Effective Information Security Management

Effective Information Security Management:

A Critical Success Factors Analysis

By zhiling tu, *b.a., MBA, m.Sc., M.Eng.*

A Thesis

Submitted to the School of Graduate Studies

In Partial Fulfillment of the Requirements

For the Degree

Doctor of Philosophy

McMaster University© Copyright by Zhiling Tu, May 2015

Descriptive Note

McMaster University DOCTER OF PHYLOSOPHY (2015) Hamilton, Ontario

TITLE: Effective Information Security Management: A Critical Success Factors Analysis

AUTHOR: Zhiling Tu, B.A. (Nanjing University), M. Eng. (Nanjing University), MBA(Maastricht School of Management), M. Sc. (Queen’s University),

SUPERVISOR: Professor Yufei Yuan

NUMBER OF PAGES: xii, 173

Lay Abstract

This thesis addresses three research questions: (1) How to measure ISM performance? (2) What are the critical factors that must be present to make ISM effective? And, (3) how do these factors contribute to the success of ISM?

To the best of the researcher’s knowledge, this is the first known study to empirically investigate the most important factors for ISM success and their impact on ISM performance. This study contributes to the advancement of the information security management literature by (1) proposing a theoretical model to examine the effects of critical organizational success factors on the organization’s ISM performance, (2) empirically validating this proposed model, (3) developing and validating an ISM performance construct, and (4) reviewing the most influential information security management standards and trying to validate some basic guidelines of the standard.

Abstract

Information security has been a crucial strategic issue in organizational management. Information security management (ISM) is 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. There is a strong need for rigorous qualitative and quantitative empirical studies in the field of organizational information security management in order to better understand how to optimize the ISM process.

Applying critical success factors approach, this study builds a theoretical model to investigate main factors that contribute to ISM success. The following tasks were carried out: (1) identify critical success factors of ISM performance; (2) build an ISM success model and develop related hypotheses; (3) develop construct measures for critical success factors and ISM performance evaluations; (4) collect data from the industry through interviews and surveys; and (5) empirically verify the model through quantitative analysis.

The proposed theoretical model was empirically tested with data collected from a survey of managers who were presently involved with decision making regarding their company's information security (N=219). Overall, the theoretical model was successful in capturing the main antecedents of ISM performance. The results suggest 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 successful information security management.

This study contributes to the advancement of the information security management literature by (1) proposing a theoretical model to examine the effects of critical organizational success factors on the organization’s ISM performance, (2) empirically validating this proposed model, (3) developing and validating an ISM performance construct, and (4) reviewing the most influential information security management standards and trying to validate some basic guidelines of the standard.

Acknowledgement

I would never have been able to complete my thesis without the guidance of my committee members, help from friends, and support from my family.

First and foremost, I would like to express my deepest gratitude to my supervisor, Dr. Yufei Yuan, for his continuous support to my Ph.D. study and research. His excellent guidance, caring, patience, motivation, enthusiasm, and immense knowledge helped me in all the time of my research and writing of this thesis.

I would like to thank the other members of my committee, Dr. Norman P. Archer and Dr. Catherine Connelly, for their encouragement, insightful comments, and the assistance they provided at all levels of the research project. My sincere thanks also go to Dr. Ofir Turel, who as a good friend, was always willing to help and give his best suggestions to my research.

Last but not the least, I would like to thank my family for the support they provided me through my entire life. In particular, I must acknowledge my husband Gary Yu Zhao and my lovely sons, Andrew and Raymond, who were always there cheering me up with their love and encouragement.

Table of Contents

[Chapter 1 Introduction 1](#_Toc425114689)

[Chapter 2 Literature Review 11](#_Toc425114690)

[2.1 ISM Performance Evaluation 11](#_Toc425114691)

[2.2 Critical Success Factors of ISM 16](#_Toc425114692)

[Chapter 3 Research Model and Hypothesis Development 31](#_Toc425114693)

[3.1 Theoretical Basis 31](#_Toc425114694)

[3.2 Research Model 38](#_Toc425114695)

[3.3 Hypotheses Development 41](#_Toc425114696)

[Chapter 4 Methodology 54](#_Toc425114697)

[4.1 Measurement development 55](#_Toc425114698)

[4.2 Qualitative Study 65](#_Toc425114699)

[4.3 Pilot Study 69](#_Toc425114700)

[4.4 Final Study 73](#_Toc425114701)

[4.5 Summary 74](#_Toc425114702)

[Chapter 5 Data Analysis and Results 76](#_Toc425114703)

[5.1 Data Collection 76](#_Toc425114704)

[5.2 Data Screening 77](#_Toc425114705)

[5.3 Demographics 79](#_Toc425114706)

[5.4 Descriptive Statistics 83](#_Toc425114707)

[5.5 Common-Method Bias Check 84](#_Toc425114708)

[5.6 Research Model Validation 85](#_Toc425114709)

[5.6.1 Measurement Model 85](#_Toc425114710)

[5.6.2 Structural Model 92](#_Toc425114711)

[5.7 Post Hoc Analysis 97](#_Toc425114712)

[5.8 Summary 101](#_Toc425114713)

[Chapter 6 Discussion and Conclusions 103](#_Toc425114714)

[6.1 Key Findings 103](#_Toc425114715)

[6.1.1 Measurement of ISM Performance 104](#_Toc425114716)

[6.1.2 Antecedents of ISM Performance 106](#_Toc425114717)

[6.1.3 Antecedents of Security Controls 110](#_Toc425114718)

[6.1.4 Other Relationships 111](#_Toc425114719)

[6.1.5 Warped Relationships 114](#_Toc425114720)

[6.1.6 Control Factors 115](#_Toc425114721)

[6.2 Contributions 117](#_Toc425114722)

[6.2.1 Theoretical Contributions 117](#_Toc425114723)

[6.2.2 Implications for Practice 120](#_Toc425114724)

[6.3 Limitations 124](#_Toc425114725)

[6.4 Future Research 127](#_Toc425114726)

[6.5 Conclusions 129](#_Toc425114727)

[References 131](#_Toc425114728)

[Appendix 1. Informed Consent Form 141](#_Toc425114729)

[Appendix 2. Survey Questionnaire 144](#_Toc425114730)

[Appendix 3. Interview Questions 155](#_Toc425114731)

[Appendix 4. Composite/Indicator Box Plots 156](#_Toc425114732)

[Appendix 5. Bivariate Data Plots 160](#_Toc425114733)

[Appendix 6. Alternative Model Test Results 170](#_Toc425114734)

List of Figures

[Figure 3.1 BSC Model for Information Security 33](#_Toc418470115)

[Figure 3.2 A Research Model Based on System Development Theories 34](#_Toc418470116)

[Figure 3.3 Adapted Alignment Performance Model 37](#_Toc418470117)

[Figure 3.4 Research Model 41](#_Toc418470118)

[Figure 5.1 PLS Model Testing Results 93](#_Toc418470119)

List of Tables

[Table 2.1 CSFs of Information Security Management 18](#_Toc418552308)

[Table 4.1 Construct Measures 62](#_Toc418552309)

[Table 5.1 Summary of Outliers 78](#_Toc418552310)

[Table 5.2 Job Positions of Participants 79](#_Toc418552311)

[Table 5.3 Industry Type 80](#_Toc418552312)

[Table 5.4 Organization Type 82](#_Toc418552313)

[Table 5.5 Organization Size 82](#_Toc418552314)

[Table 5.6 Security Standard Application of Organizations 83](#_Toc418552315)

[Table 5.7 Descriptive Statistics of Constructs 83](#_Toc418552316)

[Table 5.8 Item Reliability Assessment 86](#_Toc418552317)

[Table 5.9 Construct Reliability Assessment 87](#_Toc418552318)

[Table 5.10 Loadings and Cross-loadings, and AVEs for Multi-item Constructs 88](#_Toc418552319)

[Table 5.11 Inter-Construct Correlations and Square Roots of AVEs 89](#_Toc418552320)

[Table 5.12 Formative Construct Validity Assessment 92](#_Toc418552321)

[Table 5.13 Path Coefficients 94](#_Toc418552322)

[Table 5.14 Summary of Hypothesis Tests 95](#_Toc418552323)

[Table 5.15 Path Effect Size Analysis 97](#_Toc418552324)

[Table 5.16 Control Variable Analysis 99](#_Toc418552325)

[Table 5.17 Path Effect Sizes Analysis for Control Variables 100](#_Toc418552326)

[Table 5.18 Path Analysis with Control Variables 100](#_Toc418552327)

List of Abbreviations

|  |  |
| --- | --- |
| APC | Average Path Coefficient |
| ARS | Average R-Squared |
| AVE | Average Variance Extracted |
| AVIF | Average Variance Inflation Factor |
| BA | Business Alignment |
| BSC | Balanced Scorecard |
| CSF | Critical Success Factors |
| CIO | Chief Information Officer |
| CSO | Chief Security Officer |
| EFA | Exploratory Factor Analysis |
| GAISP | Generally Accepted Information Security Principles |
| IC | IT Competence |
| ICT | Information and Communication Technology |
| IP | ISM Performance |
| IS | Information Systems |
| ISD | Information System Development |
| ISM | Information Security Management |
| IT | Information Technology |
| ITSec BSC | IT Security Balanced Scorecard |
| OA | Organizational Awareness |
| OS | Organizational Support |
| ROI | Return on Investments |
| SC | Security Controls |
| SRM | Security Risk Management |
| SSE-CMM | System Security Engineering Capability Maturity Model |

Declaration of Academic Achievement

I declare that the work in the thesis has been performed by me. My supervisor, Dr. Yufei Yuan and my committee members, Dr. Norman P. Archer and Dr. Catherine Connelly were instrumental in offering guidance on study design, implementation, data analysis and theory construction. My original contributions to the study include the conception of the idea, theory development, submitting the proposal to the research ethics boards of McMaster University, recruitment of participants, conducting interviews, and data analysis. I wrote all chapters contained within this thesis and all committee members contributed to revisions. All members have approved the final version.

# Introduction

Information has been seen as a basic and strategic asset which is vital to organizations. It plays a major role in supporting an organization’s business operations and facilitating its achievement of 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 organizations such as hackers, viruses and worms, pharming, financial fraud, identity theft, data loss, etc. In the 2014 US State of Cybercrime Survey[[1]](#footnote-2), three in four (77%) respondents had detected a security event in the past 12 months, and more than a third (34%) said the number of security incidents detected had increased over the previous year. With the growing threat of attack, information security has become increasingly important to organizations. 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). Therefore, organizations need to adopt all the necessary measures to protect information systems and assure that information systems will behave as expected and produce reliable results (Boss et al., 2009). 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.

Although information security management (ISM) is strategically important to organizational success (Ma et al., 2009), very few published papers have formally defined this concept. According to Van Niekerk and Von Solms (2010), the problem of managing information security involves the management of many conflicts, such as conflicts between business and security objectives, conflicts between human behavior and security processes, etc. Siponen and Oinas-Kukkonen (2007) define information systems (IS) security management as “a means of maintaining secure IS in organizations, including IS planning and evaluation” (p. 62). The goal of 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). In the current study, ISM is defined 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, in order 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, enabling them to share business information in a trustworthy way (Chang et al., 2011).

Business information frequently comes into contact with technology, people and process elements, each of which has the potential to present a security risk to an organization’s business information assets (Boynton and Zmud, 1984; Posthumus and von Solms, 2004). A holistic approach to securing technology, people, processes, and other organizational factors on an enterprise scale should be considered. Organizations tend to focus on technological factors which are thought to play the primary role in effective information security solutions (Siponen, 2005). This focuses on sophisticated technologies to secure information assets and to prevent security breaches. However, such technical controls are passive instruments that are enforced or manipulated to comply with a given policy (Siponen, 2005). Effective information security management must implement organizational-level solutions to security problems in the organization’s socio-organizational context (Kayworth and Whitten, 2010). Consequently, practitioners and scholars have recognized that the emphasis of information security should go beyond technical controls and incorporate business process and organizational issues (Choobineh et al., 2007; Culnan et al., 2008; Dhillon and Backhouse, 2001; Dhillon and Torkzadeh, 2006; Kayworth and Whitten, 2010; Ma et al., 2009; Parakkattu and Kunnathur, 2010; Siponen et al., 2009; Siponen, 2005; Van Niekerk and Von Solms, 2010). However, due to the complexity of security management issues, professional guidelines are very much needed by organizations.

