Critical Success Factors Analysis on Effective Information Security Management: A Literature Review

Completed Research Paper

Zhiling Tu
McMaster University
tuz3@mcmaster.ca

Yufei Yuan
McMaster University
yuanyuf@mcmaster.ca

Abstract

Information security has been a crucial strategic issue in organizational management. Information security management is a systematic process of effectively coping with information security threats and risks in an organization. With the pressure of high implementation and maintenance cost, organizations need to distinguish between controls they need and those that are less critical. Applying critical success factors approach, this study proposes a theoretical model to investigate main factors that contribute to successful information security management. By reviewing the information security standards and literature in IS field, six critical success factors are identified and the relationship among these factors are proposed. The results reveal that with business alignment, organizational support, IT competences, and organizational awareness of security risks and controls, information security controls can be effectively developed, resulting in success of information security management.

Keywords

Critical success factor, information security management, business alignment, organizational support, organizational awareness, IT competence

Introduction

Information plays a major role in supporting an organization's business operations and facilitating an organization to achieve a competitive advantage over others (Posthumus and von Solms, 2004). While information is valuable and critical to organizations, it is also vulnerable to a variety of attacks from both inside and outside of organizations such as hackers, viruses and worms, data loss, etc. All the security risks or threats may bring organizations actual and potential losses with financial, legal, and reputation repercussions (Culnan et al., 2008; Loch et al., 1992; Straub and Welke, 1998). Information security has been a crucial strategic issue in organizational management. Implementing effective information security management is increasingly drawing attention from both practitioners and academics.

The goal of information security management (ISM) is to protect the confidentiality, integrity, and availability of information and to mitigate the various risks and threats to such information (Chang et al., 2011; Posthumus and von Solms, 2004). We thus define ISM as a systematic process of effectively coping with information security threats and risks in an organization, through the application of a suitable range of physical, technical or operational security controls, to protect information assets and achieve business goals. ISM is primarily concerned with strategic, tactical, and operational issues of the planning, analysis, design, implementation, and maintenance of an organization's information security program (Choobineh et al., 2007). ISM can help organizations reduce the security threats considerably and share business information in a trustworthy way (Chang et al., 2011).

With the pressure of high implementation and maintenance cost, organizations need to distinguish between controls they need and those that are less critical (Baker and Wallace, 2007). Focusing on critical success factors is important for organizations to effectively implement ISM. What critical factors make ISM effective and how these factors contribute to the success of ISM need theoretical modeling and empirical verification. Through a literature review, this study attempts to fill up the void by identifying critical success factors (CSFs) of ISM and developing an ISM success model that can empirically test the validity of the CSFs. The rest of the paper is organized as follows. In the next section, we will conduct a review of the literatures on main organizational factors that should contribute to the success of ISM. Then based on the review, a theoretical framework with propositions will be developed. Lastly, we will present discussion and conclusion, and highlight implications for future research and practice.

Literature Review

Rationally organizations would focus their limited resource on those things which really make the difference between success and failure to begin formal ISM programs. CSF is a widely understood concept and approach for identifying important performance requirements on which the success of the firm depends (Rockart, 1982). CSFs are those key areas, in which results, if they are satisfactory, will assure success within and of the organization (Rockart, 1979). CSFs may be used by managers as descriptions, predictors, and guidelines for achievement levels (Vedder, 1992). CSFs have been used as a management measure in different disciplines such as financial services (Boynton and Zmud, 1984), information systems (Rockart, 1982), manufacturing industry (Mohr and Spekman, 1994), project management (Davies, 2002; Pinto and Slevin, 1988), quality management (Seetharaman et al., 2006), etc.

Identifying CSFs can bridge the gap between literature and practice in the field of ISM. As a most influential practical guideline, the Standard of Good Practice for Information Security points out some critical success factors of successful ISM (ISO 27001). Combining these factors and the results of our reviewing of current literature in IS field, we identify the socio-organizational issues which are often viewed as critical to the successful implementation of ISM within an organization and group them into six key factors: business alignment, organizational support, organizational awareness, IT competence, security control development, and performance evaluation (see Table 1).

