Towards a Taxonomy of Information Security Management Practices in Organisations

Research in Progress

Moneer Alshaikh
Atif Ahmad
Sean B. Maynard
Shanton Chang
Department of Computing and Information Systems
Melbourne School of Engineering
University of Melbourne
Victoria, Australia
Email: atif@unimelb.edu.au

Abstract

*There is growing recognition of the role that management performs in protecting organisational information. However, our review of the academic and professional literatures did not find an empirically sound and coherent view of the range of management activities that can be applied as part of an information security program. As a result, organisations have insufficient guidance on what methods can be implemented to meet security objectives. Further, organisations have no empirically evidenced benchmark against which management practices can be assessed. This research project aims to develop a rigorous, comprehensive and empirically evidenced taxonomy of information security management practices (ISMPs) to provide organisations with comprehensive guidance. In this paper we report on the first phase of the development of the taxonomy. In this phase we conduct a comprehensive literature review to identify the range of ISMPs in the literature and suggest possible ways of classifying management level activity***.**

Keywords:

Information security; Information security management; information security management practice

INTRODUCTION

The threat of leakage of trade secrets and intellectual property, disruption of mission-critical systems, and malicious attack from both insiders and outsiders makes information security a high priority for organisations. Industry standards in the area of information security (e.g. ISO27000 series) suggest that organisations assess risk exposure in order to guide their selection of the particular managerial and technical security controls appropriate to achieving their information security objectives. Although technical security controls have always played a critical role in reducing security risk exposure, recent research has highlighted the critical role of managerial controls in the pursuit of security objectives (e.g. see Knapp & Ferrante 2012; Ahmad et al. 2012b; Lim et al. 2012).

A key outcome of our review of both academic and professional security literatures is the observation that it is increasingly critical for organisations to implement a range of security management activities (see the review and analysis section in this paper). We identified a large number of management activities towards achieving security objectives, for example: identifying security risks, developing security policies, and conducting security awareness training. In particular, the ISO27000 standards provides a long list of recommended activities although these are not backed by empirical evidence, nor is there a distinction between managerial and technical activities (the lack of empirical evidence is pointed out in (Siponen and Willison 2009). Our conclusion is that the academic and professional literatures do not provide an empirically sound and coherent view of the range of management activities that can be applied as part of a comprehensive information security program.

The consequences of inadequate managerial guidance on information security are significant for the modern organisation given the significant exposure to security threats. Organisations embarking on a program of information security management have insufficient guidance on what methods can be implemented to meet security objectives. Further, organisations have no widely accepted benchmark (backed by empirical evidence) against which improvement in existing management practices can be assessed.

Therefore, this research project aims to provide organisations with guidance on the range of activities that can be implemented as part of information security management. To provide *comprehensive* guidance this research project develops a taxonomy of management-level information security activities. Rather than using the term information security management *activity*, we use the term information security management *practice* (ISMP) to refer to individual management-level activities that organisations can implement to achieve information security objectives. The taxonomy provides a means for organisations to understand, implement and assess ISMPs in a systematic and comprehensive manner. For the preceding reasons, the research question in this study is:

What information security management practices should be implemented in organisations?

This research-in-progress paper reports the initial stages of the research project. It also presents the top level of the preliminary taxonomy.

This research-in-progress paper is organised as follows. First, the background to the study is discussed. Second, the research methodology is explained. Third, a review of information security management including the identification of key ISMPs areas is presented. Following this, a summary of the top level of the preliminary taxonomy of ISMPs is presented. Finally, we conclude the research in progress paper with a discussion of the main contribution and implication of the research.

BACKGROUND

Although a considerable amount of literature has been published in the last few decades on the managerial aspects of information security, the discussion has largely been focused on individual areas of practice such as risk, policy, incident response and SETA (security education training and awareness). One of the earliest studies in the literature suggests that the managerial aspects of information security are “largely diffuse and unorganised” (Madnick 1978). We argue that is still the case today.

A key indication of the immaturity in the discourse around information security management (ISM) is lack of a consensus on terminology used across the literature. For example, the terms ‘managerial control’ (Whitman 2010), formal and informal controls (Dhillon 2007), practice (Lim et al. 2012) and process (Purser, 2004) have been used to describe information security management activity. These terms are frequently not defined and are used by different authors to mean different things. For example, some authors (Guzman et al. 2010) use the term ‘security practices’ to refer to technical controls such as firewalls, while others (Lim et al. 2012) consider organisational factors such as top management support and budget allocation as security practices. In this paper, we see information security management as a process consisting of a number of practices. The term practice is used exclusively for managerial activities and does not therefore include tactical technical activities (although the management of technical activities is included).