Currently, information security standards and other best practices serve as a starting point for many organizations that wish to establish an information security strategy. Documents like information security checklists and standards suggest appropriate security controls that can preserve the confidentiality, integrity and availability of business information. They help organizations integrate information security into daily activities and functions. Checklists identify every conceivable control that can be implemented in information systems and propose solutions that would help in overcoming security threats (Baskerville, 1993; Dhillon and Backhouse, 2001; Dhillon and Torkzadeh, 2006). Information security analysts use checklists to check if security controls are already in place, to determine the adequacy of existing controls and the necessity of implementing new ones. Published security checklists in the early days include IBM’s 88-point security assessment questionnaire (IBM, 1972), the SAFE Checklist (Krauss, 1972; Krauss, 1980), the AFIPS Checklist for Computer Center Self-Audits (Browne, 1979) and the Computer Security Handbook (Hoyt, 1973; Hutt et al., 1988). As a first generation security method, the checklist approach has been criticized for its practical and theoretical weaknesses. In practice, the security checklist method is intended to provide guidelines for evaluating, but not specifying, information security. This method oversimplifies the security considerations that arise in more complex information systems, which may lead to unauthorized design shortcuts and consequent security oversights. These unstructured and narrative-style security specifications are also hard to understand and difficult to maintain (Baskerville, 1993). The checklist approach has no theoretical foundation. Checklists involve a focus on observed events and details of procedures, without considering the social nature of problems or understanding what the substantive questions are (Dhillon and Backhouse, 2001). Furthermore, the checklist approach has not been empirically verified.

Information security standards offer guidelines to organizations by identifying and introducing a set of controls that can help maintain an acceptable level of information resource protection (Chang et al., 2011). The most influential security management standards are Generally Accepted Information Security Principles (GAISP), The Code of Practice for Information Security Management (BS ISO/IEC17799), System Security Engineering Capability Maturity Model (SSE-CMM), and The Standard of Good Practice for Information Security. The latest ISO standard version, BS ISO/IEC17799: 2000 has been accepted as an ISO standard for use in securing organizational information. These standards provide a common basis for organizations to develop, implement, and measure security management practice. Aiming to provide an international, authoritative, and comprehensive benchmark for information security, they have been praised as being key to any successful information security management activities (Von Solms, 1999). However, information security standards mainly focus on the existence of processes but not their content. For instance, following the standard, a company may set up a training session or present information security policies to employees, but this does not ensure that employees will actually follow the information security procedures correctly. The existence of prescribed security processes in organizations does not mean the goals of the processes are achieved (Siponen, 2006). (Doherty and Fulford, 2005) surprisingly found that there was no statistically significant relationship between the adoption of best practices that follow the international standard and the reduction of security breach incidence. Siponen and Willison (2009) further point out that “current guidelines have two problems: First, the well-known ones are generic in scope, while organizations need methods tailored to their environment and operations. Second, they have not been validated but are fostered by an appeal to common practice, which is an unsound basis for a true standard.” (p.267). They suggest that rigorous empirical studies are needed that consider all possible variables, through either qualitative (e.g., action research, interpretive field studies, interpretive case research) or quantitative (e.g., survey) methodologies (Siponen and Willison, 2009).

Research interests in the information security field have continued to increase (Guo et al., 2011). Unlike before when information security was often seen as technically oriented and research in this area mainly focused on “technical context” (Siponen and Oinas-Kukkonen, 2007), more recent studies are focusing on the behavioral aspects of information security. Currently, individual employee security behaviors such as security policy violation or compliance have been widely studied, using different theoretical interpretations such as deterrence theory (D'Arcy et al., 2009), neutralization theory (Siponen and Vance, 2010), protection motivation theory (Anderson and Agarwal, 2010), composite behavior theory (Guo et al., 2011), and risk avoidance theory (Liang and Xue, 2009). However, research on information security at the organizational level has been relatively sparse (Kotulic and Clark, 2004). Only a few opinion-based studies have been published, which review ISM at the organizational level from different perspectives such as information security governance, risk management, and ISM processes (Chang et al., 2011; Choobineh et al., 2007; Dhillon and Backhouse, 2001; Johnston and Hale, 2009; Posthumus and von Solms, 2004; von Solms and von Solms, 2006). Some scholars describe information security governance as the process of how information security is integrated into corporate governance and addressed at an executive level (Johnston and Hale, 2009; Posthumus and von Solms, 2004; von Solms and von Solms, 2006). Others have instituted information security as one of an organization’s fundamental business operations through governance, where it can be more effectively and efficiently addressed to improved outcomes (Johnston and Hale, 2009). Still other researchers have indicated that information security is a form of risk management with which the information risk faced by the business can be managed (Chang et al., 2011). From the perspective of risk management, information can be secure if countermeasures are developed and implemented in a logical and sequential manner and if negative outcomes can be prevented (Dhillon and Backhouse, 2001). Other ISM studies conceptualize ISM as a cyclic, multiple-phase process. Pipkin (2000) identifies the ISM process as inspection, protection, detection, reaction, and reflection. Nyanchama (2005) defines an ISM life cycle which includes planning, execution, monitoring, and feedback. Ma et al. (2009) describe ISM as a continuous dynamic decision-making process which includes five steps: assess, establish, analyze, develop, and implement/evaluate. These researchers assert that assuring organizational information security requires consideration of all these phases. Although these studies address important issues of ISM, they focus on different perspectives and not on a comprehensive point of view to study how to successfully implement information security management. Furthermore, they did not provide empirical support for their models of ISM.

One group of researchers called for research to explore successful information security programs (Choobineh et al., 2007). Previous studies have often focused on the presence or absence of information security controls, rather than their quality and performance (Baker and Wallace, 2007). Since some scholars have pointed out that both the content and quality of security management matter (Siponen, 2006), how to measure the quality of ISM is an important issue for both ISM practice and research. A comprehensive and balanced system of measurement to evaluate performance in information security management needs to be developed and studied empirically. We also need to understand why certain organizations are able to implement information security management effectively, while at the same time others struggle to do so. What factors may affect the success of ISM? Several papers have tried to examine the influence of organizational factors on the effectiveness of ISM in different contexts, but they have failed to organize their research within a sound theoretical framework and empirically test it (Chang and Ho, 2006; Singh and Gupta, 2014; Smith and Jamieson, 2006; Yildirim et al., 2011). Due to the pressures of high implementation and maintenance costs, organizations need to distinguish between controls they need and those that are less critical (Baker and Wallace, 2007). This could be addressed by theory clarification and aggregation in the field of ISM critical success factors (CSFs). Most of the traditional ISM methods are based on opinion analysis and are fostered by an appeal to common practice, offering little evidence of their usefulness and relevance in practice (Siponen, 2005). Practitioners have no way of evaluating the reliability (or objectivity) of the claimed best practices (Siponen and Willison, 2009). Hence, there is a need for rigorous qualitative and quantitative empirical studies to test and refine ISM methods in practical settings. To address the major questions we have unearthed in our review, we need to focus on three research questions: (1) How to measure ISM performance? (2) What are the critical factors that must be present to make ISM effective? And, (3) how do these factors contribute to the success of ISM?

This study attempts to fill the void in understanding ISM effectiveness by identifying CSFs of ISM and developing an ISM success model to empirically test the validity of the identified CSFs. To achieve these objectives we plan to carry out the following tasks: (1) identify the objectives of ISM and the critical success factors that might contribute to the success of ISM; (2) build an ISM success model and develop hypotheses around the influence of CSFs that have been identified; (3) develop constructs for measuring for CSFs and evaluating ISM performance; (4) collect data relevant to the model from industry through interviews and surveys; and (5) empirically validate the model through quantitative analysis.

The rest of the thesis is organized as follows. In the next section, a literature review is conducted on ISM performance measurement and critical success factors of ISM. Based on the CSFs that have been identified, a research model is developed, along with relevant hypotheses. The related methodology is discussed after model development. Finally, following data analysis, a discussion and conclusions are presented, highlighting implications of this work for future research and practice.

# Literature Review

In this chapter we prepare to construct an ISM success model by first determining how to evaluate an organization’s ISM performance. Then critical success factors that can contribute to the organization’s ISM success are identified.

## ISM Performance Evaluation

To plan and manage information security, an effective and clarified performance measurement method is needed (Huang et al., 2006). ISM performance measurement can be used to monitor progress toward achieving goals, identifying causes of unsatisfactory performance, and managing continuous improvement to ensure that information security initiatives are helping to meet organizational goals (Herath et al., 2010). As information assets protected by ISM are intangible capital, their value is 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). Through our literature review, we found that the most widely used ISM performance measurement approaches can be grouped into two categories: information security standards certification and financial measures-based evaluation.

***2.1.1 Evaluation Based on ISM Standards***

ISM standards are designed to ensure good management practices in organizations and are among the most widely used methods of information security management (Hsu, 2009; Siponen, 2006). These standards specify the requirements and processes of good ISM practices by covering the aspects of people, processes, IT systems and policies that enable a business to establish, implement, review and improve information security (van Wesse et al., 2011; Von Solms, 1999). Prior literature has reviewed different international ISM standards, including the TCSEC/Orange Book, GMITS, NIST SP 800 and COBIT (ISACA 2005), IT Baseline Protection Manual, Generally Accepted Information Security Principles (GAISP), the System Security Engineering CMM (SSE-CMM), the Standard of Good Practice for Information Security, and its derivatives (BS7799, BS ISO/IEC17799: 2000, ISO/IEC 27001 and ISO/IEC 27002) (Saint-Germain, 2005; Siponen, 2006; Siponen and Willison, 2009; van Wesse et al., 2011).

Among these standards, the international standards ISO/IEC 27001 and ISO/IEC 27002, and their former versions BS7799 and BS ISO/IEC17799: 2000, have been praised as the most prominent international efforts on information security (Ma and Pearson, 2005; Siponen, 2006; van Wesse et al., 2011). These standards provide both an authoritative statement on information security and the procedures that need to be adopted by organizations to ensure information security (Ma and Pearson, 2005). ISO/IEC 27001 is an overall program that combines risk management, security management, governance and compliance, while ISO/IEC 27002 establishes guidelines and general principles for initiating, implementing, maintaining, and improving ISM within an organization (Barlette and Fomin, 2009). The standards comprise 10 security domains consisting of 36 security practices and seek to address security compliance at all levels: managerial, organizational, legal, operational, and technical (Ma and Pearson, 2005). The standard also includes 127 controls that identify specific means for meeting the relevant control objectives (Saint-Germain, 2005).

ISM standards provide a comprehensive model for ISM that helps organizations harmonize their security-related organizational processes. They also provide the basis for self-assessment, reassessing the information security practices of business partners, and the independent evaluation of ISM within the business organization (Ma and Pearson, 2005). ISM standards can be viewed as an expression of accumulated expertise (Schumacher, 2002). They provide a structured and coherent approach to comprehensive risk assessment (Hong et al., 2003). The related ISM guidelines play a key role in managing and certifying organizational information security (Siponen and Willison, 2009).

ISO/IEC 27001 sets the goal of ISM to protect information asset confidentiality, integrity and availability. Its goal is to ensure that information is accessible only to those authorized to have access to it, to safeguard the accuracy, completeness and timeliness of information and processing methods, and to ensure that authorized users have access to information and associated assets as and when required. Several studies have used these characteristics to assess the performance of ISM (Chang et al., 2011; Chang and Lin, 2007). The standard also demonstrates that periodic reviews should be scheduled to assess a security policy’s effectiveness, cost and impact of controls on business efficiency, and its effects on changes to technology. Organizations that are awarded an ISO security standard certificate are usually regarded as having successful ISM.

There are some limitations on the use of standards for ISM performance measurement. On the one hand, the complexity of the standards and the corresponding lack of guidance make standards difficult to understand and implement (Barlette and Fomin, 2009; Parker, 2006; Wiander, 2007). Thus their complexity limits their ability to help organizations effectively measure their ISM performance. On the other hand, the processes, guidelines, and principles provided by standards are abstract and simplified, and do not consider the quality of the processes (Siponen, 2006), leading to difficulties in applying the standards to assess ISM performance. Furthermore, many scholars have questioned the validity of standards since few empirical studies have been conducted to validate them (Ma and Pearson, 2005; Mercuri, 2003). ISM guidelines are fostered by an appeal to common practice and authority which is not a sound basis for important international information security guidelines (Siponen and Willison, 2009). Therefore, organizations need more specific and validated ISM performance measurements rather than standards.

***2.1.2 Evaluation Based on Financial Measures***

Several studies of ISM have proposed a cost benefit analysis or return on investments (ROI) approach for measuring security investments. These weigh the risks in relation to the value of assets in order to produce a quantitative measure of ISM impact (Erkan, 2005; Mercuri, 2003). Based on quantitative figures that depict the return on security investments, this approach can convince management and decision-makers to invest in information security technology (Erkan, 2005; Nazareth and Choi, 2015). However, neither cost benefit analysis nor an ROI approach is a complete solution since there is no inherent methodology that can be used to effectively quantify security levels (Martin et al., 2011). These traditional performance measurement methods focus on well-known financial measures and are therefore are incapable of describing and managing intangible information assets (Huang et al., 2006; Martinsons et al., 1999) .

