View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2019 Proceedings | Midwest (MWAIS)

5-21-2019

A Review of Information Systems Security Management: An Integrated Framework

Cindy Zhiling Tu
Northwest Missouri State University, cindytu@nwmissouri.edu

Joni Adkins
Northwest Missouri State University, jadkins@nwmissouri.edu

Gary Yu Zhao
Northwest Missouri State University, zhao@nwmissouri.edu

Follow this and additional works at: https://aisel.aisnet.org/mwais2019

Recommended Citation
Tu, Cindy Zhiling; Adkins, Joni; and Zhao, Gary Yu, "A Review of Information Systems Security Management: An Integrated Framework" (2019). *MWAIS 2019 Proceedings*. 15.
https://aisel.aisnet.org/mwais2019/15

This material is brought to you by the Midwest (MWAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in MWAIS 2019 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

A Review of Information Systems Security Management: An Integrated Framework

Cindy Zhiling Tu
Northwest Missouri State University
800 University Drive | Maryville, MO 64468
cindytu@nwmissouri.edu
816-752-6699

Joni Adkins
Northwest Missouri State University
800 University Drive | Maryville, MO 64468
jadkins@nwmissouri.edu
660-562-1803

Gary Yu Zhao
Northwest Missouri State University
800 University Drive | Maryville, MO 64468
zhao@nwmissouri.edu
660-541-5188

A Review of Information Systems Security Management: An Integrated Framework

Cindy Zhiling Tu
Northwest Missouri State University
cindytu@nwmissouri.edu

Joni Adkins
Northwest Missouri State University
jadkins@nwmissouri.edu

Gary Yu Zhao
Northwest Missouri State University
zhao@nwmissouri.edu

ABSTRACT

As information has been a basic commodity and strategic asset, information systems (IS) security has become increasingly important to organizations. This paper conducts a review on the prior literature that has studied non-technical factors of IS security issues from organizational perspective rather than individual level. Five key concepts are studied: IS security management, organizational factors, human factors, strategic planning, and IS security policies. By integrating the main concepts that are reflected in the literature, this paper proposes an integrated framework which provides a comprehensive look at effective IS security management. Four propositions are developed. This framework is intended to provide guidance for organizations and security practitioners that need to implement their IS security management effectively.

Keywords

IS security management, organizational factors, human factors, strategic planning, IS security policies, integrated framework

1. INTRODUCTION

Organizations are becoming more and more dependent on information systems (IS) to manage and access information resources so that they can survive and prosper (Van Niekerk and Von Solms 2010). Information has been a basic commodity and strategic asset which is vital to organizations. However, today information assets are facing increasing security breaches and IS security has become increasingly important to organizations.

Organizations have focused on technological factors which are thought to play the primary role in effective IS security solutions (Siponen 2005). However, recent research has recognized that human and organizational factors are also the key to the effectiveness of IS security controls (Kayworth and Whitten 2010; Soomro et al. 2016; Werlinger et al. 2009). Though non-technical factors are emphasized more and more in IS security research, they are seldom studied in an integrated framework. Moreover, most information security studies are conducted from individual level, trying to understand the impact of individuals' behaviors on IS security issues. Very few scholars have done research from the organizational level. There is lack of comprehensive integrated overview of the challenges faced by security practitioners.

As organizations need a systematic way to conduct effective IS security management, it is necessary to conduct a wide-ranging review of IS security management issues. The main research problems of this research are: (1) What is effective IS security management? (2) How to implement effective IS security management? This review tries to gain a deeper understanding of effective IS security management and provides an integrated framework for organizations to apply.

The rest of the paper is organized as follows. In the next section, we conduct a review of the literature on organizational IS security management. Then based on the review, we develop an integrated framework with propositions. Lastly, discussion and conclusion are presented, and implications are highlighted for future research and practice.

2. LITERATURE REVIEW

Scholars in different disciplines have developed an accumulated body of research, which addresses different aspects of the information security problems (Moody et al. 2018). The focus of this review is on the literature that has studied non-technical

factors of IS security issues from organizational perspective rather than individual level. We searched online scholarly databases with these key "information technology/IT", "information systems/IS", "security management", and "risk management". To be included in the sample, an article had to (1) study organizations' IS security problems, (2) address one or more non-technical factors, and (3) study from organizational level but not individual level.

In order to understand the effective IS security management, five key concepts are studied: IS security management, organizational factors, human factors, strategic planning, and IS security policies. The following sections describe each component of these concepts, summarize the existing literature, and highlight research gaps that provide opportunities for further research.