Key Factors	**Sources**	
	ISO 27001	**Literature**
Business Alignment	"objectives and activities that reflect business objectives"	Chang et al. (2011), Choobineh et al. (2007), Herath et al. (2010), Kayworth and Whitten (2010), Ma et al. (2009), Siponen and Oinas-Kukkonen (2007), Smith and Jamieson (2006), Spears and Barki (2010), Van Niekerk and Von Solms (2010), von Solms (1999)
Organizational Support		
Top management support	"commitment from management"	Aksorn and Hadikusumo (2008), Kankanhalli et al. (2003), Kayworth and Whitten (2010), Ma et al. (2009), Smith and Jamieson (2006), Straub (1988), Straub and Collins (1990), von Solms (1999), Werlinger et al. (2009), Yildirim et al. (2011)
Commitment of funding (resources)	"visible support from management"	Aksorn and Hadikusumo (2008), Smith and Jamieson (2006)
Organizational Structuring	"Information security is achieved by implementing … organizational	Boss et al. (2009), Kayworth and Whitten (2010), Ma et al. (2009), Straub (1988), Straub and Collins (1990)

	structures…”	
Organizational Awareness		
Staff awareness and training	“effective marketing of security to all managers and employees” “providing appropriate training and education”	Aksorn and Hadikusumo (2008), Culnan et al. (2008), Kayworth and Whitten (2010), Ma et al. (2009), Siponen et al. (2009), Smith and Jamieson (2006), van Niekerk and von Solms (2010), von Solms (1999), Werlinger et al. (2009), Yildirim et al. (2011)
Information security culture	“an approach to implementing security that is consistent with the organizational culture”	Chan et al. (2005), Chang and Lin (2007), Martins and Eloff (2002)
IT Competence		Chang et al. (2011), Eloff and Eloff (2003), Kayworth and Whitten (2010), Stewart (2005), von Solms (1999)
Security Controls Development		
Risk management	“a good understanding of the security requirements, risk assessment and risk management”	Herath et al. (2010), Straub and Welke (1998), von Solms (1999)
Security policies implementation	“distribution of guidance on information security policy and standards to all employees and contractors”	Siponen and Oinas-Kukkonen (2007), Straub and Welke (1998), von Solms (1999), Yildirim et al. (2011)
Standards compliance	“distribution of guidance on information security policy and standards to all employees and contractors”	Backhouse et al. (2006), Chang and Ho (2006), Hanseth and Braa (2001), Smith and Jamieson (2006), von Solms (1999), Yildirim et al. (2011)
Performance Evaluation	“a comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement”	Erkan (2005), Herath et al. (2010), Huang et al., 2006, Martin et al. (2011), Martinsons et al. (1999), Mercuri (2003)

Table 1. CSFs of Information Security Management

Business Alignment

Information security objectives and activities must be aligned with business objectives and requirements, and led by business management (Kayworth and Whitten, 2010; Ma et al., 2009; Siponen and Oinas-Kukkonen, 2007; Smith and Jamieson, 2006; Van Niekerk and Von Solms, 2010; Von Solms, 1999) The alignment component refers to the collaborative efforts between information security and business managers that can align ISM practices with business strategies of the organization (Chang et al., 2011). Being business aligned means that it is the responsibility of the business, but not the security function, to determine acceptable levels of security risk (Von Solms and Von Solms, 2004). Business-aligned security management is based on business objectives, values, or needs, as opposed to being technology asset focused (Spears and Barki, 2010). The alignment of information security with business strategy is to support organizational objectives (Herath et al., 2010).

Organizational Support

Organizational support comes from organizational factors which are related to the organization structure and managerial decisions around information security (Werlinger et al., 2009). Prior studies have paid most attentions on top management support, commitment of funding, and organizational structuring.

Top management support is found very crucial to the success of an organization's information security efforts (Kankanhalli et al., 2003; Kayworth and Whitten, 2010; Ma et al., 2009; Posthumus and von Solms, 2004; Straub, 1988; Straub and Collins, 1990; Werlinger et al., 2009). Top management commitment can support information 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 in developing effective and efficient organizational structures (Straub, 1988). Management must actively support safety efforts at all levels.

Management must consider and allocate sufficient resources to carry out day-to-day activities to accomplish both short-term and long-term information safety goals. An effective safety program needs an appropriate level of resources committed by the organization. The resources required for effective ISM may include sufficient staff, time, money, information, methods used in safety works, facilities, tools, machines, etc. (Aksorn and Hadikusumo, 2008).

Organizational structuring is extremely important to ISM (Boss et al., 2009; Kayworth and Whitten, 2010; Straub, 1988; Straub and Collins, 1990). ISM must have an organizational structure that supports reporting, communication, authority and work flow (Ma et al., 2009). Scholars advocate formal organizational structures for information security management. Straub and Collins (1990) suggests that a high-level committee should be created to be responsible for setting policy and establishing specific procedures that reduce the information security risk.

Organizational Awareness

An organization's information security strategy should comprehensively address the human factors such as security awareness and security training. All employees should be aware of possible security threats, as well as security basics and literacy which provide a baseline of key security concepts and vocabulary (Culnan et al., 2008). All relevant groups in the organization should be provided with sufficient training and supporting reference materials to allow them to protect information assets effectively (Straub and Welke, 1998).

