Stakeholder involvement is an important component of information security management. Tsohou, A., Karyda, M., and Kokolakis, S. (2006) examined the potential use of cultural theory as a tool for identifying patterns in stakeholders' perception of risk, and its effect on information system risk management. They maintain that awareness and training are not the only social factors that influence stakeholders' perception on security threats (Tsohou *et al,* 2006, p.198). The fundamental principle of cultural theory is that the way people socially interact encroaches on the systems of symbols they use to understand the world. The study uses this theory, as a foundation framework, to associate social context with information security risks and security management practices (Tsohou *et al,* 2006, p.207).

Human factors have always had some impact on information security programs in organizations. Besnard and Arief (2004) used a multidisciplinary approach to investigate some of the human factors in computer security. For example, a legitimate user may devise work-arounds if the security control measure that has recently been installed cannot provide good usability to the user. In some cases, legitimate users could unknowingly facilitate attacks from outside the organization. Ultimately, end user responsibility is a key component to improving user behavior in information security.

International Standards Organization/International Electrotechnical Commission (ISO/IEC) 17799 (2000) provides procedures and code of practice for information security management in the enterprise. It outlines a general framework that provides a common basis for developing enterprise security standards and effective security management practices. Other independent organizations that may be relevant to information security management include British Standards Institution (BS), Committee of Sponsoring Organizations (COSO) of the Treadway Commission, and International Federation for Information Processing (IFIP) Technical Committee 11.

Conceptualization of the Solution

The research is still in progress, and the dissertation has not been published. From the results of the research so far, the information security management viewpoint calls for a phased approach with iterative process models that include several elements, supporting methods and specific outputs. The viewpoint should also include an integrated process improvement model, with supporting methodology.

Other developments from the research include a meta model with detailed meta primitives, an architecture framework, a security governance structure, and a security management process model.

Demonstration of Concept

As the research progresses, part of the demonstration of concept stage will include conducting in-depth structured interviews with senior executives in different industries, using a set of questions derived from the conceptual model. The interviews will be limited to senior executives responsible for information security management in their organizations. This process may also include interviews with information security professionals.

Conclusion

The potential outcome and value of validation of the research proposition could be an approach to implement an information security management system. This approach would include an architectural framework and methodology, a security policy framework, and a supporting process model that could enable integration of information security management with enterprise life cycle processes.

References

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

Besnard, D., & Arief, B. (2004), Computer security impaired by legitimate users, Computers & Security, Volume 23, 253-264.

Botha, J., & von Solms, R. (2004), A cyclic approach to business continuity planning, Information Management & Computer Security, Volume 12, Number 4, 328-337.

Creswell, J. W. (2003), Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 2nd.Edition, Sage Publications, London.

Doherty, N. F., & Fulford, H. (2006), Aligning information security policy with the strategic information systems plan, Computers & Security, Volume 25, 55-63.

Heng, G. M. (1996), Developing a suitable business continuity planning methodology, Information Management & Computer Security, Volume 4, Number 2, 11-13.

Eloff, J., & Eloff, M. (2003), Information security management – a new paradigm, Proceedings of the 2003 annual research conference of the South African Institute of Computer Scientists and Information Technologists on enablement through technology SAICSIT, 130-136.

Geffert, B. T. (2004), Incorporating HIPAA security requirements into an enterprise security program, Information Systems Security, November/December, Volume 13, Issue 5, 21-28.

Gerber, M., & von Solms, R. (2001), From risk analysis to security requirements, Computers & Security, Volume 20, 577-584.

ISO/IEC 17799 (2000), Information Technology – Code of Practice for Information Security Management.

Sarbanes-Oxley (2002), Sarbanes-Oxley Act of 2002.

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.

The Open Group (2006), The Open Group Architecture Framework (TOGAF), Version 8.1, Enterprise Edition The Open Group, San Francisco.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, (2006), Formulating information systems risk management strategies through cultural theory, Information Management & Computer Security, Volume 14, Number 3, 198-217.

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.

Anene L. Nnolim

Anene is a Doctoral Candidate for the degree of Doctor of Management in Information Technology (DMIT) at Lawrence Technological University in Southfield, Michigan. He holds a bachelor's degree in business from State University of New York, Buffalo, and an

MBA from Stephen F. Austin State University, Nacogdoches, Texas. He has a Human Resources Management Certificate from University of Guelph in Ontario, Canada. He is a certified Project Management Professional (PMP).

Currently, he is the principal consultant at InfoTSG, Inc. (www.infotsg.com), an IT services consulting company with interests in business process management and information security management. His professional experience includes several years of management and leadership positions in government, telecommunications, and IT industries in Canada and U.S. He is an Adjunct Professor in business process management at Lawrence Technological University, and On-Line faculty at the University of Phoenix, teaching IT, management, and business courses.

Annette Lerine Steenkamp

Annette Lerine Steenkamp is Program Director of the Doctoral Program in Management of Information Technology and Professor in Computer and Information Systems in the College of Graduate Management at the Lawrence Technological University, Southfield, Michigan. She holds a PhD in Computer Science, with specialization in Software Engineering. Dr. Steenkamp's research interest is in approaches to information technology process improvement, enterprise architecture and knowledge management. Current research is concerned with the application of CMMI in the education sector, redesign of organization processes for mobile technology adoption, knowledge management frameworks, alignment of IT and organization strategies, and systems integration.