A further indication of the immaturity in the discourse is the lack of agreement on the levels of granularity in management activities. For example, Choobineh et al. (2007) use ‘strategic’ and ‘operational’ levels of granularity whereas (Purser 2004) uses ‘strategic’ and ‘tactical’ levels. Additionally, information security management industry standards contribute to the confusion surrounding levels of granularity and usage of terminology. For instance, the ISO27002:2006 standard for the code of practice of information security management, is organized into eleven different sections (with no justification for this method of classification) each consisting of a range of recommendations without distinguishing between types of activities and controls (e.g. managerial-level and technical-level). Further, the standards are not based on empirical evidence and do not provide any justification for how the recommendations were identified (Siponen et al. 2009).

Since the early characterisation of Madnick (1978), there has been no significant increase in research activity addressing the need to develop a coherent and comprehensive view of ISM practices. In essence, this points to the lack of a theoretical framework and conceptualisation of ISM implementation as discussed by Choobineh et al. (2007). Lim et al. (2012) reinforce this point, stating that although a number of studies do cover individual security ISMPs, none provide a comprehensive overview of these practices. A study by Ma et al. (2008) recognises the need for a comprehensive list of ISMPs and attempts to address this need. However, their ISMP framework has a number of issues. First, the framework does not distinguish between managerial and technical practices. For example, one of the ISM practices in the proposed framework is installing virus protection software, which is clearly not a management practice. Second, the framework does not distinguish between various levels of granularity (e.g. strategic, tactical and operational) of management-level activity. Finally, the ISMPs in their framework have been taken exclusively from the ISO 17799 standard and have not considered either the academic or professional literature.

From the above discussion, we argue that there is a need to identify, classify and understand the management practices of information security. Therefore, in this paper we define a taxonomy of ISMPs. The taxonomy aims to give organisations a means to understand, implement and assess ISMPs in a systematic and comprehensive manner in order to enable them to protect themselves from a wide range of threats.

RESEARCH APPROACH

The aim of this research is to classify and organize the various kinds of management activities in information security to provide comprehensive guidance to organisations for the purpose of implementation and assessment. This research uses a taxonomy for classification, which is a formal classification approach (Chrisman et al. 1988). Chrisman et al. (1988) assert that classification systems are developed for four possible reasons: (1) differentiation, (2) generalisation, (3) identification, and (4) information retrieval. In this project we aim to achieve the third objective of the classification, 'identification', which is the identification of information security management practices.

Due to the explorative nature of this study, the research project follows a qualitative research design. The intent is to develop the taxonomy in four stages. First, we conduct a comprehensive literature review. The aim of the review is to identify the range of ISMPs in the literature and to suggest possible ways of classifying management level activity towards the development of a preliminary taxonomy. This is reported on in this research-in-progress paper. Second, a set of interviews with security management experts from both industry and academia will be conducted with the aim of inviting comment on the preliminary taxonomy for the purpose of refinement. Third, a set of case studies in at least three Australian organisations that comply with industry standards will be conducted to examine the implementation of ISM. The aim of the case studies is to assess the implementation of ISM against the taxonomy. Finally, a set of focus groups with security experts (both academic and professional) will be used to perform the final validation and refinement of the taxonomy.

From a theoretical perspective, the particular kind of classification in this project falls under the Type I: Analytic theory. Gregor (2006) describes analytic theory as the most basic type of theory where the objective is to "…describe or classify specific dimensions or characteristics of individuals, groups, situations, or events by summarizing the commonalities found in discrete observations" (Gregor 2006). Analytic theory seeks to answer, the "what is" research question as opposed to explaining causality or attempting predictive generalisations, which is the main feature of the approach. This research project seeks to answer the "what is" question by describing information security management level activity identified in the literature and classifying it using the taxonomy. Thus, in terms of Information Systems theories, the analytic theory is the most appropriate theory to describe this research project.

There are different views on whether taxonomies are theories or typologies. For example Weber (2012) believes "that type I theories: analytical theories are topologies and not theories" (p. 5). However, authors such as (Doty and Glick 1994; Mckelvey 1982) regard taxonomies as theory. Doty and Glick (1994) argue that "When typologies are properly developed and fully specified, they are complex theories that can be subject to rigorous empirical testing." (p. 230). In addition, McKelvey (1982) classifies research into two types: "systematic" and "functional science". Our research fits into the first type as it develops a theory of the distinctions between the different practices of information security management in organisations: in the form of a taxonomy.