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 information security (Van Niekerk and Von Solms, 2010). There must have a good understanding of security risks (threats and vulnerabilities) to company's information assets, and the level of security inside the organization. The awareness of information security needs to be recognized not only by staff but also by senior management. Security must be effectively marketed to all managers and employees (Von Solms, 1999).

A successful safety program can be achieved if all employees are given periodic educational and training programs in order to improve their knowledge and skills on safety at work (Aksorn and Hadikusumo, 2008). Organizationally sponsored security awareness, training, and education program is the formal social alignment mechanism to increase the overall awareness and understanding of information security (Culnan et al., 2008; Kayworth and Whitten, 2010; Ma et al., 2009; Werlinger et al., 2009). The training program is the primary way of communicating information security policies, procedures, and requirements across the organization (Culnan et al., 2008). Training can thus increase employees' security awareness, understanding and participation (Ma et al., 2009).

Information security culture, which is the way people behave towards information security in the organization, is regarded as an important factor for supporting and guiding ISM practice (Chan et al., 2005; Chang and Lin, 2007; Martins and Eloff, 2002). Culture can guide how employees think, act, and feel, thus influence the operation activities of an organization and the effectiveness of its information security practice. As new security policies may conflict with the way employees have done their jobs for years, it is critically important that an organization facilitates organizational culture in carrying out ISM, building shared values, beliefs and norms for ISM practices.

IT Competencies

IT competence is a very important ISM issue which plays a significant role in ISM, as information security technologies are used to sustain the security of information (Stewart, 2005). IT competences refer to the integrated and interrelated capabilities of internally consistent elements essential for fulfilling an IT or business objective (King, 2002). Several previous studies have demonstrated that solid organizational IT competences positively affect organization's performance and sustainable competitive advantages (Bharadwaj, 2000; Croteau and Raymond, 2004; Dehning and Stratopoulos, 2003; Santhanam and Hartono, 2003). Scholars have emphasized the same importance of technical subjects as managerial ones (Eloff and Eloff, 2003; Kayworth and Whitten, 2010; von Solms, 2000). ISM implementation is a top-down process involving technical IT resources and operations. The ability to deploy and utilize information technologies can help the organization to apply the information security technologies (Chang et al., 2011). The enhancement of IT competences has become a critical organizational issue for ISM and can help strengthen the management of information security.

Security Controls Development

To achieve an acceptable level of information security, the correct set of security controls must be identified, implemented and maintained. Security controls development can be a very complicated and resource-intensive process, which requires special resources and expertise (Chang and Ho, 2006). Through the literature review, the following critical security controls development processes are identified: risk management, security policies implementation, and standards compliance.

Risk management is the effective management and mitigation of a variety of risks by implementing cost-effective countermeasures and by reducing potential impacts on information resources to an acceptable level (Herath et al., 2010). There are four phases in formal risk management: problem identification, risk analysis, solutions generation, and solution selection (Straub and Welke, 1998). Risk management has been recognized as the most effective approach to identify the most effective set of security controls (Von Solms, 1999).

Organizational security policies are examples of organizational-level solutions to security problems, such as countermeasures and strategies adopted to reduce systems risk (Siponen and Oinas-Kukkonen, 2007; Straub and Welke, 1998). Information security policies illustrate the importance of security to the organization, define information security objectives, and specify the information security responsibility of employees (Ma et al., 2009). In general, information security is the effective implementation of policies that counteract security threats to ensure the confidentiality, availability, and integrity of information assets (Posthumus and von Solms, 2006; Smith and Jamieson, 2006). ISM standards also emphasize the need of establishing security policies so that specific information security objectives of the organization can be met (ISO 27001).

ISM standards are fundamental compatibility specifications that shape the configuration of information systems (Backhouse et al., 2006). The standards identify and introduce a set of baseline security controls conducive to an acceptable minimum level of information security to most organizations under normal circumstances (Chang and Ho, 2006; Von Solms, 1999). The objectives of the security standards are to offer a common basis for companies to develop, implement and measure effective security management practice (Von Solms, 1999). Currently, the widely accepted information security standards of principles and practice rules have embraced ISM in all aspects by providing the best information security practice guidelines in general for preventing an organization from security threat (Chang and Ho, 2006). Internationally agreed and tested standards must be followed in implementing information security (Yildirim et al., 2011).