Huang et al. (2006) developed a general balanced scorecard (BSC) model of ISM, to build a strategy map which expresses how to link 12 strategy themes to 35 key performance indicators extracted from a proper extension of information security research and guidelines. Then they translated the ISM strategy map into a Scorecard model with four perspectives: financial, customer, internal process, and learning and growth. The linked relationship through the strategic themes of each perspective shows clearly that the objectives for internal processes are to increase financial performance and the objectives for the learning and growth perspective are to support internal processes that help to create financial value. Herath et al. (2010) also established a conceptual framework for strategic implementation of information security performance management using a balanced scorecard approach. Four interrelated perspectives are presented: business value, stakeholder orientation, internal process, and future readiness. Considering that a balanced scorecard for ISM should have a mix of common measures and measures unique to the strategy, they provide a measurement characteristic dimension to the framework. Information security performance would be monitored by periodically reviewing performance measures versus targets from all perspectives.

Based on the use of a BSC to measure ISM performance, these studies have shown that a BSC can provide organizations with results on increasing value by improvements to measures and management insight in business. This can help organizations to assess the value of ISM and how to link ISM performance to business strategies (Herath et al., 2010; Huang et al., 2006). However, approaches that use the BSC model for ISM need further empirical investigation and validation.

## Critical Success Factors of ISM

Organizations need information security management programs to protect their information assets. High implementation and maintenance costs of security controls are increasing the pressure on managers to distinguish between controls their organizations need and those that are less critical. Rational organizations would then focus their limited resources on those things which really make the difference between success and failure. The use of critical success factors (CSFs) is a widely understood concept for identifying important performance requirements upon which the success of the firm depends (Rockart, 1982). CSFs are defined as measures of key areas in the firm that, if they are satisfactory, will assure success within and of the organization (Rockart, 1979). Leidecker and Bruno (1984) define CSFs as a few things that must go right for the business to reach its goals. CSFs may be used by managers as descriptions, predictors, and guidelines for achievement levels (Vedder, 1992). CSFs were one of the earliest and most actively researched management tools (Lee and Ahn, 2008). They have been used as management measures 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), and quality management (Seetharaman et al., 2006), etc. However, CSFs have seldom been used in the information security management field. Since the CSF approach is suitable for analysis at the organizational level, this thesis will apply it to the study of organizational ISM.

The objectives of information security are to preserve an organization’s information assets and the business processes they support, in the context of confidentiality, availability, and integrity (Smith and Jamieson, 2006). ISM is conceptualized as a continuous dynamic decision-making process which involves all crucial components such as organizational infrastructure, human factors and information security practices. Therefore, identifying suitable CSFs for ISM needs a holistic view of the organization. To bridge the gap between literature and practice in the field of information security management, both the information security standards and current literature in IS field are reviewed in this research. As a practical guideline, “Information technology — Code of practice for information security management” which is the main information security standard, simply points out some factors of successful ISM (ISO, 2005). Meanwhile, although a few papers have listed some organizational factors that are critical to the effectiveness of ISM, they did not establish a sound theoretical framework and empirically test and validate it (Chang and Ho, 2006; Smith and Jamieson, 2006; Yildirim et al., 2011). By combining the results of our review, we can identify the socio-organizational issues which are often viewed as critical to the successful implementation of ISM. Based on categories in the literature and standards, we group these issues into five key factors: business alignment, organizational support, organizational awareness, IT competence, and security controls and they are summarized in Table 2.1. Each of these factors is explored in more detail below the table.

Table 2.1 CSFs of Information Security Management

|  |  |  |
| --- | --- | --- |
| **Key Factors** | **Sources** | |
| **ISM Standard[[2]](#footnote-3)** | **Literature** |
| Business Alignment | “objectives and activities that reflect business objectives” (p. xi) | 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” (p. xi) | Aksorn and Hadikusumo (2008), Hu et al. (2012), Kankanhalli et al. (2003), Kayworth and Whitten (2010), Ma et al. (2009), Nazareth and Choi (2015), 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” (p. xi) | Aksorn and Hadikusumo (2008), Smith and Jamieson (2006) |
| Organizational Structuring | “Information security is achieved by implementing … organizational structures...” (p. viii) | Boss et al. (2009), Kayworth and Whitten (2010), Ma et al. (2009), Straub (1988), Straub and Collins (1990) |
| Organizational Awareness |  |  |
| Staff awareness and training | “effective marketing of security to all managers and employees”  “providing appropriate training and education” (p. xi) | Aksorn and Hadikusumo (2008), Culnan et al. (2008), Kayworth and Whitten (2010), Ma et al. (2009), Nazareth and Choi (2015), 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” (p. xi) | Chan et al. (2005), Chang and Lin (2007), (Hu et al., 2012), Martins and Eloff (2002), Nazareth and Choi (2015) |
| IT Competence | Not mentioned | Chang et al. (2011), Eloff and Eloff (2003), Kayworth and Whitten (2010), Stewart (2005), von Solms (2000) |
| Security Controls |  |  |
| Risk management | “a good understanding of the security requirements, risk assessment and risk management” (p. xi) | 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” (p. xi) | Nazareth and Choi (2015), Siponen and Oinas-Kukkonen (2007), Straub and Welke (1998), von Solms (1999), Yildirim et al. (2011) |
| Standards application | “distribution of guidance on information security policy and standards to all employees and contractors” (p. xi) | 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” (p. xi) | Erkan (2005), Herath et al. (2010), Huang et al., 2006, Martin et al. (2011), Martinsons et al. (1999), Mercuri (2003), Nazareth and Choi (2015) |

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 purpose of the alignment of information security with business strategy is to support organizational objectives (Herath et al., 2010).

It is important to integrate information security into mainstream aspects of the business in designing effective ISM. The major challenge is to determine the balance between enabling the business and securing information assets (Kayworth and Whitten, 2010). Strict controls may inhibit business responsiveness, while lax controls may lead to serious risks for information assets. So ISM activities should be driven by organizational objectives, which secure information assets and enable the business simultaneously (Choobineh et al., 2007).

Organizational Support

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

Top management support has been found to be crucial to the success of an organization’s information security efforts (Hu et al., 2012; Kankanhalli et al., 2003; Kayworth and Whitten, 2010; Ma et al., 2009; Nazareth and Choi, 2015; Posthumus and von Solms, 2004; Straub, 1988; Straub and Collins, 1990; Werlinger et al., 2009). The active support of top management was ranked the most important issue and rated number one in priority in Smith and Jamieson’s (2006) survey. Top management is ultimately accountable and charged with the task of initiating and supporting important projects with adequate funding and resources. 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 for dealing with ISM (Straub, 1988). Management must actively support information security efforts at all levels in the organization.

Management must allocate sufficient resources to carry out day-to-day activities to accomplish both short-term and long-term information safety goals. An effective ISM safety program needs an appropriate level of resource commitment including sufficient staff, time, money, information, methods used in safety works, facilities, tools, machines, etc. (Aksorn and Hadikusumo, 2008).

Organizational structure is extremely important to information security management (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. According to Straub (1988), information security can be placed at several levels, both vertically and horizontally in the organization. The vertical perspective is about management reporting level, in which the placement of the information security function should be as high as possible in the organization. The horizontal perspective is about the functional area of primary reporting responsibility, in which the information security function should be in the Information Systems department, or a technologically-advanced Corporate Security department, or in an autonomous entity. Straub and Collins (1990) suggest that a high-level committee should be created to be responsible for setting policy and establishing specific procedures that reduce the information security risk. Kayworth and Whitten (2010) propose a structure including an information security organization, a top security executive (the chief information security officer or CISO), and an internal audit function. Such a structure will help to facilitate the organizational integration needed to achieve security goals and address the importance of information security at the organizational level.

Organizational Awareness

An organization’s information security strategy should address human factors such as security awareness and security training comprehensively. All employees should be made aware of possible security threats, as well as security basics and the literacy which provides 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 supportive reference materials to allow them to protect information assets effectively (Straub and Welke, 1998). In a Yildirim et al. (2011) survey, 70% of employees polled were found to be aware of information security policies in the organizations and some of the employees had participated in IS training.

If there is an inadequate level of user cooperation and a lack of knowledge, employees may misuse or misinterpret certain security techniques and thus become a great threat to the organization’s information security (Van Niekerk and Von Solms, 2010). To avoid this, employees and management must have a good understanding of security risks (threats and vulnerabilities) to the 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. Indeed, security must be effectively marketed to all managers and employees (Von Solms, 1999).

A successful security program can be achieved if all employees are given periodic education and training in order to improve their knowledge and skills on security at work (Aksorn and Hadikusumo, 2008; Nazareth and Choi, 2015). Organizationally sponsored security awareness, training, and education programs create the formal social alignment mechanism that is needed 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, if the proper rules of behavior for using the organization’s information systems are explained by the training program effectively (Culnan et al., 2008).

Using training sessions, employees must be convinced that they truly face information security threats and that these threats can cause serious negative consequences to their organization. They should also understand the user-friendliness and effectiveness of information security policies so that they can believe that complying with these policies will prevent information security breaches (Siponen et al., 2009). Straub and Welke (1998) argue that information security training is an effective way of stressing the two central tenets of general deterrence theory: certainty of sanctioning and severity of sanctioning, as well as the general effectiveness of information security policies.

Training focuses on providing knowledge and skills of information security appropriate to individuals. Ma et al. (2009) suggest a good training program which consists of courses, regular updates, collateral material such as posters, and a system of rewards and penalties for desirable and undesirable behavior. Verbal persuasion, possible security breach examples (Siponen et al., 2009), information security mentoring (Kayworth and Whitten, 2010), and the process of designing security policies (Werlinger et al., 2009) can be used to train and educate stakeholders within organizations. Training can thus increase employee security awareness, understanding and participation (Hu et al., 2012; 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; Hu et al., 2012; Martins and Eloff, 2002; Nazareth and Choi, 2015). This culture exists as the medium between management and organizational behavior, which accounts for success or failure of an organization (Deal and Kennedy, 1982; Douglas, 1985). Culture can guide how employees think, act, and feel, and thus influence the operations of an organization and the effectiveness of its information security practices. Employee attitudes towards information security and how they perceive it will result in certain behaviors (Martins and Eloff, 2002). 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 implementing revised security practices through ISM, by building shared values, beliefs and norms for ISM practices across the entire organization.

IT Competencies

IT competence is an 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 organizational performance and sustainable competitive advantage (Bharadwaj, 2000; Croteau and Raymond, 2004; Dehning and Stratopoulos, 2003; Santhanam and Hartono, 2003). Scholars have emphasized that technical and managerial subjects have similar importance (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 chosen information security technologies (Chang et al., 2011). The enhancement of IT competences has become a critical organizational issue for ISM, which can help strengthen the management of information security.

Security Controls

To achieve an acceptable level of information security, the correct set of security controls must be identified, implemented and maintained. The US National Institute of Standards and Technology classifies information security controls into three categories (Baker and Wallace, 2007): (1) Technical controls, which traditionally include products and processes (such as firewalls, antivirus software, intrusion detection, and encryption techniques), focusing mainly on protecting an organization’s ICTs and the information flowing across and stored in them; (2) Operational controls, which include enforcement mechanisms and methods for correcting operational deficiencies (such as physical access controls, backup capabilities, and protection from environmental hazards); and (3) Management controls, which target information security’s nontechnical areas, such as usage policies and business continuity planning. Security controls development can be a very complicated and resource-intensive process, which requires special resources and expertise (Chang and Ho, 2006). Through our literature review, we identified the following critical security controls: risk management, security policy implementation, and standards application.

Risk management is the effective management and mitigation of a variety of risks to information systems 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. First, information security problems regarding the risk of information security breaches are identified and formulated. Then, risk analysis is conducted to evaluate and prioritize threats inherent in identified problem areas. In phase three, various possible solutions are generated to meet organizational needs specified during the risk analysis phase. In the final phase, appropriate solutions are selected to match the threats (Straub and Welke, 1998). The risk management approach has been recognized as the best way to identify the most effective set of organizational 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). Organizations need to establish policies or countermeasures and implement them to protect information security. In general, information security is the effective implementation of policies that counteract security threats, to ensure the confidentiality, availability, and integrity of information assets (Nazareth and Choi, 2015; 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, 2005). Aiming to provide management direction and support for information security, information security policies should be communicated throughout the organization in a form that is relevant, accessible and understandable to employees.

ISM standards are fundamental compatibility specifications that shape the configuration of information systems (Backhouse et al., 2006). Standards can identify and introduce a set of baseline security controls conducive to an acceptable minimum level of information security for most organizations under normal circumstances (Chang and Ho, 2006; Von Solms, 1999). The objectives of security standards are to offer a common basis for companies to develop, implement and measure effective security management practice (Von Solms, 1999). They can influence how information systems are used and managed (Hanseth and Braa, 2001). Currently, 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 protecting an organization from security threats (Chang and Ho, 2006). Internationally agreed and tested standards must be followed in implementing information security (Yildirim et al., 2011).