In order to provide theoretical rigor in developing the ISMPs model, the taxonomy, once completed, will be evaluated against the characteristics of analytic theory proposed by Gregor (2006). These characteristics or qualities of good analytic theory are: (1) model completeness, (2) model parsimony, and (3) mutual exclusivity

A REVIEW AND ANALYSIS OF THE INFORMATION SECURITY MANAGEMENT ACTIVITIES IN THE LITERATURE

We conducted a comprehensive and rigorous review of the information security literature focusing on two sources: 1) papers published in both the academic and professional literatures, and 2) textbooks (both title and content area) on the topic of information security management. For both academic and professional literature, we used the following keywords to search SpringerLink, IEEE Xplore, ScienceDirect, the ACM digital library, ProQuest and Google Scholar: 'information security', 'information systems security', information technology security', 'information security management', 'cyber security', 'information assurance', 'information security practices', 'information security management practices' and 'security practices'. The preliminary results consisted of 496 scholarly articles, industry standards, and technical reports. A review of abstracts resulted in the elimination of 212 papers that were not related to ISMPs, leaving 284 ISMP related papers.

We identified, using the google search engine, 192 textbooks of which the majority took a technical view of information security, and did not deal with managerial activities. However, significant in the minority of management-oriented textbooks were Whitman & Mattord (2010) "Management of Information Security" and Whitman & Mattord (2011a) "Principles of Information Security", as well as Dhillon (2001) "Information

Security Management: Global Challenges in the New Millennium" and Raggad (2010) "Information Security Management : Concepts and Practice".

Content analysis was used to decide which articles contribute significantly to the field of ISM. An open coding process was followed to categorise the contents thematically. Inter-rater reliability was achieved through Creswell (2013) process of coding, debate and discussion on the agreed themes between researchers. During the analysis of the papers, any management-level activity that organisations could implement to achieve information security objectives was determined to be an ISMP. This produced a large number of ISMP's. As the analysis continued, the ISMP's were grouped with guidance from the textbooks for categorisation purposes. This resulted in an imbalance of ISMP's within each category – with a high number in categories in which there is much research (e.g. policy and risk management) and fewer in categories where there is less research (e.g. intra-organisational liaison). This reinforces the view of Lim et al (2012) and Choobineh et al. (2007) who state that the focus of papers tends to be on individual ISMPs rather than on the provision of a rigorous collection of practices.

The management textbooks provided two distinct contributions that allowed us to categorize the ISMPs. From Whitman and Mattord (2010) we learnt that since information security is implemented through a process of institutionalisation, ISMPs can be categorized in terms of the particular phase in the process lifecycle (e.g. develop, implement & maintain, evaluate). The second contribution was a useful categorization of the topic areas in information security management that align with our definition of management practices (examples include: Information Security Risk Management, Information Security Policy, and Incident Response).

Whitman & Mattord (2010) point out that information security in general can only be implemented through a process of institutionalisation. They propose a security system development lifecycle (SecSDLC) consisting of six phases (Investigation, Analysis, Logical Design, Physical Design, Implementation, and Maintenance and Change) designed to implement an information security project in an organisation. The SecSDLC lifecycle engages in an analysis of the full-spectrum of controls (managerial and technical) already in place in an organisation before engaging in the design of a new blueprint that is ultimately implemented to achieve new security objectives.

Unlike the SecSDLC lifecycle, which adopts a project-oriented view of the full spectrum of security controls, this project takes a process-oriented view within the narrow scope of information security management with the aim of developing a taxonomy of practices (rather than a method for implementation). However, the concept of institutionalisation applies to implementation of managerial practices as much as it does to security systems. Since the process-view does not consider project implementation, we propose the project-specific stages of investigation, analysis, logical design and physical design be replaced with the proposition that management functions in general undergo 'development'. Since management functions must be implemented in the organisation, 'implementation' and 'maintenance' are relevant to the process-view as well. Whitman and Mattord (2010) suggest that information security measures must 'change' to adapt to the security environment. From a process point of view this concept has been incorporated in the notion of 'evaluation' which focuses on the need for feedback and improvement of management functions. There is support for this kind of categorization in academic literature. Some academic papers (e.g. Rees et al. 2003) discuss practices related to the development of security policy whereas others (e.g. Gaunt 1998) have focused on the practices related to implementation of security policy. Still others (e.g. Whitman 2008) discuss the importance of evaluating security policy to ensure its effectiveness.