Performance Evaluation

To plan and manage information security effectively, an effective and clarified performance measurement method is needed (Huang et al., 2006). ISM performance measurement is used to monitor progress toward achieving goals, identifying causes of unsatisfactory performance, and managing continuous improvement to ensure that information security initiatives are helping in meeting organizational goals (Herath et al., 2010). As information asset protected by ISM is a kind of intangible capital, its values are not easy to assess (Ittner and Larcker, 2003; Morgan and Strong, 2003). Prior literature has pointed out that there are many difficulties related to justification or valuation of security investment outcomes (Herath and Herath, 2009).

Several studies have proposed a cost benefit analysis or return on investments (ROI) approach for measuring security investments, which weighs the risks in relation to the value of assets to produce a quantitative measure (Erkan, 2005; Mercuri, 2003). However, these traditional performance measurement methods focus on well-known financial measures and are not enough to describe and manage intangible information assets (Huang et al., 2006; Martinsons et al., 1999).

Huang et al. (2006) develops a general BSC model of ISM, with four perspectives: financial perspective, customer perspective, internal process perspective, and learning and growth perspective. Based on BSC to measure ISM performance, studies provide organizations with the increasing value from improving measures and management insight in business. The results can help organizations assess values of ISM and consider how to link ISM performance to business strategies (Herath et al., 2010; Huang et al., 2006).

Theoretical Development

Effective organizational information security encompasses managing three components: people, process and technology (Parakkattu and Kunnathur, 2010). Based on literature review and a user participation model in information systems security risk management (Spears and Barki, 2010), we develop our research model (see figure 1) which investigates the critical factors contribute to the success of an organization's information security management. This ISM success model has six constructs: business alignment, organizational support, IT competence, organizational awareness, security controls development and ISM performance. We propose that the performance of information security management is affected by organizational support, organizational awareness and the implementation of security controls. And, organizational support, IT competence and organizational awareness predict the improvements in security controls development. Business alignment influences organizational awareness, IT competences and organizational support, which in turn all affect security controls development. And, organizational support also influences organizational awareness.

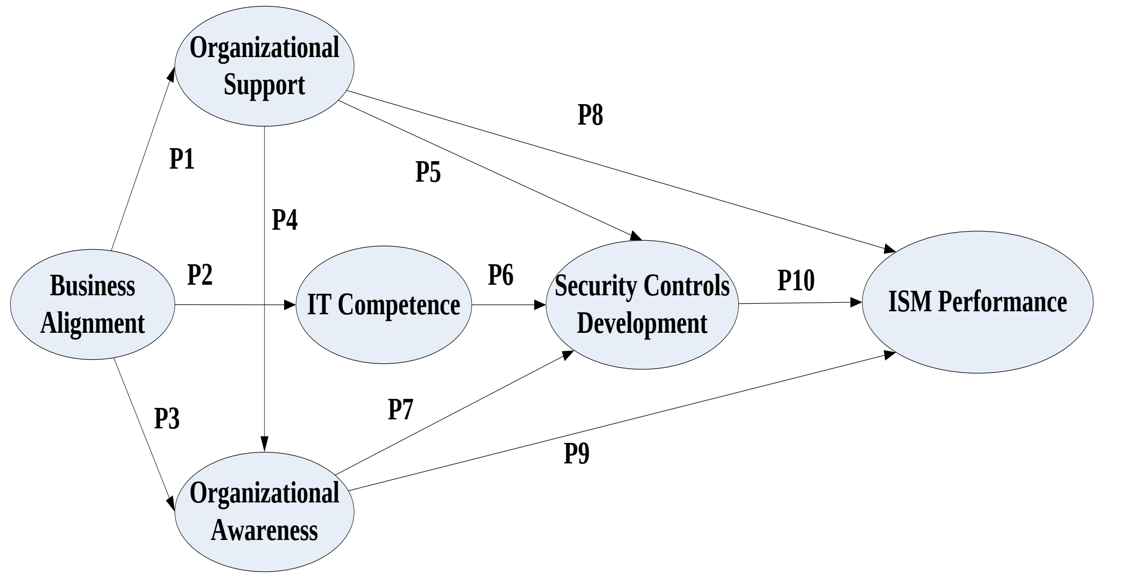

Figure 1. Research Model

An effective information security strategy should be strategically focused or business driven and thus information security is perceived as an important core business issue (Kayworth and Whitten, 2010). It must secure information assets while still enabling the business. Information security is often seen as conflict to business goals because it makes systems less usable and thus impedes achieving the normal business goals of maximizing productivity and minimizing cost (Van Niekerk and Von Solms, 2010). The lack of fit between the security objectives and the business objectives may lead to the fact that information security policies and budgets do not reflect the needs of the business (Kayworth and Whitten, 2010; Siponen and Oinas-Kukkonen, 2007).