According to our review, there has been very little discussion of CSFs in published IS security studies, but their importance relative to ISM performance has also not been studied. Next, we will develop a research model to empirically examine how these success factors can contribute to ISM performance.

# Research Model and Hypothesis Development

## Theoretical Basis

***3.1.1 The Balanced Scorecard for ISM Performance Measurement***

The balanced scorecard (BSC) (Kaplan and Norton, 1992) is a common organizational performance measurement system, which is widely used in practice and has been extensively researched (Marr and Schiuma, 2003). It has been applied in IS domain to measure performance of IT management (Bremser and Chung, 2005; Huang et al., 2006; Kaplan and Norton, 2004).

The basic BSC model was introduced by (Kaplan and Norton, 1993). BSC is built on a framework for selecting multiple performance measures related to the organization’s strategic goals. This supplements traditional financial measures by integrating these measures with non-financial measures reflecting customer satisfaction, internal processes and the ability to learn and grow. In addition, Kaplan and Norton (2004) have proposed cause-effect relationships among the important components of organizational strategy, thereby providing a generic architecture for describing the strategy. Kaplan and Norton’s (1992) original generic BSC model features four perspectives: 1) the financial perspective with strategic financial outcome measures such as return on investment and earnings growth; 2) the customer perspective that focuses on the customer value proposition, customer relationship management, and image; 3) the internal perspective that includes four key areas: operations management, customer management, innovation, and the regulatory and social environment measures; and 4) the learning and growth perspective with performance measures for human capital (skills, training, and knowledge), information capital (systems, databases, and networks), and organizational capital (culture, leadership, alignment and teamwork).

The generic BSC model has been adapted for strategic management and leveraging of IT resources in organizations (Martinsons et al., 1999). In these adapted IT balanced scorecards, there are four suggested perspectives: user orientation (end-user view), business value (management view), internal processes (operation-based view), and future readiness (innovation and learning view). It has been argued that the methods for measuring ISM performance are close to those for evaluating IT performance, so BSC is suitable for measuring intangible assets such as information security management (Herath et al., 2010; Huang et al., 2006). Herath et al. (2010) established a balanced scorecard model for information security (Figure 3.1), but their model has not been empirically validated as yet.

The Huang et al. (2006) BSC framework set up performance indexes for information security management in organizations and attempted to empirically test the resulting model. The study established 35 key performance indicators and focused on the internal relationships among the strategy themes of the four perspectives of the BSC framework. However, there was a lack of solid theoretical support for their research model, and construct development for operationalizing the model was not clearly demonstrated. The authors also called for more empirical studies on BSC based ISM performance assessment. In our study, we adapt the BSC model for evaluation of ISM and empirically verify it.

|  |
| --- |
| Figure 3.1 BSC Model for Information Security  (Herath et al., 2010) |

***3.1.2 System Development Theories in IS Security Risk Management***

Spears and Barki (2010) examine user participation in information systems security risk management (SRM) and its influence in the context of regulatory compliance via a multi-method study at the organizational level. This study found that user participation contributes to improved security control performance through greater awareness, greater alignment between IS security risk management and the business environment, and improved control development (see Figure 3.2).

|  |
| --- |
| Figure 3.2 A Research Model Based on System Development Theories  (Source: Spears and Barki, 2010) |

SRM is defined as a continuous process for identifying and prioritizing IS security risk, and implementing and monitoring controls (i.e., countermeasures and safeguards) that address those risks (Spears and Barki 2010). Effective SRM is expected to result in a system of controls that collectively protect IS security. They adapted two theories of information system development (ISD), i.e. buy-in theory and system quality theory, to examine the outcomes of user participation in the SRM context. With the theoretical support, the authors found that user participation in SRM raises organizational awareness of IS security risks and controls and that user participation contributes to an alignment between SRM and the business context. This in turn contributes to greater organizational awareness of IS security. Both user participation and organizational awareness of SRM contribute to perceived improvements in control development; also both user participation and organizational awareness of SRM positively influence the perceived performance of security controls. In addition, improvements in control development positively influence the performance of security controls.

By applying these two extant theories in ISD, outcomes in the SRM context appear to be improvements in control development (i.e., the design and implementation of IS security controls) and control performance (i.e., greater efficiency and reduced deficiencies in the system of IS security controls). This model uses user participation as a starting point for information security management and focuses on testing the impact of user participation. It also examines the relationship between certain organizational factors of SRM, such as business alignment, organizational awareness, security controls development and security controls performance. According to our literature review, these organizational factors are all critical success factors of an organization’s information security management process. Thus, this model and its empirical examination will be adapted to support our research.

***3.1.3 Strategy Alignment Performance Model***

Alignment between business strategy and IS strategy is believed to improve business performance (Sabherwal and Chan, 2001). Sabherwal and Chan (2001) examined the impact of strategy alignment on perceived business performance using the popular classifications of Defender, Analyzer, and Prospector business strategies (Miles et al., 1978). A theoretical model was developed based on extant strategic IS management literature (see Figure 3.3). Their theory is that IS strategy is concerned primarily with aligning business and information strategies with business needs and using them to derive strategic benefits. Their study empirically investigated the alignment between a company’s IS strategy and business strategy, including the increased likelihood that information systems are more critical to the organization and thus there is an increased likelihood of top management support for IS projects. Greater alignment between an organization’s business strategy and IS strategy indicates that the organization is more likely to utilize IS for a competitive advantage. Thus, the alignment between business and IS strategies helps enhance performance.

|  |
| --- |
| Figure 3.3 Adapted Alignment Performance Model  (Sabherwal and Chan, 2001) |

This model suggests that an organization’s business alignment is positively associated with organizational performance, including both IS success and business success. Consequently, when an organization’s information security strategy is better aligned with the organization’s business strategy, the organization’s ISM will be more successful. According to the foregoing literature review, business alignment can be considered as one of the critical success factors of ISM success and it may be also correlated to other critical success factors. Therefore, this model provides us with a solid theoretical basis to study the relationships among business alignment, other critical success factors and ISM performance, the goal of this study.

## Research Model

Effective organizational information security encompasses the management of three components: people, process and technology (Parakkattu and Kunnathur, 2010). Through literature review, we have identified the critical success factors of effective ISM, which cover all the three components. Business alignment addresses process; organizational support and organizational awareness both address people and process; IT competence addresses both people and technology; and security controls address process and technology. Although individual relevant success factors have previously been identified in different IS security studies, there lacks theoretical model to systematically integrate a well-defined set of factors which are critical to information security management success. Furthermore, their relative importance associated with ISM performance has not yet been studied. Information security management should be viewed from a company’s strategic perspective using a top-down approach. Since no existing ISM theory was found in the current literature, we developed our research model by combining certain characteristics of the three models previously discussed: the Herath et al. (2010) BSC model, the Spears and Barki (2010) SRM model, and the Sabherwal and Chan (2001) alignment performance model.

First, in our model, we focus on the performance of ISM using Herath et al. (2010) BSC model as our model’s output. Spears and Barki (2010) model examines the relationships among certain organizational factors of security risk management, including business alignment, organizational awareness, security controls and security controls performance. However, this model only addresses security risk management, in organization’s information systems development process. Our research will try to study the information security management from an organization’s strategic perspective, investigating the impact of the critical organizational factors on the performance of the whole organization’s information security management. Different from Spears and Barki (2010) model which measures the output only on the performance of security controls, our research model will measure the output on performance of the whole organization’s security management based on Herath et al.’s (2010) balanced scorecard model which has much broader range and is much more comprehensive.

Second, we adopt strategic view from Sabherwal and Chan’s (2001) alignment performance model and using strategic alignment as a starting point. Spears and Barki (2010) model uses user participation as a starting point and focuses on testing the impact of user participation. User participation is not listed as a critical success factor associated with project management for information systems development but lack of user involvement is listed as an important failure factor (Fowler and Horan, 2008). For more than four decades it has been intuitively accepted that user involvement (UI) during system development lifecycle leads to system success. However when the researchers have evaluated the user involvement and system success (UI-SS) relationship empirically, the results were not always positive (Bano and Zowghi, 2015). In our literature review we did not find user participation is widely mentioned as critical success factor to the organization’s information security management thus we did not explicitly include it in our model. Some aspects of user participation can be reflected in organizational awareness, security control and computer competence. To study how an organization can achieve effective ISM performance, our research model will focus on more strategic factors which are critical to the whole organization’s ISM success. According to Sabherwal and Chan (2001) model, strategy alignment positively influences business performance. Thus, business alignment and its impact on organization’s ISM performance will be studied as starting point in our research model.

Finally, all critical success factors previously identified in section 2.2 are included in the resulting research model where they are linked to the performance of information security management. The research model (see figure 3.4) investigates how the CSFs contribute to the success of an organization’s ISM from a top-down strategic implementation perspective. This ISM success model has six constructs: business alignment, organizational support, IT competence, organizational awareness, security controls and ISM performance. Borrowing from the Herath et al. (2010) framework of IT Security Balanced Scorecard (ITSec BSC), ISM performance is considered to have four dimensions: business value, internal process, user orientation, and future readiness.

|  |
| --- |
| Figure 3.4 Research Model |

It is proposed that the performance of ISM is affected by organizational support, organizational awareness, and the implementation of security controls. Organizational support, IT competence and organizational awareness predict the improvements in security controls development. Business alignment determines organizational awareness, IT competences and organizational support, which in turn all affect security controls development. Finally, organizational support also influences organizational awareness.

## Hypotheses Development

An effective information security management 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 being in conflict with business goals because it makes systems less usable and thus impedes the normal business goals of maximizing productivity and minimizing cost (Van Niekerk and Von Solms, 2010). A lack of fit between security objectives and business objectives may lead to the situation where information security policies and budgets do not reflect the needs of the business (Kayworth and Whitten, 2010; Siponen and Oinas-Kukkonen, 2007). In such a case, investment decisions are driven by short-term priorities without well-conceived strategic priorities, and top management may pay little attention to information security (Kayworth and Whitten, 2010).

Information security objectives should be aligned with business strategy. This alignment could 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). Through 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 thereby be more convinced about the importance of information security and more fully appreciate the importance of the ISM processes within the business framework (Smith and Jamieson, 2006; Werlinger et al., 2009). When there is 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 of 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 the necessary resources needed to support ISM. The alignment also helps to establish a formal security structure in which managers at all levels of the organization are more responsible and willing to support sound ISM practices (Chang et al., 2011). Business alignment facilitates organizational support for ISM, suggesting the hypothesis:

*H1: Business alignment positively affects organizational support for 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 an 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 hypothesize:

*H2: Business alignment positively affects an 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 gain alignment with the business environment, organizational awareness of security risks and controls increases. Spears and Barki (2010) found that security policies and procedures that are integrated with business objectives help to focus more attention on information security risks, policies, and related procedures in business processes. This suggests the following hypothesis:

*H3: 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 employees, such as taking training and awareness programs. Previous studies have indicated the positive role of top management in encouraging an organizational security culture (Barling et al., 2002; Chan et al., 2005; Hu et al., 2012; 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, since senior management has the 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 informed about such security problems, and what can be done to prevent them. Organizationally sponsored security awareness, training, and education programs are the primary formal social alignment mechanism for increasing the overall awareness and understanding of information security and thus, employee 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 security risks and policies. This suggests that:

*H4: Organizational support raises organizational awareness of information security risks and controls.*

Organizations need to establish security controls and practice them in order to protect information security. Security controls include security policies and countermeasures that can protect information systems from security risks. Based on General Deterrence Theory, Straub and his research partners categorize information security policies into four distinct, sequential activities: deterrence, prevention, detection, and recovery (Straub, 1990; Straub and Nance, 1990; Straub and Welke, 1998).

Deterrents are passive administrative controls that restrict the use of system resources (Straub and Nance, 1990). Security guidelines and policy statements are examples. Preventive approaches allow only authorized users to access the system. For instance, preventive measures include physical restraints such as locks on computer equipment room doors, and security software such as password protection (Straub, 1990; Straub and Nance, 1990). Detection is “a proactive strategy that involves purposeful investigation of system activity to identify and follow up on possible irregularities” (Straub and Nance 1990, p.46). Detection strategies include recording and tracking unusual activities by randomly scanning files, and exception reporting. Recovery policies remedy the harmful effects of an offensive act and may find and punish the offender(s). Organizations may impose internal sanctions to discipline offenders in the form of warnings, fines, reprimands, and termination of employment. They may report offenses to outside groups and take legal actions such as criminal and civil suits. Technical remedies, like software recovery facilities, are also included in this process (Straub and Nance, 1990; Straub and Welke, 1998).