2.1 IS Security Management

IS security management is strategically important to organization's success (Kauspadiene et al. 2017). According to Van Niekerk and Von Solms (2010), the problem of managing information security is the management of many conflicts, such as conflict between business and security objectives, conflict between human behavior and security process, etc. Siponen and Oinas-Kukkonen (2007) define IS security management as "a means of maintaining secure IS in organizations, including IS planning and evaluation (p.62)". It also includes key management, creation of organizational security policies and guidelines, backup, recovery, contingency management, security checklist, and management standards (Moody et al. 2018; Safa et al. 2016). IS security management is conceptualized as a continuous dynamic decision-making process which involves all crucial components such as organizational infrastructure, human factors and information security practices (Ma et al. 2009).

Though some efforts have been made to figure out what effective IS security management is, there is lack of "big picture" of this issue. Researchers from different disciplines contribute very different views on IS security management, which lead to fragmentation in this field. Interdisciplinary research is needed to address IS security problems (Siponen and Oinas-Kukkonen 2007). Since the organizational level defines the organizational role and context of IS, IS security should consider organizational factors and human factors as well as technology issues (Siponen and Oinas-Kukkonen 2007). The goal of effective IS security management is to figure out organizational-level solutions to security problems in the organization's socio-organizational context (Kayworth and Whitten 2010).

2.2 Organizational Factors

Organizational factors are those related to the organization structure and managerial decisions around IT security (Werlinger et al. 2009). What have gained most attention are top management commitment and organization structuring.

Top Management Commitment. Top management is found very crucial to IS security management (Carcary et al. 2016; Kankanhalli et al. 2003; Kayworth and Whitten 2010; Ma et al. 2009; Straub and Collins 1990; Werlinger et al. 2009). Top management commitment can support IS security as an important enterprise-wide function in many ways, including funding, allocation of human and financial resources, promotion of buy-in, and stressing the importance of security to other groups within the organization (Kayworth and Whitten 2010). Moreover, top management plays the most important role on developing effective and efficient organizational structures (Straub 1988). Top management can be convinced about the importance of security by penetration testing, security vulnerability, and risk analysis reports (Werlinger et al. 2009).

Organizational Structuring. Organizational structuring is extremely important to IS security management (Boss et al. 2009; Kayworth and Whitten 2010; Straub and Collins 1990). Scholars advocate formal organizational structures for IS security management. Straub and Collins (1990) suggest that a high-level committee should be created to be responsible for setting policy and establishing specific procedures that reduce the IS security risk. Kayworth and Whitten (2010) propose a structure including an information security organization, a top security executive (the CISO), and an internal audit function. Such structure will help to facilitate the organizational integration to gain security goals and further address the importance of IS security at the organizational level.

2.3 Human Factors

Human factors are those related to individual cognition, culture and interaction with other people (Werlinger et al. 2009). Due to an inadequate level of user cooperation and a lack of knowledge, employees may misuse or misinterpret many security techniques and thus become the greatest threat to the organization's IS security (Van Niekerk and Von Solms 2010). An organization's IS security strategy should comprehensively address the human factors such as security culture and security training.

Organizationally sponsored security awareness, training, and education program is the primary formal social alignment mechanism to increase the overall awareness and understanding of IS security and thus, participation (Culnan et al. 2008; Kauspadiene et al. 2017; Kayworth and Whitten 2010; Ma et al. 2009; Siponen et al. 2009; Werlinger et al. 2009). The training

program is the primary way of communicating IS security policies, procedures, and requirements across the organization, because the proper rules of behavior for using the organization's information systems are explained by the training program effectively (Culnan et al. 2008). Ma et al. (2009) suggests a good training program which consists of courses, regular updates, collateral material such as posters and a system of rewards and penalties for desirable and undesirable behavior. Verbal persuasion, possible security breach examples (Siponen et al. 2009), IS security mentoring (Kayworth and Whitten 2010), and the process of designing security policies (Werlinger et al. 2009) can be used to train and educate stakeholders within organizations.

It is found by empirical studies that it is difficult to change employees' existing security practices if there is lack of IS security culture within organizations (Werlinger et al. 2009). Through establishing IS security culture, employees can become a security asset, instead of being a risk (Van Niekerk and Von Solms 2010). The underlying values about IS security must fit the values of the organization (Tang and Zhang 2016). If IS security programs do not mesh with the organizational culture, individuals may act inconsistently with IS security policies and standards (Kayworth and Whitten 2010).