Information security objectives should be aligned with business strategy. Such alignment may be achieved through information security planners' understanding of organizational objectives, mutual understanding between top management and information security planners, and a heightened view of the information security function within the organization (Ma et al., 2009). With the business alignment, information security initiatives are addressed at the strategic level and thus are more likely to be recognized and supported by top management (Johnston and Hale, 2009). Top management can be convinced about the importance of information security and fully appreciate the importance of ISM processes within the business framework (Smith and Jamieson, 2006; Werlinger et al., 2009). With top management commitment, information security can be regarded as an important enterprise-wide function (Kayworth and Whitten, 2010). Top management has a direct corporate governance responsibility towards ensuring that all the information assets of the company are secure (Von Solms and Von Solms, 2004). Thus the alignment helps facilitate acquisition and deployment of necessary resources to support ISM. And, the alignment helps establish formal security structure in which managers at all levels of the organization are more responsible and willing to conduct sound practices of ISM (Chang et al., 2011). Business alignment facilitates organizational support to ISM, suggesting the proposition:

P1: An alignment between security management and the business context positively affects organizational support to ISM.

Technical competence is a key element that must be incorporated in an effective information security strategy. An organization's IT competences include IT resources and operations, which are the technical foundation of ISM. Studies have asserted that organization's IT competences are affected by strategic alignment (Chang et al., 2011; Kayworth and Whitten, 2010). The collaborative efforts between information security objectives and business strategies help facilitate acquisition and deployment of IT resources that are in agreement with the organization's long-term vision (Ma et al., 2009). IT competences must be complemented with a strategy to align information security practices with business units (Kayworth and Whitten, 2010). Therefore, we propose:

P2: Business alignment positively affects organization's IT competence.

All employees should be aware of possible security threats, as well as security basics and literacy which provide a baseline of key security concepts and vocabulary (Culnan et al., 2008). All relevant groups in the organization should be provided with sufficient training and supporting reference materials to allow them to protect information assets effectively (Straub and Welke, 1998).

As security policies and procedures gained alignment with the business environment, organizational awareness of security risks and controls increases. Spears and Barki (2010) finds that security policies and procedures that are integrated with business objectives solicit greater attention to information security risks, policies, and procedures in business processes. Hence, it suggests the following proposition:

P3: Business alignment contributes to greater organizational awareness of information security risks and controls.

Top management commitment toward information safety is demonstrated through practices which are observed by individual employee, such as providing training and awareness programs. Previous studies have indicated the positive role of top management in providing organizational security culture (Barling et al., 2002; Chan et al., 2005; Knapp et al., 2006). Top management can make appropriate choices and adopt various approaches to shape the culture of their organizations for the purpose of information security, for senior management has authority and leadership to overcome cultural and organizational barriers (Barlette and Fomin, 2009; Chang and Lin, 2007).

As stated by von Solms and von Solms (2004), employees cannot be held responsible for security problems if they are not told what such security problems are, and what they should do to prevent them. Organizationally sponsored security awareness, training, and education program is the primary formal social alignment mechanism to increase the overall awareness and understanding of information security and thus, participation (Culnan et al., 2008; Kayworth and Whitten, 2010; Ma et al., 2009; Siponen et al., 2009; Werlinger et al., 2009). Further, top management commitment and efficient security structuring can enhance the whole organization's awareness of the security risks and policies. This suggests that:

P4: Organizational support raises organizational awareness of information security risks and controls.

Organizations need to establish security controls and take them into effect to protect information security. Security controls include security policies and countermeasures that can protect information systems from the security risks.

Security controls development can be a very complicated and resource-intensive process, which requires special resources and expertise (Chang and Ho, 2006). Top management commitment can guarantee the required resources for improvement. A formal security structure facilitates setting policy and establishing specific procedures that reduce the information security risk (Straub and Collins, 1990). Top management support, commitment of resources, and effective security structuring positively influence security policy enforcement (Barlette and Fomin, 2009; Kayworth and Whitten, 2010; Knapp et al., 2009). Therefore, we propose that:

P5: Organizational support positively affects the development of information security controls.

The technical IT resources provide the organization with an effective technology base, and the competent IT staff with proficient IT skills is intangibles for operating technical IT resources (Ross et al., 1996). Such IT competences influence the ability of an organisation to deploy and to utilise IT and thus help the organisation to apply the information technologies in security controls developing processes (Chang et al., 2011). On the one hand, information security controls include technical controls such as firewalls, antivirus software, intrusion detection, and encryption techniques, etc. The organization's IT capabilities would be indispensible to implement these technical controls. On the other hand, operational security controls (e.g. access controls, backup mechanism) and security management controls (e.g. usage policies) also need support from information technologies. Thus, the effectiveness of the development of information security controls is influenced by the organization's IT competence, suggesting the following proposition:

P6: IT competences positively affect the development of information security controls.