Security controls development is a dynamic process. Risk analysis should first be conducted to identity threats inherent to IS security. Based on the identified risks, compliance enforcement and monitoring measures such as security policies, protective countermeasures, and protective procedures are established. Further adjustments to controls can be accomplished through feedback from the organization. Spears and Barki (2010) indicate that there are two components of a security control development: its design and performance. The design of a control is evaluated to determine if it is appropriate to mitigate a particular security risk. The performance of a control is assessed to determine if it is functioning as designed. Organizational support contributes to improvements in control development by providing needed information and resources to control designers. With organizational support, employees are trained to use the controls and may provide valuable feedback on whether or not the controls could feasibly be performed in the business environment. Based on feedback, controls can be modified as needed.

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 such improvements. A formal security structure facilitates setting policy and establishing specific procedures that reduce information security risks (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 hypothesize that:

*H5: Organizational support positively affects information security controls.*

Technical IT resources provide the organization with an effective technology base, and competent IT staff with proficient IT skills are intangible resources that operate the technical IT resources (Ross et al., 1996). Such IT competences influence the ability of an organization to deploy and to utilize IT and thus help the organization to apply information technologies in the security controls development processes (Chang et al., 2011). On the one hand, information security controls include technical controls such as firewalls, antivirus software, intrusion detection, encryption techniques, etc. The organization’s IT capabilities are essential to the implementation of these technical controls. On the other hand, operational security controls (e.g. access controls, backup mechanisms) and security management controls (e.g. usage policies) are also supported by information technologies. Thus, the effectiveness of information security controls is influenced by the organization’s IT competence, suggesting the following hypothesis:

*H6: IT competences positively affect 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, 2005). Empirical evidence indicates that it is 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 greater awareness gained by users enables control designers to implement security controls more consistently (Spears and Barki, 2010).

Employees have their own individual attitudes towards information security in the organization. These attitudes could be positive or negative and will result in certain behavior (Martins and Eloff, 2002). Employee behaviors directly influence the implementation of security controls. If they feel negative about a security policy and do not accept it, the policy will fail to be effective. Thus, fostering an organization’s information security culture and aligning employee behaviors with such a culture is one way to ensure the effectiveness of security controls development (Hu et al., 2012; Von Solms and Von Solms, 2004). All these suggest that security controls implementation improves when there is greater organizational awareness.

*H7: Organizational awareness positively affects 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 the senior managers who control 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 found empirically that the greater top management support is, the more effective information security is in organizations, as more resources are spent to prevent security incidents (Werlinger et al., 2009). Top management is also charged with developing effective and efficient organizational structures (Straub, 1988). If top executives perceive information security as a technological issue, the information security group tends to be positioned at a low functional level in organizations (Kayworth and Whitten, 2010). 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 organizational integration to achieve security goals and further address the importance of information security at the organizational level, thus improving the effectiveness and efficiency of security controls (Boss et al., 2009; Kayworth and Whitten, 2010; Straub, 1988; Straub and Collins, 1990). Hence, organizational support can directly affect ISM performance.

*H8: Organizational support positively influences the performance of ISM.*

Organizational training is the primary way of communicating information security policies, measures, procedures, and requirements across the organization, if the proper rules of behavior for using the organization’s information systems are explained effectively by the training program (Culnan et al., 2008). Through training sessions, employees must be convinced that they truly face information security threats and these threats can cause serious negative consequences to their organization. They should also understand the user-friendliness and effectiveness of information security policies so that they can believe that complying with these policies will help prevent security breaches (Siponen et al., 2009). Straub and Welke (1998) argue that information security training is an effective way of stressing the general effectiveness of information security policies.

The security culture of an organization may have a huge impact on the performance of ISM. The success of ISM requires a positive attitude to information security throughout the whole organization (Vroom and Von Solms, 2004). Prior studies have found that forming an atmosphere and culture is imperative for organizations to achieve the goal of effectiveness (Boggs, 2004; Denison et al., 2004; Yeh et al., 2006). Chang and Lin (2007) also emphasize the importance of security culture to the success of information security initiatives.

Organizational awareness can result in making employees aware of the organization’s information security risks, and the potential damage they can cause. Employees must also be made aware of information security policies, procedures and countermeasures existing in the company. If employees lack knowledge about security controls, they may misuse or misinterpret them, causing the security controls to 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 stronger 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 of the security management system (Spears and Barki, 2010). We therefore hypothesize that:

*H9: Organizational awareness positively influences the performance of ISM.*

A clearly defined set of policies regarding proper and improper use of the information system is a precondition to implementing the effective security management (Straub, 1990). Better designed and implemented controls will result in better control performance from fewer errors or increased efficiency (Spears and Barki, 2010). Both scholars and ISM standards developers have asserted that information security will be achieved only if a correct set of security controls is identified, implemented and maintained (Chang et al., 2011; Chang and Lin, 2007; ISO, 2005). In order to determine whether information security management is meeting its goals, the organization needs to measure the progress of all organizational 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).

*H10: Effective security controls positively influences the performance of ISM.*

In summary, with business alignment, organizational support, IT competences, and organizational awareness of security risks and controls, the preceding ten hypotheses maintain that information security controls can be effectively developed, resulting in successful information security management.

# Methodology

A multi-method approach was chosen based on the premise that separate and dissimilar data sets drawn from the same phenomenon would provide a richer picture of the concept than would a mono-method approach (Spears and Barki, 2010). This study included three phases: a qualitative study, a pilot study, and the final full empirical study. A combination of data collection and analysis methods were used on separate samples to examine how the critical success factors of ISM affect ISM performance. In the first phase, interviews were conducted with IT professionals who had worked on information security management, in order to discern key information from practitioners about critical factors that make ISM effective and about ISM performance measurement. This information was then used to confirm the CSFs abstracted from prior literature and to aid in research instrument development. In the second phase, a pilot study was used for refining and validating the measurement scales derived partly from existing scales which were adapted to the context of ISM. In the third phase, statistical data were collected in a field survey that reflected the hypothesized research model of Figure 3.4 and subjected to SEM analyses for validating the model. Participation in the study was voluntary. Prior literature has indicated that it is nearly impossible to extract information about the actions of security practitioners from business organizations without including a major supporter of security in that organization in that discussion, because there is almost always a general mistrust of any ‘‘outsider’’ attempting to obtain security-related data from the organization (Kotulic and Clark, 2004). Due to the sensitivity of the topic and the difficulty of reaching IT managers directly, participants were recruited by a commercial market research company[[3]](#footnote-4). This company has provided high quality data from online sample surveys since 2005, so it qualifies as a trustworthy survey company for the purposes of data collection in this study. Potential online participants are recruited over a period of time by the company, along with demographic data from each person. This is stored in the research company’s database, and participants who matched our stated requirements were informed by the company about the survey, and that they could participate as they wished. Each participant is compensated through points they receive and prize draws in which they were included. We paid the market research firm an amount based on the number of usable participant responses collected.

## Measurement development

All constructs were measured by multiple items. As very limited empirical studies have been done on ISM at the organization level, few predefined scales were found for the social-organizational factors of ISM. Thus, new multiple-item scales were constructed for this study. Wherever possible, initial scale items were taken from validated measures in the existing literature, reworded to relate to the context of information security management. The items were scored on a five-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree).

Constructs can be reflective or formative, depending on the relationships between measurement items and constructs (Petter et al., 2007). In most cases constructs are assumed to be reflective, meaning that the measurement items are a reflection of the construct. Reflective measures should be unidimensional and the correlation between any two measures should be positive (Bollen and Lennox, 1991). However, formative constructs are sometimes used when the items describe and define the construct (Petter et al., 2007). Formative constructs are a composite of multiple measures which capture differing aspects of the constructs to which they belong (MacCallum and Browne, 1993). A formative construct should be developed when multiple sub-constructs and measurement items are necessary to fully capture the entire domain of the construct (Petter et al., 2007). Thus, in this study, one construct was operationalized with formative items, according to results from the literature review.

Prior IS security literature has indicated that effective ISM must be in alignment with organizational objectives, business requirements, and relative business value (Spears, 2005; Suh and Han, 2003). I developed two items of business alignment from the Spears and Barki (2010) research, with modifications to adapt them to the information security management context. A new item was developed based on results from the literature review. As a result, business alignment was measured via three reflective items: (1) the extent to which security management objectives reflect business objectives; (2) the extent to which security policies and controls are based on business objectives, value, or needs; and (3) the extent to which business users routinely contribute a business perspective to information security management.

No predefined scales were found for organizational support. According to the literature review, organizational support includes top management support, commitment of funding and resources, and organizational structuring. As such, three reflective items were developed to measure organizational support: (1) the extent to which top management commits to information security management; (2) the extent to which sufficient funding and resources are allocated to information security management; and (3) the extent to which a formal organizational structure for information security is established.

Organizational awareness is conceptualized as a state that is reflected in the behavior of employees, including a raised consciousness of and an enhanced adoption of security policies and countermeasures (Spears and Barki, 2010). Measures for organizational awareness were taken from research by Spears and Barki (2010), adapted to an information security management context. Two new items were developed: one to measure organizational security education and training programs and a second one to measure employee consciousness of security threats. Thus, organizational awareness was assessed with four reflective items: (1) Formal information security educational and training programs provided to employees; (2) heightened awareness of potential security threat that the organization faces and the need for ISM; (3) heightened awareness of policies, procedures, or countermeasures for information security; and (4) the extent to which employees exhibit a sense of proactiveness in protecting information security.

IT competence refers to the ability of an organization to deploy and to utilize IT in a manner that can help the organization apply information security technologies (Chang et al., 2011). Items for this construct were derived from Chang et al. (2011) and Croteau and Raymond (2004), summarizing IT resources, IT staff, and IT operations. As such, the IT competence construct was measured by three formative items: (1) the extent to which the organization’s IT resources (e.g., networks, hardware, software, etc.) are available and flexible; (2) the extent to which IT staff is knowledgeable and capable of developing and maintaining information security technologies; and (3) the extent to which the end users of IT systems follow sound operations processes.

For the purposes of this research, security controls refers to the design and implementation of information security controls which include risk management, security policies, and ISM standards application. In the Spears and Barki (2010) research on user participation in information systems security risk management, control development was assessed as perceived improvements that had occurred in the definition or implementation of access control, segregation of duties, and security policy. In the context of overall organizational information security management, this study measured security controls development by three reflective items: (1) the extent to which a formal risk management program has been designed and implemented; (2) the extent to which formal security policies have been defined and implemented; and (3) the extent to which specific ISM standards have been applied.

Based on Herath et al. (2010) and Huang et al. (2006) studies, ISM performance is considered from four perspectives: business value, internal process, user orientation, and future readiness. The ideal performance measures for the BSC model should be as objective, verifiable, and auditable as possible. However, some scholars have argued that subjective measures are often unavoidable and may have to be included in the measurement (Herath et al., 2010). Our ISM performance model will use subjective measures which investigate related subject perceptions.

Information security is emerging as a value creator which is related to the protection of valuable information assets against loss, improper disclosure or damage while in storage, transmittal or processing (Herath et al., 2010). The importance of value has been highlighted in various fields such as decision-making (Keeney, 1994), security planning (Straub and Welke, 1998), knowledge management (Spender, 1998) and assessing company innovation capability (Wheeler, 2002). The value proposition associated with information security can be defined as the net benefit and cost of maintaining information security in the organization (Dhillon and Torkzadeh, 2006). ISM should accomplish value delivery, i.e., it should optimize investments in information security to achieve organizational objectives (Herath et al., 2010). Therefore, the business value construct of ISM was assessed by the following three items: (1) perceived cost-effectiveness, the extent to which the benefit of ISM is greater than cost; (2) the extent to which ISM has contributed value to organization as whole; and (3) the extent to which top management is satisfied with the implementation of ISM.

Information security management needs to consider different types of users and stakeholders while providing information security services (Herath et al., 2010). Prior studies have emphasized the importance of understanding individual stakeholder assumptions and values for successfully dealing with organizational changes (Orlikowski and Gash, 1994; Simpson and Wilson, 1999). The main stakeholders of an organization’s ISM are employees and customers. Employee behaviors are an important part of enterprise-wide information security. Organizational practices also have to be secure enough to satisfy customers (Herath et al., 2010). Thus, the user orientation related ISM performance construct can be assessed by measuring three items: (1) the extent to which employees comply with information security policies; (2) the extent to which employees strengthen transaction security; and (3) the extent to which customers are satisfied with the organization’s information security practices.

Internal processes relate to planning, acquiring, deploying, and maintaining information security practices and services. These processes include managing requests from all users and stakeholders, providing routine operations management, and providing training for end users (Herath et al., 2010). ISM standards have indicated that all security procedures within an area of responsibility should be verifiably carried out correctly (ISO, 2005). In addition, all areas within the organization should be considered for regular review to ensure compliance with security policies and standards. Thus, from an internal process perspective, ISM performance was assessed by three items: (1) the extent to which the processes of planning and implementing ISM have been improved; (2) the extent to which information security policies are effective and efficient; and (3) the extent to which ISM standards compliance has been improved.