Therefore, we propose that institutionalisation of information security management takes place in distinct stages. The process must be: 1) developed, 2) implemented and maintained in the organisation. Further, the process must undergo 3) evaluation for the purpose of feedback and improvement. These three institutionalisation stages provide structure for our taxonomy. As per the previous example, the academic literature related to particular ISMPs tends to make these distinctions as well.

Regarding the problem of categorizing the areas of practice, we synthesized the various perspectives of the textbooks to help us in the analysis process which lead to five key categories: security policy, security risk management, security incident response, security education, training and awareness, and technical management (i.e. management of technical controls). The analysis also identified a sixth category that was not apparent in the textbooks which we have named "intra-organisational liaison". Intra-organisation liaison activities include the communication, collaboration and coordination with other management functions such as human resources, audit and finance. The "intra-organisation liaison" term has been used in industry standards such as NIST (Swanson et al. 1996) in a similar vein. Table 1 summarises ISMPs areas. These areas are discussed in the remaining of this section.

Security Policy Management

ISM and information security literature in general discuss security policy and the importance of providing organisations with management guidelines and directions for information security (Knapp et al. 2009; Ruighaver et al. 2010). Policy is an essential element of an effective ISM program (Rees et al. 2003). Rees et al. (2003) proposed a framework of security policy that includes administering a security policy during the development, implementation and evaluation processes. Each of these security policy management processes includes a number of practices undertaken by an organisation's security managers. Examples of these practices include forming a policy development team, assessing the current security policy and identifying the organisation's security requirements to establish a security policy (; Rees et al. 2003; Whitman 2008; Whitman & Mattord 2010).

Table 1: Summary of Literature Review of ISMPs

ISMPs Areas	Representative References
Security policy management	Gaunt (1998); Karyda et al. (2005); Knapp et al. (2009); Rees et al. (2003); Whitman (2008); Whitman & Mattord (2010, 2011a, 2011b)
Security risk management	Finne (2000); Gerber & von Solms (2005); Shedden et al. 2010; Stoneburner et al. 2002; Tsoumas & Tryfonas (2004); Zafar et al. (2014)
Security incident response management	Grance et al. (2004); ISO/IEC18044 (2006); Northcutt (2003); Shedden et al. (2011); Tan et al. (2003)
Security education, training and awareness management	Tsohou et al. (2008); Tsohou et al. (2010b); Waly et al. (2012); Whitman (2008); Whitman & Mattord (2010, 2011a, 2011b); Wilson & Hash (2003)
Technical management	Rees et al. (2003); Tsohou et al. (2010a)
Intra-organisation liaison management	Lim et al. (2010); Lim et al. (2012); Purser (2004); von Solms (1996); Whitman & Mattord (2011b);

Security Risk Management

ISO/IEC27005 (2012:2012) defines risk management as "coordinated activities to direct and control an organisation with regard to risk" (p. 8) and describes the risk management process as 'a continuous process for systematically identifying, analysing, treating, and monitoring risk throughout the life cycle of a product or service' (p. 8). Risk management consists of four main processes: risk assessment, risk treatment, risk acceptance and risk communication (Stoneburner et al. 2002). Each of these risk management processes has a set of practices that should be performed to ensure the protection of organisations (Finne 2000; Gerber et al. 2005; Shedden et al. 2010). For example conducting risk assessment includes identifying threats and vulnerability in organisational information systems, determining the risk to organisational assets, and analysing risk. Information security managers have the key responsibility of managing information security risk in an organisation by doing risk management practices (Stoneburner et al. 2002; Whitman & Mattord 2010).

Security incident response management

Regardless of the information security controls that organisations implement, the elimination of security incidents cannot be guaranteed. Recent security reports have shown an increase in the number of security incidents, both internal and external (Baker et al. 2013; Richardson 2010). Therefore, incident response management is critical to ISM (Grance et al. 2004; ISO/IEC18044 2006). It aims to effectively manage the response to security incidents to minimise their impact and protect organisations. Ahmad et al. (2012a) state that the response process consists of five main practices, namely "preparation for, identification, containment, eradication and recovery from incidents" (p. 643). Appropriate and effective incident management is important to reduce the impact of threats and maintain business continuity. Security managers should lead and manage the incident response process and have adequate skills and knowledge to manage incident response teams (Werlinger et al. 2010).