2.4 Strategic Planning

IS security planning or strategy should be aligned with business objectives (Kayworth and Whitten 2010; Ma et al. 2009; Siponen and Oinas-Kukkonen 2007; Van Niekerk and Von Solms 2010). The lack of fit between the security objectives and the business objectives may lead to the fact that IS security policies and budgets do not reflect the needs of the business (Kayworth and Whitten 2010; Siponen and Oinas-Kukkonen 2007). In such case, investment decisions are driven by short-term priorities without well-conceived strategic priorities, and top management may pay little attention to IS security. The major challenge is to determine the balance between enabling the business and securing information assets (Kayworth and Whitten 2010). IS security strategic planning must be business driven, trying to achieve securing information assets and enabling the business simultaneously (Nazareth and Choi 2015).

An IS security strategic plan should put various best security practices together and shows how these practices can be used to cope with IS security threats (Siponen et al. 2009). With strategic planning of IS security, managers are aware of the full range of security controls available and implement the most effective controls. Straub and Welke (1998) propose the strategic planning process which can provide practitioners with guidelines to conduct IS security strategic planning.

2.5 IS Security Policies

Organizational security policies are examples of organizational-level solutions to security problems, such as countermeasures and strategies adopted to reduce systems risk (Safa et al. 2016; Siponen and Oinas-Kukkonen 2007). Based on General Deterrence Theory, Straub and his research partners categorize IS security policies into four distinct, sequential activities: deterrence, prevention, detection, and recovery (Straub 1990; Straub and Nance 1990; Straub and Welke 1998).

Deterrence. Deterrents are passive, administrative controls that restrict the use of system resources inactively (Straub and Nance 1990). Security guidelines and policy statements are examples.

Prevention. Preventives only admit authorized users to access the system. For instance, physical restraints such as locks on computer equipment room doors, and security software such as password protection (Straub 1990; Straub and Nance 1990).

Detection. Detection is "a proactive strategy that involves purposeful investigation of system activity to identify and follow up on possible irregularities (Straub and Nance 1990, p.46). Detection strategies include recording and tracking unusual activities to randomly scanning files, and exception reporting.

Recovery. Recovery policy is to remedy the harmful effects of an offensive act and to punish the offender(s). Organizations may impose internal sanctions to discipline offenders in the form of warnings, fine, reprimands, and termination of employment. They may report offenses to outside groups and take legal actions such as criminal and civil suits. Technical remedies, like software recovery facilities, are also included in this process (Straub and Nance 1990; Straub and Welke 1998).

3. AN INTEGRATED FRAMEWORK

We develop an integrated framework for effective IS Security management, by integrating the main concepts that are reflected in the literature (see Figure 1). This framework is composed of four main parts: environment, planning, action, and control.