Adapted from the Kaplan and Norton (2004) BSC model, the future readiness perspective can also be explained as a learning and growth perspective, which involves priorities to create a climate that supports organizational change, innovation, and growth (Huang et al., 2006). From a future readiness perspective, continuous training of employees on information security threats, countermeasures and policies is necessary. Further, information security staff should also proactively think of the occurrence of new threats and the countermeasures to deal with them (Herath et al., 2010). The ISM performance construct on future readiness was thus measured by: (1) the extent to which the organization’s ISM provides continuing information security training to employees; (2) the extent to which the organization’s ISM prepares for potential changes and challenges; and (3) the extent to which the organization’s ISM is positioned to meet future needs.

In summary, this study measures ISM performance by four items according to the four perspectives: (1) perceived cost-effectiveness, the extent to which the benefit of ISM is greater than cost; (2) the extent to which employees comply with information security policies; (3) the extent to which information security policies are effective and efficient; and (4) the extent to which the organization’s ISM is positioned to meet future needs.

Given the importance of establishing content validity for all constructs, several methods were applied before data collection started. First, as mentioned above, I have scoped the domain of the constructs via literature review. Then, following guidelines for validating constructs (Petter et al., 2007), we have used expert validation to evaluate if the measures can be categorized as per the theoretical predictions. One professor who has much experience in information security research reviewed all the items. Some items were modified or rephrased. After that, I interviewed two information security managers (one from a university and the other from a government ministry) for their opinions on effective ISM and the related success factors (Interview questions in Appendix 3). These interviews confirmed the measurement items.

All the measurements for each of the constructs are summarized in Table 4.1.

Table 4.1 Construct Measures

|  |  |  |  |
| --- | --- | --- | --- |
| **Construct** | | **Item** | **Source** |
| Business Alignment (BA)  (Reflective) | | My organization’s information security management objectives reflect business objectives. | Self-developed |
| My organization’s security policies and controls are based on business objectives, value, or needs. | Spears and Barki (2010) |
| In my organization, business users routinely contribute a business perspective to information security management. | Spears and Barki (2010) |
| Organizational Support (OS)  (Reflective) | | In my organization, top management actively supports information security management as a vital enterprise-wide function. | Self-developed |
| In my organization, sufficient funding and resources are allocated to information security management. | Self-developed |
| A formal organizational unit for information security is established within my organization. | Self-developed |
| Organizational Awareness (OA)  (Reflective) | | In my organization, information security educational and training programs are provided to employees periodically. | Self-developed |
| In my organization, employees are aware of potential security threats and understand the need for information security management. | Self-developed |
| In my organization, employees are aware of policies, procedures, or countermeasures for information security. | Spears and Barki (2010) |
| In my organization, employees exhibit a sense of proactiveness in protecting information security. | Spears and Barki (2010) |
| IT Competence (IC)  (Formative) | | My organization’s IT resources (e.g., networks, hardware, software, etc.) are available and flexible. | Chang et al. (2011), Croteau and Raymond (2004) |
| In my organization, IT staff (both inbound and outsourced) is knowledgeable and capable of developing and maintaining information security technologies. | Chang et al. (2011) |
| In my organization, end users of IT systems follow sound operation processes. | Chang et al. (2011) |
| Security Controls (SC)  (Reflective) | | In my organization, a formal risk management program has been designed and implemented. | Self-developed |
| In my organization, formal security policies have been defined and implemented. | Self-developed |
| In my organization, specific ISM standards have been applied to enhance information security management. | Self-developed |
| ISM Performance (IP)  (Reflective) | | My organization’s ISM is cost-effective, i.e., the cost is justified by the potential benefit. | Self-developed |
| In my organization, employees comply with information security policies. | Self-developed |
| My organization’s information security policies are effective and efficient to protect information asset. | Self-developed |
| My organization’s ISM program is positioned to meet future needs. | Self-developed |
|  | Business Value | My organization’s ISM is cost-effective, i.e., the cost is justified by the potential benefit. | Self-developed |
| My organization’s ISM has contributed value to organization as whole. | Self-developed |
| In my organization, top management is satisfied with the implementation of ISM. | Self-developed |
| User Orientation | In my organization, employees comply with information security policies. | Self-developed |
| In my organization, employees have strengthened transaction security. | Self-developed |
| Customers are satisfied with my organization’s information security practices. | Self-developed |
| Internal Process | The processes of planning and implementing ISM have been improved in my organization. | Self-developed |
| My organization’s information security policies are effective and efficient to protect information asset. | Self-developed |
| ISM standards compliance in my organization has been improved. | Self-developed |
| Future readiness | My organization’s ISM program provides continuing information security training to employees. | Self-developed |
| My organization’s information security management program prepares for potential changes and challenges, such as social networking, BYOD (Bring Your Own Device), and outsourcing. | Self-developed |
| My organization’s ISM program is positioned to meet future needs. | Self-developed |

## Qualitative Study

After the literature review, I interviewed two information directors who were in charge of the security management of their organizations’ information systems. One manager worked at a university with over 10 thousand students, and the other one was from a government ministry. Interviews were conducted with a set of open questions regarding the critical success factors of ISM and their organizations’ ISM performance measurement.

First, the interviewees were asked about their organizations’ current information security policies and measures to protect information security. Both of them stated that their organizations had relative good security policies. One manager expressed satisfaction with his/her organization’s current policies and measures, while the other pointed out some limits to his/her organization’s policies and the need for improvement.

“There are written security policies, but lack of effective implementing measures. Many policies are developed to remedy after breaches happening, but not to prevent the security threat.”

“There is a full portfolio of security standards and policies set out by a dedicated security branch. There are also different processes to enforce the security policies.”

Next, the interviewees were asked how they measured the performance of their organizations’ information security management. Both managers answered that there were no specific ISM performance measures. The two organizations used quite simple criteria to assess their information security performance ---- the fewer system breaches occurred, the higher was information security performance. Their focus was mainly on the working status of their organizations’ information systems. If the information systems could work smoothly without any breach, the organization’s ISM was regarded as satisfactory. They did not consider developing more comprehensive ISM performance measurements.

“It is quite well done. There have been very limited media exposure against information security breach(es).”

“The performance of information security management is mainly assessed by whether there are breaches or not. The fewer breaches, the higher ISM performance.”

Then, both were asked “What factors do you think are critical to the success of your organization’s information security management?” The managers differed in their focus for this answer. One manager said that two factors are critical to the success of ISM ---- support from top management, which can guarantee the sufficient organization resources, and the information security staff’s technical competence which can solve security problems at the technological level. The other manager mentioned more factors such as business alignment, information security controls and employee education. He emphasized that the organization needed comprehensive security controls to achieve ISM success. Their controls included applying security standards, developing security policies, following specific processes to protect classified information, using security related products, and implementing secure information system architecture.

“The most important factor is top management commitment. It decides how much organization resources can be assigned to information security management. Sometimes investing resources into security management may not be able to bring obvious performance improvement. Only if the top management realizes that importance of information security, they are willing to support security management and assign organization resources. Another factor is the information security staff’s technical competence. Most security risks happen at the technological level of the system. Whether such security risks or problems can be prevented or thoroughly solved highly depends on the technical abilities of the security staff who implement the information security measures.”

“Information security is an integral part of overall organizational objectives. It affects almost every area of the business. I think the very critical factors include security standards, security policies, processes to safeguard classified information, security related products, a secure by default architecture, and more education to personnel.”

Finally, they were asked to state their opinions about what should be improved for their organizations’ information security management. They each expressed one concern on one critical factor improvement. One manager expected more support from top management and the other one stated a need for better security education and training to employees.

“I hope our top management is willing to assign more organization resources to information security management, including human resources and financial resources.”

“We need better communications of information security related policies and better education to employees.”

These interviews demonstrate that information directors’ views on critical success factors are consistent with what I abstracted from the literature review. The main CSFs they mentioned were business alignment, top management support, organizational security education and training, technical competence, and formal information security controls. These results confirm the constructs proposed for the research model, and provide support for survey questionnaire design.

## Pilot Study

After the initial development process, a pilot study was conducted to validate the instrument and to do a preliminary test of the proposed research model. The model was developed to test the validity of a set of hypotheses in information security contexts at an organizational level of analysis. Organizational level data can be gathered from managers who can describe intra- (and/or inter-) organizational behavior (Massetti and Zmud, 1996). Thus participants were Chief Information Officers (CIOs), Chief Security Officers (CSOs), IT managers, information security managers, and senior IT staff from different geographical areas. All participants from these classes of employees had to be presently involved with decision making regarding their overall company's information security before being invited to participate in the survey. An online survey was conducted because of its advantages over traditional paper-based mail-in surveys: (1) the sample is not restricted to a specific geographical location so that large samples are possible, (2) costs are lower, and (3) faster responses are obtained (Bhattacherjee, 2001). A total of 99 usable responses were obtained through Empanel Online[[4]](#footnote-5), a commercial market research company. Prior to analysis, all variables were examined through various SPSS programs. The accuracy of data entry was checked and no missing values were found through data screening.

The preliminary consistency and reliability of reflective multi-item scales was first established with Cronbach’s alpha scores. The scores for five were acceptable (αBusiness Alignment = 0.704, αOrganizational Support = 0.731, αOrganizational Awareness = 0.814, αSecurity Controls Development = 0.703, and αPerformance = 0.815), being greater than 0.70, the conventional standard for acceptable reliability (Nunnally, 1987). Cronbach’s alpha estimate for the formative construct, IT Competence, was 0.563. As formative measures examine different facets of the construct, internal consistency or reliability is unimportant. It has been suggested that formative measures should not have strong correlations with one another because excessive multicollinearity in formative measures can destabilize the construct (Petter et al., 2007). Follow Petter et al. (2007) guidelines, the VIF (variance inflation factor) statistic can be applied to determine if the formative measures are too highly correlated. VIFs for each item of the formative construct, IT Competence, were as follows: 1.090, 1.250, 1.236. These VIFs suggested that multicollinearity was not a concern as all the VIFs were less than 3.33 (Diamantopoulos and Siguaw, 2006).

Construct validity (discriminant validity and convergent validity) was tested with the confirmatory factor analysis (Applegate et al.) technique. Loadings of items should be at least .40 and there should be no cross-loading of items above .40. As a result of the CFA test, all items of the five reflective constructs were satisfactory and subsequently no item was dropped from the item pool. A partial least squares (PLS)-based confirmatory factor analysis (Applegate et al., 1996) was also completed to test the reliability and validity of the instrument. The measurement model of a PLS analysis provides indices for assessing convergent validity and discriminant validity of the scale. Convergent validity is generally achieved if three criteria are met (Fornell and Larcker, 1981): 1) all item factor loadings should be significant and greater than .70; 2) the average variance extracted (AVE, the amount of variance captured by a latent variable relative to the amount caused by measurement error) should be greater than .50 (or square root of AVE > .707); and 3) the composite reliability index for each construct should be greater than .80. Based on these criteria, the PLS results indicated that a satisfactory level of convergent validity was achieved. All item loadings of the five reflective constructs were greater than .70. In addition, all item loadings were significant (p< .001). Furthermore, the square root of AVE was greater than .707 for each construct. The composite reliabilities of all reflective constructs also met the minimum criterion of .80.

Since the measures of formative constructs are not normally highly correlated, common factor analysis, which focuses on common variance and is the method used for determining construct validity with reflective constructs, is useless for formative constructs (Rossiter, 2002). Instead, principal components analysis was applied to examine the item weightings for measures to assess formative construct validity (Petter et al., 2007). The weightings for the three items of IT competence were all significant at 0.387 (p<0.001), 0.490 (p<0.001), and 0.482 (p<0.001) respectively. When the full research model was tested statistically using PLS the average path coefficient (APC) was 0.396 (p<0.001), the average R-squared (ARS) was 0.580 (p<0.001), and the average variance inflation factor (AVIF) was 3.293 (acceptable if <= 5, ideally <= 3.3). Therefore the overall model fit was good.

These analyses suggested that the scales of the five reflective constructs and the one formative construct were reliable and valid. All items were kept without modification, which retained content validity. The final pool contained three items for business alignment, three items for organizational support, four items for organizational awareness, three items for IT competence, three items for security controls development, and four items for ISM performance (see Table 4.1).

## Final Study

As the pilot study did not result in any change in the measurement instrument, the 99 data cases from the pilot study were included in the data set for the final study. After the pilot study, we delegated the commercial survey company to complete our online survey. Participants were Chief Information Officers (CIOs), Chief Security Officers (CSOs), IT managers, information security managers, and senior IT staff from different geographical areas. All participants were presently involved with decision making regarding their company's information security.