Security education, training and awareness management

Security education, training and awareness programs have a significant role in protecting the organisation's assets (Nosworthy 2000; Tsohou et al. 2008). SETA enables employees to comply with information security policy and procedures (Puhakainen et al. 2010; Wilson & Hash 2003). A significant proportion of security incidents are caused by employees' lack of awareness, which leads to the misuse or misinterpretation of technology or procedures. Thus, SETA management is a crucial part of ISMPs (Tsohou et al. 2010b). SETA management includes practices such as managing the design and implementation of these programs and assessing their outcome (Wilson & Hash 2003). Whitman (2003) suggests that one of the practices "that should be developed early is the design and implementation of an employee security education, training, and awareness program" (p95). SETA programs should be effectively designed and conducted to positively influence employee's behaviour towards information security. People are an important element in protecting an organisation's security; therefore, they should be appropriately trained and educated about security issues. SETA management involves the active promotion of SETA programs as a part of ISM systems (Spurling 1995).

Technical management

Due to the fact that security has traditionally been perceived as a technical problem, there is considerable research on operational level activities in regard to technical security controls, such as installing and configuring firewall systems (Whitman & Mattord 2010). Our review of the literature revealed that little focus has been given to the managerial activities regarding technical controls (strategic level activities). Ma et al. (2008) argue that the effective implementation of technical controls of an information security system depends on how well these controls have been managed. Therefore our focus is on the managerial activities required for technical controls. These activities involve practices such as the selection of appropriate technical controls and the establishment of rules and requirements for these controls. It also includes assigning the role and responsibility of maintaining meaningful documentations of technical controls (Rees et al. 2003; Tsohou et al. 2010a).

Intra-organisation liaison management

The role of intra-organisation liaison management can be articulated in three words: communication, collaboration and coordination (Savola et al. 2006). It involves two-way communication between security managers and the rest of the organisation. Having security managers communicating to the rest of the organisation is an important practice as it aims to convince top management and other departments such as human resources and finance about the importance of information security in helping the organisation achieve its business objectives and sustain a competitive advantage (Purser 2004). Having communication from the rest of the organisation (including the top management) to the security manager is important to ensure that business requirements, management directions and procedures are considered with respect to information security (Tu et al. 2014). If these communication channels are well established and maintained, security will be recognised as an important element of the organisation and will not be seen as a burden on the organisation's budget. Furthermore, the organisation will cultivate a security culture in which every employee will recognise the importance of information security and will act accordingly, resulting in the improved security of the organisation (Lim et al. 2010). We contend that security managers are the central point of this communication and that communication should be an integral part of their responsibilities. Successful intra-organisation liaison management should result in the attainment of top management support, the justification of budget and resource allocation, the assignment of roles and responsibilities and the recognition of the necessity of security functions (Lim et al. 2012; Savola et al. 2006).

PROPOSED TAXONOMY

As a result of our analysis of the academic and professional literatures, along with our use of textbooks to guide our analysis we have developed a preliminary taxonomy. Table 2 shows a summary of the top level of the preliminary taxonomy with some examples of the lower level practices that expected to appear.

The taxonomy identifies 6 areas of management practice. Within each area, the stages of institutionalisation are listed and, due to space constraints, a representative management practice is shown for illustrative purposes. In the literature analysis we identified two deficiencies: first, the literature doesn't distinguish between managerial and technical practices, and second, it doesn't distinguish between various levels of granularity. In our taxonomy we are only focusing on managerial security practices and by identifying these we are helping to address the first deficiency. This initial work is the first step towards this.

The second deficiency will be addressed in the next stage of the research, where we will extend the proposed taxonomy to distinguish between practices that are strategic, tactical or operational. This will be done within each of the institutionalisation stages, and will provide a third level to the taxonomy, prior to identifying the management practices.

The taxonomy is an important step in the maturity of information security management practice in organisations. It will allow organisations to implement a program of information security management with sufficient guidance in order to meet their security objectives. Organisations will be able to use the taxonomy as a guide to the practices that are required within each practice area, and will be able to self-select practices to be followed depending on the organisation's security requirements. They may also determine whether some of these security practices could be outsourced, depending on a variety of factors, including organisation size, the organisations risk propensity and their in-house expertise. The taxonomy will be able to be further used by organisations as a benchmarking tool against which improvement in existing management practices can be assessed.