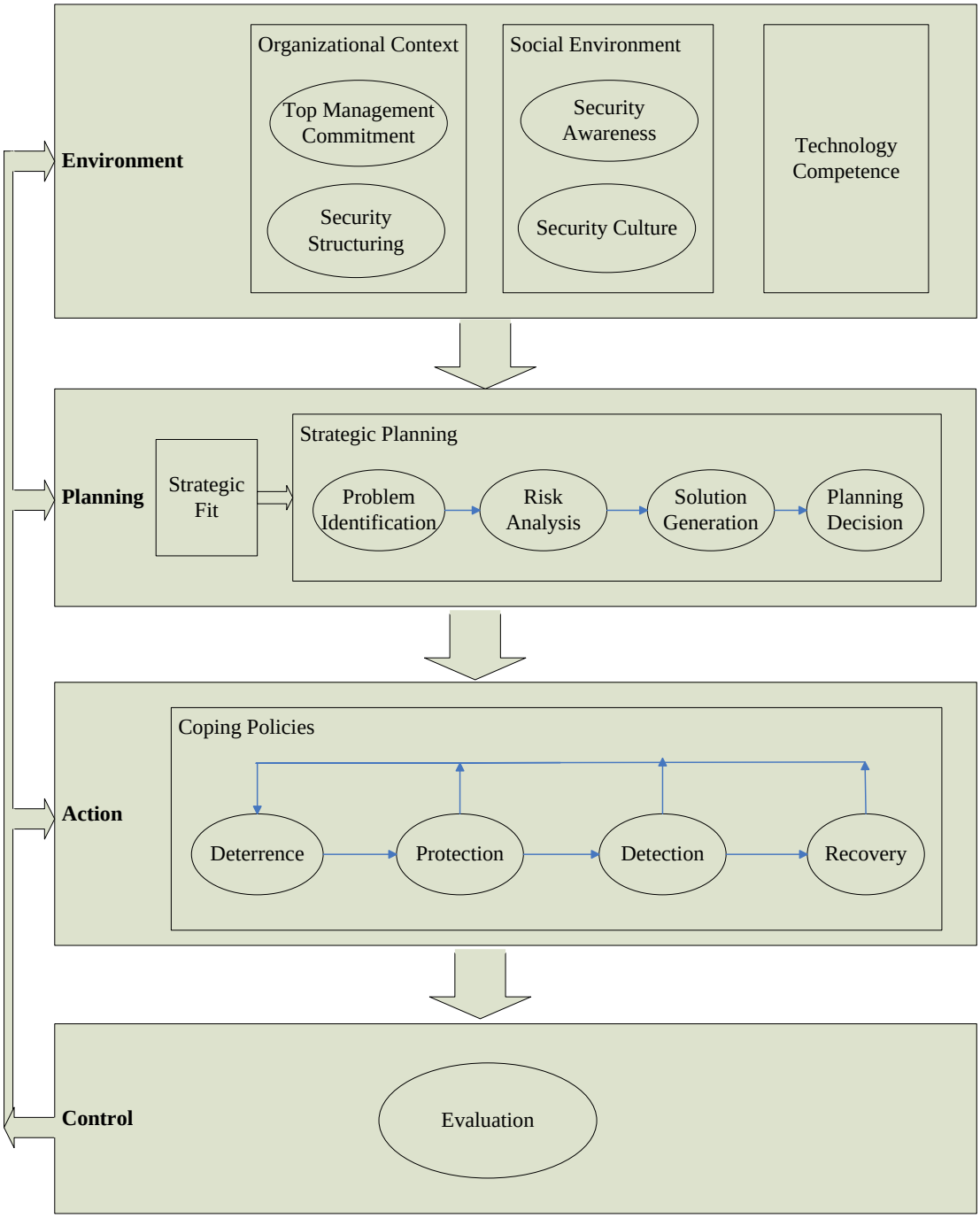

Figure 1. An Integrated Framework for Effective IS Security Management

3.1 Environment

The implementation of effective IS security management needs support from all kinds of environmental factors: organizational context which includes top management commitment and security structuring, social environment which includes security awareness and security culture, and technology competence. We propose that:

> *P1: A balanced socio-organizational-technological approach that includes organizational integration, social alignment and technological competence will facilitate the effective IS security strategy.*

3.2 Planning

An effective IS security strategy should be strategically focused or business driven and thus IS security is perceived as an important core business issue (Kayworth and Whitten 2010). Based on Straub and Welke's (1998) security risk planning model which guides the overall security planning effort, we can propose four phases for IS security planning process: problem identification, risk analysis, solution generation, and planning decision. Accordingly, we propose that:

> *P2: Strategic IS security planning which is aligned with business objectives will facilitate the implementation of effective IS security management.*

3.3 Action

Organizations need to establish policies or countermeasures and take them into effect to protect IS security. Drawn from General Deterrence Theory, Straub and Welke's (1998) security action cycle is integrated into this framework to present the effective actions for managing IS security. We therefore propose that:

> *P3: The IS security action cycle which cope with all kinds of security risks and threats will implement the effective IS security management.*

3.4 Control

In order to determine whether the IS security policies are meeting the goals, the organization needs to measure the progress of these policies (Ma et al. 2009). Evaluation is a control procedure, through which the return on investment can be figured out and the effectiveness and efficiency of the IS security management can be checked. The results of evaluation can influence environmental factors, strategic planning, and policies establishment. We propose that:

> *P4: Evaluation of the implementation of IS security management will increase the effectiveness of IS security management.*

4. DISCUSSION AND CONCLUSION

After reviewing prior literature on IS security management, this paper proposes an integrated framework which provides a comprehensive look at effective IS security management. Many variables are integrated in this framework and several propositions are developed. More research is needed to fully understand the complex system of IS security management. The propositions can be empirically examined in the future research.