After full data collection, the research model was tested using the partial least squares (PLS) approach, a latent structural equation modeling technique. I selected PLS because: (1) it has the capacity to estimate both the structural model and the measurement model simultaneously, (2) as a component-based structural equation model (SEM), it can analyze a model that includes both formative and reflective indicators, and (3) it has minimal demands on sample size, measurement scales, and residual distributions (Chin, 1998; Lee and Larsen, 2009). The software I used was WarpPLS 4.0[[5]](#footnote-6), which is very easy to use for validating the measurements and testing the hypotheses of a SEM model. It provides users with a wide range of features. It also explicitly identifies nonlinear functions connecting pairs of latent variables in SEM models and calculates multivariate coefficients of association accordingly (Kock, 2013).

The evaluation of an SEM model includes two steps: (1) the assessment of the measurement model, and (2) the assessment of the structural model (Chin, 2010). The measurement model shows how items relate to their respective constructs or latent variables (Chin, 1998). The evaluation of the measurement model focuses on the reliability and the validity of the measures used to represent the model’s constructs. Tests performed to evaluate the constructs include item reliability, construct reliability, convergent validity and discriminant validity. The structural model is evaluated to test the hypotheses of the SEM model, which determines whether there is evidence to support the theoretical model. Analyses are conducted to test the goodness of model fit, which include R2 for endogenous variables, path coefficients significance and goodness of fit (GoF) index. All analyses performed are presented in Chapter 5.

## Summary

This chapter presented overall research procedures, measurement scale development and the research methodologies employed in this study. Based on the foregoing literature review, the measurement instrument utilized in this study was developed and supported by qualitative interview studies. A pilot study was conducted to validate the instrument and do a preliminary test of the proposed research model. The analysis of the pilot study data indicated that the instrument is sufficiently reliable and valid. Finally, analyses of the final study were described, which include the procedures to validate the hypothesized theoretical models. All details and results of the analyses performed in the final study are presented in the next chapter.

# Data Analysis and Results

## Data Collection

As introduced in the previous chapter, the targeted population of this study was managers who are presently involved with decision making regarding their company's information security. Data were collected through an online survey hosted by the Empanel Online Company. The letter of information and a consent form were presented to participants, and they were required to electronically approve consent before starting the survey. Only those who agreed to participate could enter the online survey. One screening question, “Are you working as an information security officer or involved with decision making regarding your company's information security”, was used to qualify the participants to respond to the survey questions. The letter of information, consent form and the survey are shown in Appendix 1 and Appendix 2 respectively.

Participants for both pilot and final studies were recruited by a commercial market research company, Empanel Online. The pilot study was conducted from December 26, 2013 to January 4, 2014. There were 99 valid responses obtained. Since there was no change in the measurement instrument and questionnaire, the 99 data cases from the pilot study were included in the data set of the final study. Participants in the final study were recruited between January 7, 2014 and January 14, 2014. In total, there were 503 IS professionals attempted to fill the survey, but 190 participants were filtered by the first screening question. Therefore, including the 99 pilot study responses, we finally received a total of 313 responses from qualified IS managers.

## Data Screening

To determine whether the responses collected online were valid and to screen out unusable data, the following procedures were carried out. First, there were two screening questions to assure that participants had answered all questions attentively but not filled the survey only with the purpose of collecting incentives. The two screening questions were mixed with the survey questions, asking the participant to choose a specific answer (see question 19 and 32 in Appendix 2). It was believed that those participants who did not answer the screening questions correctly were inattentive participants. Thus 81 invalid responses were removed and there were 232 samples that could be used.

Second, we detected outliers, which are “cases with extreme or unusual values on a single variable (univariate) or on a combination of variables (multivariate)” (Meyers et al., 2006, p.65). IBM SPSS Statistics version 22 was used to search for outliers. For all the reflective constructs in the research model, composite values were calculated and converted into standardized scores. Composite scores were not created for the formative construct as these items do not share the same theme or have the same content (Petter et al., 2007). Therefore, values of each individual indicator of the formative construct, IT competence, were converted into standardized scores. Then box plots for all reflective variables and formative construct indicators were created to identify the outliers. A total of 13 unique cases were detected as outliers (representing 5.6% of the total number of cases). These cases were deleted from the data set since there was no known explanation for them (Meyers et al., 2006). A summary of the deleted outliers is shown in Table 5.1. Separate box plots for all individual reflective constructs and formative indicators can be found in Appendix 4.

Table 5.1 Summary of Outliers

|  |  |  |  |
| --- | --- | --- | --- |
| **Construct** | **Outlier Case ID** | **Number of Outliers** | **Number of New Outliers** |
| Business Alignment | 50, 140, 184 | 3 | 3 |
| Organizational Support | 17, 50, 130, 140 | 4 | 2 |
| Organizational Awareness | 50, 184, 187 | 3 | 1 |
| Security Controls Development | 50, 140, 145, 167, 179 | 5 | 3 |
| ISM Performance | 67, 116, 140 | 3 | 2 |
| IT Competence  -IT Resources | 37, 176 | 2 | 2 |
| IT Competence  -IT Staff | 116, 184 | 2 | 0 |
| IT Competence  -End Users | 50, 179 | 2 | 0 |
|  |  | **Total** | 13 |

As a result of the above data screening procedures, a usable data set of 219 cases was obtained for testing the theoretical model. Using a regression heuristic of 10 cases per predictor, the sample size requirement should be 10 times either one of the following, whichever is the greater (Chin, 1998): (1) the block with the largest number of formative indicators, or (2) the dependent variable with the largest number of independent variables impacting it. Thus the sample size of the current study (N = 219) is sufficient.

## Demographics

As some demographic questions were included in the survey, the demographic characteristics of the participants were summarized. All participants were senior IT managers who were involved with decision making regarding their companies’ information security. Table 5.2 shows the distribution of participants’ job positions. From the pool of participants, about one third was from top management (24.7% Chief Information Officers and 11% Chief Security Officers). Most participants were IT managers (39.7%). Of the rest, 10% were information security managers and 10.5% were senior IT staff. About 4.1% of the participants chose an option of “Other”, and indicated their job positions as “IT Director”, “IT Support Specialist”, “IT Administrator”, “CTO”, and “IT analyst”.

Table 5.2 Job Positions of Participants

|  |  |  |
| --- | --- | --- |
| **Job Position** | **Count** | **Percentage** |
| Chief Information Officer (CIO) | 54 | 24.7% |
| Chief Security Officer (CSO) | 24 | 11.0% |
| IT manager | 87 | 39.7% |
| Information security manager | 22 | 10.0% |
| Senior IT staff | 23 | 10.5% |
| Other | 9 | 4.1% |
| **Total** | **219** | **100%** |

Participants were asked to indicate their organizations’ industry type, from ten possible options. Most participants indicated that they were in a technology industry (29.7%) and manufacturing industry (22.4%). The rest were distributed in other industries. About 6.4% of the participants chose the option of “Other” and categorized their organizations into different industries such as “Construction”, “Non-profit”, “Services”, “Logistics”, “Aerospace”, “Engineering”, and “Real Estate”. Table 5.3 shows the industry variety of the participants.

Table 5.3 Industry Type

|  |  |  |
| --- | --- | --- |
| **Industry** | **Count** | **Percentage** |
| Manufacturing | 49 | 22.4% |
| Retail and distribution | 18 | 8.2% |
| Financial Services | 21 | 9.6% |
| Technology | 65 | 29.7% |
| Health | 23 | 10.5% |
| Telecommunication | 14 | 6.4% |
| Travel, leisure and entertainment | 1 | 0.5% |
| Education | 8 | 3.7% |
| Utilities, energy and mining | 4 | 1.8% |
| Government | 2 | 0.9% |
| Other | 14 | 6.4% |
| **Total** | **219** | **100%** |

Among the total of 219 participants, 216 indicated that their companies were in North America. Only 2 were from Europe and 1 was from South America. These three participant responses were kept in the data set as this small difference was not expected to affect results from the majority in North America. Table 5.4 shows that 58.4% of the organizations were domestic and the rest were international organizations. In terms of organization size, Table 5.5 shows that most participants worked in large organizations. About 42.9% indicated that there were more than 500 employees in their organizations and 32.4% were in an organization with between 201 and 500 employees. 16.5% worked in medium-sized organizations with between 51 and 200 employees. Only 8.2% of the participants were from small organizations with fewer than 50 employees.

Table 5.4 Organization Type

|  |  |  |
| --- | --- | --- |
| **Organization Type** | **Count** | **Percentage** |
| Domestic | 128 | 58.4% |
| International | 91 | 41.6% |
| **Total** | **219** | **100%** |

Table 5.5 Organization Size

|  |  |  |
| --- | --- | --- |
| **Organization Size** | **Count** | **Percentage** |
| 1-50 | 18 | 8.2% |
| 51-200 | 36 | 16.5% |
| 201-500 | 71 | 32.4% |
| Above 500 | 94 | 42.9% |
| **Total** | **219** | **100%** |

It is worth mentioning that participants were asked if their organizations applied any national or international information security standards. About 68% of the participants answered “No” and 32% answered “Yes”. Through an open-ended question, the participants also specified the information security standards that had been applied in their organizations. Responses included “ISO/IEC 13335”, “ISO9000”, “COMP TIA Security+”, “ISO4000”, “NIST”, “CISA”, “ISO 27001”, “ISO 17799”, “HIPAA”, “ISC”, etc.

Table 5.6 Security Standard Application of Organizations

|  |  |  |
| --- | --- | --- |
| **Applied Security Standard** | **Count** | **Percentage** |
| Yes | 70 | 32.0% |
| No | 149 | 68.0% |
| **Total** | **219** | **100%** |

## Descriptive Statistics

A summary of descriptive statistics for all the constructs is shown in Table 5.7, including skewness and kurtosis values for each construct. These results indicate that responses were not normally distributed in this study. Considering that normality is not always required for analysis and that PLS imposes minimum demands in terms of variable distributions (Chin, 1998), the non-normal distributions in the research model were not deemed problematic for model testing and analysis.

Table 5.7 Descriptive Statistics of Constructs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Construct** | **Mean** | **Std. Dev.** | **Skewness** | **Kurtosis** |
| Business Alignment | 4.24 | 0.54 | -0.95 | 1.64 |
| Organizational Support | 4.24 | 0.62 | -1.04 | 1.37 |
| Organizational Awareness | 4.23 | 0.63 | -1.31 | 2.91 |
| IT Competence | 4.21 | 0.58 | -1.01 | 2.40 |
| Security Controls Development | 4.23 | 0.63 | -1.34 | 3.39 |
| ISM Performance | 4.18 | 0.57 | -0.89 | 1.63 |

## Common-Method Bias Check

As data were collected through the self-reported survey method, common-method bias may be present. When measures are collected using the same method, the variance attributable to measurement method rather than the constructs is a potential problem in behavioral research (Podasakoff et al., 2003). Although prior research indicates that the biasing effect may not be substantial (Malhotra et al., 2006), it is strongly recommended to check for common method bias (Straub et al., 2004; Straub and Burton-Jones, 2007).

Two procedural remedies were performed before data collection to control common method bias, following recommendations from the literature (Podasakoff et al., 2003). First, respondents’ anonymity was protected by not asking identifying information in the questionnaire. Participants were asked to respond to the questions as honestly as possible without worrying about the correctness of answers. These steps may help to reduce participant evaluation apprehension and the likelihood of obtaining socially desirable responses (Podsakoff et al., 2012). Second, the scale items were improved by providing examples to help reduce item ambiguity (e.g. including examples for IT resources). In addition, every Likert scale point (from 1 to 5) rather than only end points in the response scales was labeled (Krosnick, 1991).

After data collection, a Harman’s single-factor test (Podasakoff et al., 2003) was applied to check for common method bias. In this test, all the measurement items in the research model were loaded into a single exploratory factor analysis and the unrotated solution was examined to determine the number of factors that account for the variance of the measures. The unrotated factor solution indicated that: (1) more than one factor emerged from the factor analysis; and (2) no single general factor accounted for the majority of the covariance (the most covariance explained by one factor was 46%). This result suggested that there was no substantial common method variance (CMV) and that it was not a problem.

## Research Model Validation

The research model was tested using the partial least square (PLS) software, specifically WarpPLS 4.0 (Kock, 2013). In this section, the analyses performed to evaluate both the measurement and the structural models are presented.

### Measurement Model

The measurement model (or “outer model”) shows how each block of items relates to its construct or latent variable (Chin, 1998). There are five reflective constructs and one formative construct in the research model. For reflective constructs, the measurement model provides indices for assessing convergent validity and discriminant validity of the scale. The formative construct needs to be validated differently, as the observed variables “cause” the construct and represent several dimensions of it (Gefen et al., 2000). Therefore, the analysis of the measurement model was split into two sections.

***Reflective constructs***

The first evaluation of reflective constructs was to test the reliability of their items. This was determined by checking the indicator loadings and the corrected item-total correlations, which are the correlations between each item and a scale score that excludes that item (Gefen et al., 2000). As shown in Table 5.8, all items meet the criteria that indicator loading is greater than 0.40 and corrected item-total correlation is greater than 0.50.