Table 2: A summary of the top level of the preliminary taxonomy

Practice Area	Institutionalisation Stage	Representative examples of practices
Security Policy	Develop	Assess existing organisational policies (Rees et al. 2003)
	Implement & Maintain	Distribute policy (Whitman & Mattord 2010)
	Evaluate	Review policy periodically (Knapp et al. 2009).
Security Risk management	Develop	Develop risk management plan (NIST 2011)
	Implement & Maintain	Conduct risk assessment (Humphreys 2008)
	Evaluate	Review risk management plan (Stoneburner et al. 2002)
Security incident response	Develop	Form incident response team (Ahmad et al. 2012a)
	Implement & Maintain	Deploy the incident response team (Mitropoulos et al. 2006)
	Evaluate	Review security incident response plan (Grance et al. 2004)
Security education, training and awareness	Develop	Conduct a SETA needs Assessment (Wilson & Hash 2003)
	Implement & Maintain	Conduct SETA program using available delivery techniques (Whitman & Mattord 2010)
	Evaluate	Review SETA programs periodically (Wilson & Hash 2003)
Technical management	Develop	Identify security controls (Swanson et al. 1996)
	Implement & Maintain	Implement selected controls (NIST 2007)
	Evaluate	Review the implementation plan (Bowen et al. 2006)
Intra-organisation liaison management	Develop	Develop a communication plan (Savola et al. 2006)
	Implement & Maintain	Implement communication plan (Anttila et al. 2004)
	Evaluate	Review communication plan (Savola et al. 2006)

CONCLUSION & FUTURE RESEARCH

This research-in-progress paper has discussed the first phase of the development of a taxonomy of ISMPs for organisations. a summary of the top level of the preliminary taxonomy was presented which consists of six areas of management practice. Institutionalisation stages are identified and example practices are listed within each area of management practice. We argue that the pursuit of security objectives necessarily requires organisations to implement a selection of the kinds of ISMPs represented in Table 2.

This research will have several important implications for practitioners and researchers. For ISM practitioners, the proposed taxonomy provides comprehensive guidance on information security management practices that can be implemented and what activities can be performed to deliver effective security management. Additionally practitioners will be able to benchmark their information security management activities against the taxonomy.

ISM researchers can map existing ISM research activity to the taxonomy (i.e. the ISMP areas as well as the individual ISMPs) to identify fertile areas for future research. The taxonomy provides valuable into what ISMPs may exist in organisations, which is useful for all practice-based research. In particular, since ISMPs collectively contribute to the success of a security management program, research findings in one area of practice can be related to other areas of practice. The taxonomy provides an exhaustive list of practice areas and practices that can be used by researchers for comprehensive systematic analysis.

The development of phase one of the taxonomy addresses one of the two deficiencies identified in the literature: the literature doesn't distinguish between managerial and technical practices. As the taxonomy is about managerial practices, it identifies from the numerous ISMPs found in the literature which ones are managerial, and thus by omission which ones are technical.

The taxonomy produced in this first phase of the research project provides a sound basis for further work. In the next stage of taxonomy development the second deficiency will be addressed. We intend to extend the proposed taxonomy to distinguish between practices that are strategic, tactical or operational. This will be done within each of the institutionalisation stages, and will provide a third level to the taxonomy, prior to identifying the management practices. Subsequent to this, we will empirically refine and validate the taxonomy using, in turn, a set of expert interviews, a set of case studies within Australian organisations and finally a set of focus groups. The expert interviews will be conducted to gain comment on the taxonomy for the purpose of refinement. The case studies will allow the assessment of ISMP implementation against the taxonomy. Finally, the focus groups will perform the final validation of the taxonomy.

REFERENCES

Ahmad, A., Hadgkiss, J., and Ruighaver, A. B. "Incident response teams – Challenges in supporting the organisational security function," Computers & Security (31:5) 2012a, pp 643-652.

Ahmad, A., Maynard, S., and Park, S. "Information security strategies: towards an organizational multi-strategy perspective," Journal of Intelligent Manufacturing), 2012/07/22 2012b, pp 1-14.

Anttila, J., Kajava, J., and Varonen, R. 2004. "Balanced Integration of Information Security into Business Management," Euromicro Conference, 2004. Proceedings. 30th, pp. 558-564.

Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C., Ostertag, D., Porter, C., Rosen, M., and Sartin, B. "2013 Data Breach Investigations Report," in: United States Secret Service, 2013.