This framework is intended to provide guidance for those organizations and security practitioners that need to implement their IS security management effectively. Firstly, organizations should use a balanced socio-organizational-technological approach, which includes organizational integration, social alignment and technological competence, to design the IS security management. Top management commitment and appropriate security structuring are necessary organizational support which can guarantee resources for IS security in the organization. Security awareness training make employees to be knowledgeable about IS security and to understand security policies better. A formal security culture and leadership of IS managers are important factors to constitute the social environment. The organizational context and social environment, complemented with technology competence, are basic preconditions for organizations to implement effective IS security management.

Secondly, strategic IS security planning which is aligned with business objectives should be conducted. To implement the IS security management successfully, a formal strategic planning process should be applied. Before the planning, IS managers need to analyze the internal and external conditions of the organization to align the objectives of IS security planning with the objectives of business. A four-phase planning process is suggested: problem identification, risk analysis, solution generation, and planning decision.

Thirdly, a comprehensive package of IS security policies should be established and appropriate actions should be taken to deal with various security threats or risks. Based on General Deterrence Theory, four types of coping actions can be taken in the whole security management procedure: deterrence, prevention, detection, and recovery.

Finally, effective IS security management needs a control mechanism. Evaluation of the security policies can be used to measure the performance of the management system. Feedback provided by evaluation to other factors can improve the progress of the whole system as well.

In closing, what is effective IS security management? Effective IS security management is a systematic process of effectively coping with information systems security threats and risks in an organization, through top management commitment, security structuring, security awareness training and education, creating security culture, applying competent technologies, strategic planning, establishing comprehensive security policies, and control, to protect information assets and achieve business goals.

REFERENCES

Boss, R. B., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18), pp. 151-164.

Carcary, M., Renaud, K., McLaughlin, S., and O'Brien, C. 2016. ". A Framework for Information Security Governance and Management," *IT Professional* (18:2), pp. 22-30.

Culnan, M. J., Foxman, E. R., and Ray, A. W. 2008. "Why It Executives Should Help Employees Secure Their Home Computers," *MIS Quarterly Executive* (7:1), pp. 49-56.

Kankanhalli, A., Teo, H. H., Tan, B. C., and Wei, K. K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp. 139-154.

Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S., and Ramanauskaite, S. 2017. "High-Level Self-Sustaining Information Security Management Framework," *Baltic Journal of Modern Computing* (5:1), p. 107.

Kayworth, T., and Whitten, D. 2010. "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Quarterly Executive* (9:3), pp. 163-175.

Ma, Q., Schmidt, M. B., and Pearson, J. M. 2009. "An Integrated Framework for Information Security Management," *Review of Business* (30:1), pp. 58-69.

Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1), pp. 285-A222.

Nazareth, D. L., and Choi, J. 2015. "A System Dynamics Model for Information Security Management," *Information & Management* (52:1), pp. 123-134.

Safa, N. S., Von Solms, R., and Furnell, S. 2016. "Information Security Policy Compliance Model in Organizations," *Computers & Security* (56), pp. 70-82.

Siponen, M., Mahmood, M. A., and Pahnila, S. 2009. "Are Employees Putting Your Company at Risk by Not Following Information Security Policies?," *Communications of the ACM* (52:12), pp. 145-147.

Siponen, M. T. 2005. "An Analysis of the Traditional Is Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14:3), pp. 303-315.

Siponen, M. T., and Oinas-Kukkonen, H. 2007. "A Review of Information Security Issues and Respective Research Contributions," *The DATA BASE for Advances in Information Systems* (38:1), pp. 60-80.

Soomro, Z. A., Shah, M. H., and Ahmed, J. 2016. "Information Security Management Needs More Holistic Approach: A Literature Review," *International Journal of Information Management* (36:2), pp. 215-225.

Straub, D. W. 1988. "Organizational Structuring of the Computer Security Function," *Computers & Security* (7:2), pp. 185-195.

Straub, D. W. 1990. "Effective Is Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Straub, D. W., and Collins, R. W. 1990. "Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy," *MIS Quarterly* (14:2), pp. 143-156.

Straub, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), pp. 45-60.

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22), pp. 441-470.

Tang, M., and Zhang, T. 2016. "The Impacts of Organizational Culture on Information Security Culture: A Case Study," *Information Technology and Management* (17:2), pp. 179-186.

Van Niekerk, J. F., and Von Solms, R. 2010. "Information Security Culture: A Management Perspective," *Computers & Security* (29:4), pp. 476-486.

Werlinger, R., Hawkey, K., and Beznosov, K. 2009. "An Integrated View of Human, Organizational, and Technological Challenges of It Security Management," *Information Management & Computer Security* (17:1), pp. 4-19.