ISM standards require that all employees of the organization should receive appropriate training and regular updates in organizational policies and procedures to ensure that they are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work (ISO 27001). Empirical evidence indicates that it will be difficult to implement security controls if people have insufficient training about best IT security practices (Werlinger et al., 2009). Whitman (2008) demonstrates that the purpose of security awareness (and training) is to modify employee behavior so that the individual performs according to organizational standards. Empirical evidence has found that the greater awareness gained by users enables control designers to implement the control more consistently (Spears and Barki, 2010).

Employees have their own attitudes towards information security in the organization. These attitudes could be positive or negative and result in certain behavior (Martins and Eloff, 2002). Employees' behaviors directly influence the implementation of security controls. Thus, fostering organization's information security culture and aligning employees' behaviors with such culture is one way to ensure the effectiveness of security controls development (Von Solms and Von Solms, 2004). All these suggest that security controls implementation improves when there is greater organizational awareness.

P7: Organizational awareness positively affects the development of information security controls.

ISM performance evaluation is a control procedure, through which the return on investment can be figured out and the effectiveness and efficiency of the information security management can be checked. Management plays a very important role in an efficient and effective safety program. Management takes charge of implementing safety actions, including issuing safety policies, allocating sufficient resources, promptly reacting to safety suggestions and complaints, attending regular safety meetings and training, regularly visiting the workplace, following the same safety rules as others, etc. (Aksorn and Hadikusumo, 2008). Top management commitment establishes a focus on security within the highest levels of the organization. Support from senior management who controls system resources provides ISM with a solid foundation to succeed under the pressure of politics and budget limitations (Datta and Banerjee, 2011).

It has been empirically found that the greater the top management support, the more effective information security is in organizations, as more resources are spent to avoid security incidents (Werlinger et al., 2009). Top management is also charged with developing effective and efficient organizational structures (Straub, 1988). Straub (1988) argues that the information security group should be placed as high as possible in the organization to maximize effectiveness. Effective organizational structuring helps facilitate the organizational integration to gain security goals and further address the importance of information security at the organizational level, thus improve the effectiveness and efficiency of security controls (Boss et al., 2009; Kayworth and Whitten, 2010; Straub, 1988; Straub and Collins, 1990). Hence,

P8: Organizational support positively influences the performance of ISM.

Organizational awareness represents that employees are aware of the organization's information security risks, and the potential damage they can cause. And, they are aware of the information security policies, procedures and countermeasures existing in the company. If employees lack the knowledge of security controls, they may misuse or misinterpret many security controls and thus the security controls may fail (Van Niekerk and Von Solms, 2010). Empirical studies have shown that if employees are aware of how vulnerable their organization is to security threats and the severity of these threats, they will have a strong intention to comply with information security policies (Siponen et al., 2009). Meanwhile, when potential offenders realize that the risk of punishment is high and penalties for violation are severe, they will be inhibited from committing misbehavior (Straub and Collins, 1990). Therefore, organizational awareness of security risks and controls enables the organization to improve effectiveness and efficiency in the security management system (Spears and Barki, 2010). We then propose that:

P9: Organizational awareness positively influences the performance of ISM.

A clearly defined set of policies regarding proper and improper use of the information system is the precondition to implementing all the effective security management (Straub, 1990). Better designed and implemented controls will result in better control performance from fewer errors or increased efficiency in the system of controls (Spears and Barki, 2010). Both scholars and ISM standards have asserted that information security will be achieved only if a correct set of security controls is identified, implemented and maintained (ISO 27001; Chang et al., 2011; Chang and Lin, 2007). In order to determine whether the information security management is meeting the goals, the organization needs to measure the progress of all security controls (Ma et al., 2009). In addition, complying with ISM standards constitutes important drivers to success of information security management (Martins and Eloff, 2002).

P10: Effective security controls development positively influences the performance of ISM.

Discussion and Conclusion

Applying critical success factors approach, this study proposes a theoretical model to investigate main factors that contribute to successful information security management. By reviewing the ISM standards and literature in IS field, six critical success factors are identified and the relationship among these factors are proposed. The results reveal that with business alignment, organizational support, IT competences, and organizational awareness of security risks and controls, information security controls can be effectively developed, resulting in success of information security management.