Bowen, P., Hash, J., and Wilson, M. "SP 800-100. Information Security Handbook: A Guide for Managers,") 2006.

Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J. "Management of Information Security: Challenges and Research Directions," Communications of the Association for Information Systems (20) 2007, pp 958-971.

Chrisman, J. J., Hofer, C. W., and Boulton, W. B. "Toward a System for Classifying Business Strategies," Academy of Management Review (13:3) 1988, pp 413-428.

Creswell, J.W. 2013. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage.

Dhillon, G. Information security management : global challenges in the new millennium Idea Group Pub, Hershey, Pa. ; London, 2001, pp. ii, 184 p.

Dhillon, G. Principles of Information Systems Security: text and cases Wiley New York, 2007.

Doty, D.H., and Glick, W.H. 1994. "Typologies as a Unique Form of Theory Building: Toward Improved Understanding and Modeling," *The Academy of Management Review* (19:2), pp. 230-251.

Finne, T. "Information Systems Risk Management: Key Concepts and Business Processes," Computers & Security (19:3) 2000, pp 234-242.

Gaunt, N. "Installing an appropriate information security policy," International Journal of Medical Informatics (49:1) 1998, pp 131-134.

Gerber, M., and von Solms, R. "Management of risk in the information age," Computers & Security (24:1) 2005, pp 16-30.

Grance, T., Kent, K., and Kim, B. "Computer security incident handling guide," pp. 800-861.

Gregor, S. "The nature of theory in information systems," Mis Quarterly) 2006, pp 611-642.

Guzman, I. R., Galvez, S. M., Stanton, J. M., and Stam, K. R. "Information Security Practices in Latin America: The case of Bolivia,") 2010.

Humphreys, E. "Information security management standards: Compliance, governance and risk management," Information Security Technical Report (13:4) 2008, pp 247-255.

ISO/IEC18044, A. N. "Information technology-security techniques-information security incident management ", 2006.

ISO/IEC27005 "Australian/New Zealand Standard: Information technology - Security Techniques- Information security risk management ", 2012.

Karyda, M., Kiountouzis, E., and Kokolakis, S. "Information systems security policies: a contextual perspective," Computers & Security (24:3) 2005, pp 246-260.

Knapp, K. J., Franklin Morris Jr, R., Marshall, T. E., and Byrd, T. A. "Information security policy: An organizational-level process model," Computers & Security (28:7), 10// 2009, pp 493-508.

Knapp, Kenneth J., and Claudia J. Ferrante. "Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations." Journal of Management 13.5 (2012): 67.

Lim, J.S., Chang, S., Ahmad, A., and Maynard, S.B. "Towards an Organizational Culture Framework for Information Security Practices," in: Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions, IGI Global, 2012, pp. 296-315.

Lim, J.S., Ahmad, A., Chang, S., Maynard, S.B.: Embedding information security culture emerging concerns and challenges. In: Pacific Asia Conference on Information Systems, PACIS 2010, Taipei, Taiwan (July 2010)

Madnick, S. E. "Management policies and procedures needed for effective computer security," Sloan Manage Rev (20:1), Fall 1978, pp 61-74.

McKelvey, B. 1982. *Organizational Systematics--Taxonomy, Evolution, Classification*. Univ of California Press.

Mitropoulos, S., Patsos, D., and Douligeris, C. "On Incident Handling and Response: A state-of-the-art approach," Computers & Security (25:5), 7// 2006, pp 351-370.

NIST "800-53 Recommended Security Controls for Federal Information Systems and Organizations," pp. 800-853.

NIST "NIST Special Publication 800-39 Managing Information Security Risk: Organization, Mission, and Information System View," p. 88.

Northcutt, S. "COMPUTER SECURITY INCIDENT HANDLING STEP BY STEP," SANS Institute.

Nosworthy, J. D. "Implementing Information Security In The 21st Century — Do You Have the Balancing Factors?" Computers & Security (19:4) 2000, pp 337-347.

Puhakainen, P., and Siponen, M. "Improving employees' compliance through information systems security training: an action research study," MIS Quarterly (34:4) 2010, pp 757-778.

Purser, S. A. "Improving the ROI of the security management process" Computers & Security (23:7) 2004, pp 542-546.

Ma, Q., Johnston, A. C., and Pearson, J. M. "Information security management objectives and practices: a parsimonious framework," Information Management & Computer Security (16:3) 2008, pp 251-270.