This study is expected to contribute to both academics and management practice. Theoretically, this study proposes a theoretical model of successful information security management that can be empirically tested. While practitioners have developed information security standards and guidelines, both theory clarification and rigorous empirical studies are strongly needed in the academic area. To the best of our knowledge, this is the first study that attempts to study these very practical issues with theoretical support and potential empirical verification. Practically, the results of this research will help organizations better implement information security management. With the identification of critical success factors, managers can focus on the key issues to ISM success and better arrange limited resources to secure the implementation of ISM. Further, the potential empirical test of this study can provide manages with a way of evaluating the reliability or objectivity of the claimed best practices in practical standards and guidelines.

This study provides recommendations for future research avenues. First, empirical study needs to be conducted. The theoretical model is developed through literature review and has never been tested. The model's reliability and validity need support from empirical studies. Second, as little empirical study has been done on information security management from organizational level, the operationalization of all constructs needs to be developed and further validated. Finally, stronger theory base is needed to further support this research model.

REFERENCES

Aksorn, T., and Hadikusumo, B. H. W. 2008. "Critical Success Factors Influencing Safety Program Performance in Thai Construction Projects," *Safety Science* (46:4), pp 709-727.

Backhouse, J., Hsu, C. W., and Silva, L. 2006. "Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard," *MIS quarterly* (30:Special Issue on Standard Making (Aug., 2006)), pp 413-438.

Baker, W. H., and Wallace, L. 2007. "Is Information Security under Control?: Investigating Quality in Information Security Management.," *IEEE Security & Privacy* (5:1), pp 36-44.

Barlette, Y., and Fomin, V. V. 2009. "The Adoption of Information Security Management Standards:A Literature Review," IGI Global, pp. 119-140.

Barling, J., Loughlin, C., and Kelloway, E. K. 2002. "Development and Test of a Model Linking Safety-Specific Transformational Leadership and Occupational Safety," *Journal of Applied Psychology* (87:3), pp 488-496.

Bharadwaj, A. S. 2000. "A Resourced-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation," *MIS Quarterly* (24:1), pp 169-196.

Boss, S. R., 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.

Boynton, A. C., and Zmud, R. W. 1984. "An Assessment of Critical Success Factors," *Sloan Management Review* (25:4), pp 17-27.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of information privacy and security* (1:3), pp 18-41.

Chang, S. E., Chen, S.-Y., and Chen, C.-Y. 2011. "Exploring the Relationships between It Capabilities and Information Security Management " *International Journal of Technology Management* (54:2/3), pp 147-166.

Chang, S. E., and Ho, C. B. 2006. "Organizational Factors to the Effectiveness of Implementing Information Security Management," *Industrial Management & Data Systems* (106:3), pp 345-361.

Chang, S. E., and Lin, C.-S. 2007. "Exploring Organizational Culture for Information Security Management," *Industrial Management & Data Systems* (107:3), pp 438-458.

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

Croteau, A.-M., and Raymond, L. 2004. "Performance Outcomes of Strategic and It Competencies Alignment," *Journal of Information Technology* (19:3), pp 178-190.

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.

Datta, S. P., and Banerjee, P. 2011. "Guidelines for Performance Measures of Information Security of It Network and Systems," *International Journal of Research and Reviews in Next Generation Networks* (1:1), pp 39-43.

Davies, T. 2002. "The 'Real' Success Factors on Projects," *International Journal of Project Management* (20:3), pp 185-190.

Dehning, B., and Stratopoulos, T. 2003. "Determinants of a Sustainable Competitive Advantage Due to an It-Enabled Strategy," *The Journal of Strategic Information Systems* (12:1), pp 7-28.

Eloff, J. H. P., and 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 2003), South African Institute for Computer Scientists and Information Technologists2003, pp. 130–136.

Erkan, K. 2005. "Evaluating It Security Performance with Quantifiable Metrics," http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.4000&rep=rep1&type=pdf.

Herath, H., and Herath, T. 2009. "Investments in Information Security: A Real Options Perspective with Bayesian Post-Audit," *Journal of Management Information Systems* (25:3), pp 337-375.

Herath, T., Herath, H., and Bremser, W. G. 2010. "Balanced Scorecard Implementation of Security Strategies: A Framework for It Security Performance Management," *Information Systems Management* (27:1), pp 72-81.

Huang, S.-M., Lee, C.-L., and Kao, A.-C. 2006. "Balancing Performance Measures for Information Security Management: A Balanced Scorecard Framework," *Industrial Management & Data Systems* (106:2), pp 242-255.

ISO 27001, "Information Technology - Code of Practice for Information Security Management."

Ittner, C. D., and Larcker, D. F. 2003. "Coming up Short on Nonfinancial Performance Measurement," *Harvard Business Review* (81:11), pp 88-95.

Johnston, A. C., and Hale, R. 2009. "Improved Security through Information Security Governance," *Communications of the ACM* (52:1), pp 126-129.

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.

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.

King, W. R. 2002. "It Capabilities, Business Processes, and Impact on the Bottom Line," *Information Systems Management* (19:2), pp 85-87.

Knapp, K. J., Marshall, T. E., Rainer, R. K., and Ford, N. F. 2006. "Information Security: Management's Effect on Culture and Policy," *Information Management and Computer Security* (14:16), pp 24-36.

Knapp, K. J., R. Franklin Morris, J., Marshall, T. E., and Byrd, T. A. 2009. "Information Security Policy: An Organizational-Level Process Model," *computers & security* (28:7), pp 493-508.

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. "Threat to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), pp 173-186.

Ma, Q., Schmidt, M. B., and Pearson, J. M. 2009. "An Integrated Framework for Information Security Management," *Review of Business* (30:1) 09/22/2009, pp 58-69.

Martins, A., and Eloff, J. 2002. "Assessing Information Security Culture," *Information Security South Africa (ISSA), Johannesburg, South Africa.*), pp 1-14.

Martinsons, M., Davison, R., and Tse, D. 1999. "The Balanced Scorecard: A Foundation for the Strategic Management of Information Systems," *Decision Support Systems* (25:1), pp 71-88.

Mercuri, R. T. 2003. "Analyzing Security Costs," *Communications of the ACM* (46:6), pp 15-18.

Mohr, J., and Spekman, R. 1994. "Characteristics of Partnership Success: Partnership Attributes, Communication Behavior, and Conflict Resolution Techniques," *Strategic Management Journal* (15:2), pp 135-152.

Morgan, R. E., and Strong, C. A. 2003. "Business Performance and Dimensions of Strategic Orientation," *Journal of Business Research* (56:3), pp 163-176.

Parakkattu, S., and Kunnathur, A. S. 2010. "A Framework for Research in Information Security Management," *2010 Northeast Decision Sciences Institute Proceedings*), pp 318-323.

Pinto, J. K., and Slevin, D. P. 1988. "Critical Success Factors across the Project Life Cycle," *Project Management Journal* (19:3), pp 67-75.

Posthumus, S., and von Solms, R. 2004. "A Framework for the Governance of Information Security," *Computers & Security* (23), pp 638-646.

Posthumus, S., and von Solms, R. 2006. "A Responsibility Framework for Information Security," *Security Management, Integrity, and Internal Control in Information Systems* (193), pp 205-221.

Rockart, J. F. 1979. "Chief Executives Define Their Own Data Needs," *Harvard Business Review* (57:2), pp 81-93.

Rockart, J. F. 1982. "The Changing Role of the Information Systems Executive: A Critical Success Factors Perspective," *Sloan Management Review* (24:1), pp 3-13.

Ross, J. W., Beath, C. M., and Goodhue, D. L. 1996. "Develop Long-Term Competitiveness through It Assets," *Sloan Management Review* (38:1), pp 31-42.

Santhanam, R., and Hartono, E. 2003. "Issues in Linking Information Technology Capability to Firm Performance," *MIS Quarterly* (27:1), pp 125-153.

Seetharaman, A., Sreenivasan, J., and Boon, L. P. 2006. "Critical Success Factors of Total Quality Management," *Quality and Quantity* (40:5), pp 675-695.

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., 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.

Smith, S., and Jamieson, R. 2006. "Determining Key Factors in E-Government Information System Security," *Information systems management* (23:2), pp 23-32.

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS quarterly* (34:3), pp 503-522.

Stewart, A. 2005. "Information Security Technologies as a Commodity Input," *Information Management & Computer Security* (13:1), pp 5-15.

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

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

Vedder, J. N. 1992. "How Much Can We Learn from Success?," *The Executive* (6:1), pp 56-66.

von Solms, B. 2000. "Information Security - the Third Wave?," *Computers & Security* (19:7), pp 615-620.

Von Solms, B., and Von Solms, R. 2004. "The 10 Deadly Sins of Information Security Management," *Computers & Security* (23:5), pp 371-376.

Von Solms, R. 1999. "Information Security Management: Why Standards Are Important," *Information Management & Computer Security* (7:1), pp 50-58.

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.

Yildirim, E. Y., Akalp, G., Aytac, S., and Bayram, N. 2011. "Factors Influencing Information Security Management in Small-and Medium-Sized Enterprises: A Case Study from Turkey," *International Journal of Information Management* (31:4), pp 360-365.