Raggad, B. G. Information security management: concepts and practice CRC Press/Taylor & Francis, Boca Raton, FL, 2010, pp. xxxv, 832 p.

Rees, J., Bandyopadhyay, S., and Spafford, E. H. "PFIRES: a policy framework for information security," Commun. ACM (46:7) 2003, pp 101-106.

Richardson, R. "2011 CSI computer crime and security survey," 2011," 2010.

Ruighaver, AB; Maynard, SB; Warren, M. "Ethical Decision Making: Improving the Quality of Acceptable Use Policies", Computers & Security, Volume 29, Issue 7, October 2010, Pages 731-736,.

Savola, R., Anttila, J., Sademies, A., Kajava, J., and Holappa, J. "Measurement of Information Security in Processes and Products," in: Security Management, Integrity, and Internal Control in Information Systems, P. Dowland, S. Furnell, B. Thuraisingham and X.S. Wang (eds.), Springer US, 2006, pp. 249-265.

Shedden, P., Ahmad, A., and Ruighaver, A. B. "Informal Learning in Security Incident Response Teams," 2011.

Shedden, P., Smith, W., and Ahmad, A. "Information security risk assessment: towards a business practice perspective,") 2010.

Siponen, M., and Willison, R. "Information security management standards: Problems and solutions," Information & Management (46:5) 2009, pp 267-270.

Spurling, P. "Promoting security awareness and commitment," Information Management & Computer Security (3:2) 1995, pp 20-26.

Stoneburner, G., Goguen, A., and Feringa, A. "Risk management guide for information technology systems," NIST Special Publication (800:30) 2002, pp 800-830.

Swanson, M., and Guttman, B. "NIST SP 800-14 “Generally Accepted Principals and Practices for Securing Information Technology Systems”."

Tan, T., Ruighaver, T., and Ahmad, A. "Incident Handling: Where the need for planning is often not recognised," Proceedings of the 1st Australian Computer, Network & Information Forensics Conference) 2003.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. A. "Aligning Security Awareness with Information Systems Security Management," Journal of Information System Security (6:1) 2010a, pp 36–54.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. "Investigating information security awareness: research and practice gaps," Information Security Journal: A Global Perspective (17:5-6) 2008, pp 207-227.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., and Gritzalis, S. "A security standards' framework to facilitate best practices' awareness and conformity," Information Management & Computer Security (18:5) 2010b, pp 350-365.

Tsoumas, V., and Tryfonas, T. "From risk analysis to effective security management: towards an automated approach," Information Management & Computer Security (12:1) 2004, pp 91-101.

Tu, Z., and Yuan, Y. "Critical Success Factors Analysis on Effective Information Security Management: A Literature Review," in: Twentieth Americas Conference on Information Systems, Savannah, 2014.

von Solms, R. "Information security management: The second generation," Computers & Security (15:4) 1996, pp 281-288.

Waly, N., Tassabehji, R., and Kamala, M. "Improving organisational information security management: The impact of training and awareness," 2012, pp. 1270-1275.

Weber, R. 2012. "Evaluating and Developing Theories in the Information Systems Discipline," *Journal of the Association for Information Systems* (13:1), pp. 1-30.

Werlinger, R., Muldner, K., Hawkey, K., and Beznosov, K. "Preparation, detection, and analysis: the diagnostic work of IT security incident response," Information Management & Computer Security (18:1) 2010, pp 26-42.

Whitman, M. E. "Enemy at the gate: threats to information security," Communications of the ACM (46:8) 2003, pp 91-95.

Whitman, M. E. "Security policy: from design to maintenance," in: Information security: policy, processes, and practices. Advances in management information systems, D.W. Straub, S.E. Goodman and R. Baskerville (eds.), Armonk, New York : M.E. Sharpe, c2008., London, England 2008, pp. 123-151.

Whitman, M. E., and Mattord, H. J. Management of information security CengageBrain.com, 2010.

Whitman, M. E., and Mattord, H. J. Principles of Information Security Cengage Learning, 2011a.

Whitman, M. E., and Mattord, H. J. Roadmap to Information Security: For IT and Infosec Managers CengageBrain. com, 2011b.

Wilson, M. and Hash, J. "Building an information technology security awareness and training program," p. 50, 2003

Zafar, H., Ko, M. S., and Clark, J. G. "Security Risk Management in Healthcare: A Case Study," Communications of the Association for Information Systems (34:1) 2014.

COPYRIGHT