Table 5.8 Item Reliability Assessment

|  |  |  |  |
| --- | --- | --- | --- |
| **Construct** | **Item** | **Item Loading[[6]](#footnote-7)** | **Corrected Item-total Correlation** |
| Business Alignment | BA\_1 | 0.69 | 0.64 |
| BA\_2 | 0.67 | 0.62 |
| BA\_3 | 0.65 | 0.61 |
| Organizational Support | OS\_1 | 0.72 | 0.67 |
| OS\_2 | 0.70 | 0.65 |
| OS\_3 | 0.68 | 0.64 |
| Organizational Awareness | OA\_1 | 0.66 | 0.62 |
| OA\_2 | 0.72 | 0.68 |
| OA\_3 | 0.75 | 0.70 |
| OA\_4 | 0.71 | 0.67 |
| Security Controls | SC\_1 | 0.66 | 0.61 |
| SC\_2 | 0.76 | 0.72 |
| SC\_3 | 0.70 | 0.66 |
| ISM Performance | IP\_1 | 0.64 | 0.60 |
| IP\_2 | 0.63 | 0.59 |
| IP\_3 | 0.70 | 0.65 |
| IP\_4 | 0.65 | 0.61 |

The second step was to assess the reliability of all reflective constructs using Cronbach’s alpha and composite reliability values. Given the criteria that both Cronbach’s alpha and composite reliability scores should be greater than 0.70 (Fornell and Larcker, 1981; Johnston and Warkentin, 2010), the reliability values of all the constructs are acceptable (see Table 5.9).

Table 5.9 Construct Reliability Assessment

|  |  |  |  |
| --- | --- | --- | --- |
| **Construct** | **Composite Reliability** | **Cronbach’s Alpha** | **AVE** |
| Business Alignment | 0.84 | 0.71 | 0.63 |
| Organizational Support | 0.85 | 0.74 | 0.66 |
| Organizational Awareness | 0.87 | 0.80 | 0.62 |
| Security Controls | 0.85 | 0.74 | 0.66 |
| ISM Performance | 0.85 | 0.77 | 0.59 |

Next, the convergent and discriminant validity of the constructs was examined. Convergent validity is generally demonstrated if (1) all item loadings are significant and greater than 0.70; (2) average variance extracted (AVE, the amount of variance captured by a latent variable relative to the amount caused by measurement error) for each construct is above 0.50 (or square root of AVE is greater than 0.707); and (3) composite reliability index for each construct exceeds 0.80 (Fornell and Larcker, 1981; Johnston and Warkentin, 2010).

As shown in Table 5.10, all item loadings are greater than 0.70. All item loadings are significant (p<0.001) and AVE for each construct is greater than 0.50. Furthermore, the composite reliabilities of all constructs are also greater than 0.80 (shown in Table 5.11). The square root of AVE for each construct meets the criterion of 0.707. Based on the above criteria, the PLS results indicate an acceptable level of convergent validity.

Table 5.10 Loadings and Cross-loadings, and AVEs for Multi-item Constructs

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Construct & Item** | **BA** | **OS** | **OA** | **IC** | **SC** | **IP** | **P** | **AVE** |
| BA\_1 | 0.78 | -0.10 | 0.13 | -0.17 | 0.31 | 0.05 | <0.001 | 0.63 |
| BA\_2 | 0.78 | 0.20 | -0.02 | 0.31 | -0.45 | -0.10 | <0.001 |
| BA\_3 | 0.83 | -0.10 | -0.10 | -0.13 | 0.14 | 0.04 | <0.001 |
| OS\_1 | -0.00 | 0.77 | 0.07 | 0.16 | 0.12 | -0.03 | <0.001 | 0.66 |
| OS\_2 | 0.11 | 0.83 | 0.04 | 0.02 | -0.29 | -0.01 | <0.001 |
| OS\_3 | -0.11 | 0.83 | -0.10 | -0.17 | 0.19 | 0.04 | <0.001 |
| OA\_1 | -0.29 | 0.24 | 0.74 | -0.04 | 0.15 | -0.06 | <0.001 | 0.62 |
| OA\_2 | 0.00 | -0.15 | 0.82 | 0.17 | 0.04 | -0.18 | <0.001 |
| OA\_3 | 0.11 | -0.02 | 0.81 | -0.11 | 0.11 | 0.01 | <0.001 |
| OA\_4 | 0.16 | -0.05 | 0.78 | -0.03 | -0.30 | 0.24 | <0.001 |
| SC\_1 | 0.03 | 0.24 | -0.14 | 0.76 | -0.38 | -0.03 | <0.001 | 0.59 |
| SC\_2 | -0.05 | -0.10 | -0.06 | 0.78 | 0.28 | -0.05 | <0.001 |
| SC\_3 | 0.02 | -0.14 | 0.21 | 0.75 | 0.10 | 0.08 | <0.001 |
| IC\_1 | -0.02 | -0.21 | 0.13 | 0.07 | 0.81 | -0.23 | <0.001 | 0.66 |
| IC\_2 | -0.06 | 0.20 | -0.17 | 0.03 | 0.86 | 0.08 | <0.001 |
| IC\_3 | 0.08 | -0.00 | 0.06 | -0.11 | 0.77 | 0.16 | <0.001 |
| IP\_1 | 0.01 | 0.23 | -0.12 | 0.01 | -0.13 | 0.76 | <0.001 | 0.59 |
| IP\_2 | -0.10 | -0.29 | 0.29 | 0.05 | 0.15 | 0.71 | <0.001 |
| IP\_3 | 0.15 | -0.05 | -0.01 | -0.19 | -0.00 | 0.83 | <0.001 |
| IP\_4 | -0.07 | 0.09 | -0.14 | 0.14 | -0.01 | 0.78 | <0.001 |

Notes: Loadings are unrotated and cross-loadings are oblique-rotated. P values < 0.05 are desirable for reflective indicators.

Table 5.11 Inter-Construct Correlations and Square Roots of AVEs

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Construct** | | **CR** | **BA** | **OS** | **OA** | **SC** | **IP** |
| BA | Business Alignment | 0.84 | **0.80** |  |  |  |  |
| OS | Organizational Support | 0.85 | 0.71 | **0.81** |  |  |  |
| OA | Organizational Awareness | 0.87 | 0.68 | 0.73 | **0.79** |  |  |
| SC | Security Controls | 0.85 | 0.75 | 0.73 | 0.72 | **0.81** |  |
| IP | ISM Performance | 0.85 | 0.63 | 0.67 | 0.71 | 0.64 | **0.77** |

Notes: CR = Composite Reliability. Off diagonal numbers are inter-construct correlations. Diagonal numbers are the square roots of AVE (average variance extracted).

Discriminant validity is verified by the difference between the AVE of a construct and its correlations with other constructs. Discriminant validity is achieved if (1) the square root of each construct’s AVE is greater than its correlations with other constructs and (2) item loadings on their respective constructs are greater than their cross loadings on other constructs (Fornell and Larcker, 1981; Johnston and Warkentin, 2010). As indicated in Table 5.11, the highest construct correlation is 0.75 and the lowest square root of AVE is 0.77. Furthermore, item loadings on their corresponding constructs are greater than their cross loadings on other constructs (Table 5.10). Thus, all reflective constructs meet the conditions. The results demonstrate a satisfactory level of discriminant validity.

***Formative constructs***

Formative indicators are not used to account for observed variances in the outer model, thus internal consistency is unimportant because measures are examining different facets of the construct (Petter et al., 2007). The only formative construct in the research model, IT competence, was assessed for validity.

First, it was ensured that this construct was correctly specified as formative. Four decision rules have been outlined in the literature (Diamantopoulos and Winklhofer, 2001; Jarvis et al., 2003; Petter et al., 2007). The first rule is to determine that the theoretical direction of causality is from the measures to the construct. An increase in the availability and flexibility of an organization’s IT resources (e.g., networks, hardware, software, etc.) is theoretically posited to increase the organization’s IT competence. When its IT staff (both inbound and outsourced) is more knowledgeable and more capable of developing and maintaining information security technologies, the organization’s IT competence increases. In addition, as the end users of IT systems in an organization follow sound operation processes more, the organization obtains more IT competence. This suggests that these three indicators define the characteristics of the IT competence construct, i.e., these indicators predict the construct. The second rule is to examine the interchangeability of the construct indicators. The three indicators (IT resources, IT staff and IT systems end users) measure different aspects of IT competence. They do not have the same content and dropping an indicator may affect the measuring of the construct. This suggests that these indicators are formative and not reflective in nature. The third rule is to test the covariation among indicators. In the case of IT competence, indicators do not necessarily covary with each other. For example, a change in one measure of the construct (e.g., IT systems end users) does not require a change in all other measures of the construct (IT resources and IT staff). Thus these three indicators can be considered as formative. The fourth rule considers the nomological net of construct indicators. Formative indicators are not required to have the same antecedents or consequences. The three measures of IT competence may share the same consequence (i.e. IT competence), but their antecedents may be different. IT resources may be affected by the organization’s financial investment, while IT staff is determined by the organization’s human resources. End user capability may depend on the organization’s training and education programs. Therefore, following these criteria, IT competence can be identified as a formative construct.

Next, the validity of the formative construct was assessed with the weights of its indicators and their significance (Petter et al., 2007). As shown in Table 5.12, all three items of IT competence achieve significance at the 0.001 level. Also, the variance inflation factor (VIF) was examined to determine whether multicollinearity exists between indicators. Each indicator meets the criterion that VIF is less than 3.3, which suggests that no multicollinearity exists for the formative construct (Diamantopoulos and Siguaw, 2006). Thus, the validity of the formative construct (IT competence) was established.

Table 5.12 Formative Construct Validity Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Construct** | **Items** | **Weight** | **Significance** | **VIF** |
| IT Competence | IC\_IT Resources | 0.43 | <0.001 | 1.26 |
| IC\_IT Staff | 0.44 | <0.001 | 1.29 |
| IC\_End Users | 0.43 | <0.001 | 1.24 |

### Structural Model

The hypotheses of the proposed theoretical model were tested by examining the PLS structural model. The first measure was the R2 values of the dependent variables which represent the predictive power of the theoretical model (Chin, 1998). As shown in Figure 5.1, the research model accounted for 63 percent of variance in security controls and 57 percent of variance in ISM performance. In addition, the R2 value for organizational support was 0.50, R2 for organizational awareness was 0.59, and R2 for IT competence was 0.39. The literature suggests that the R2 value of a dependent variable should be at least 10 percent in order to result in any meaningful interpretation (Falk and Miller, 1992). Thus, the theoretical model demonstrated substantive explanatory power.

|  |
| --- |
| Figure 5.1 PLS Model Testing Results |

Next, the significance of the path coefficients was measured. The standardized path coefficients indicate the strength of the relationship between independent and dependent variables (Chin, 1998). The results are shown in Table 5.13. WarpPLS 4.0 automatically finds any non-linear relationship between latent variables in the research model to obtain the best fit. All the relationship plots are shown in Appendix 5. As hypothesized, ISM performance was significantly determined by security controls (β=0.15, p<0.005), organizational support (β=0.29, p<0.001), and organizational awareness (β=0.39, p<0.001), providing support for H10, H8, and H9. Security controls was significantly determined by organizational support (β=0.38, p<0.001), organizational awareness (β=0.27, p<0.001), and IT competence (β=0.23, p<0.001). This supported H5, H7, and H6. Furthermore, organizational support had a strong direct effect on organizational awareness, as demonstrated by the significant path coefficient (β=0.49, p<0.001). Business alignment had a direct effect on organizational support (β=0.71, p<0.001), organizational awareness (β=0.34, p<0.001), and IT competence (β=0.62, p<0.001). Thus, H4, H1, H2, and H3 were all supported. A summary of the hypotheses test results is shown in Table 5.14.

Table 5.13 Path Coefficients

|  |  |  |  |
| --- | --- | --- | --- |
| **Dependent Variable** | **Independent Variable** | **Path Coefficient** | **Significance** |
| ISM Performance  (IP) | Organizational Support  (OS) | 0.29 | P<0.001 |
| Organizational Awareness  (OA) | 0.39 | P<0.001 |
| Security Controls Development  (SC) | 0.15 | P<0.005 |
| Security Controls  (SC) | Organizational Support  (OS) | 0.38 | P<0.001 |
| Organizational Awareness  (OA) | 0.27 | P<0.001 |
| IT Competence  (IC) | 0.23 | P<0.001 |
| Organizational Awareness  (OA) | Business Alignment  (BA) | 0.34 | P<0.001 |
| Organizational Support  (OS) | 0.49 | P<0.001 |
| Organizational Support  (OS) | Business Alignment  (BA) | 0.71 | P<0.001 |
| IT Competence  (IC) | Business Alignment  (BA) | 0.62 | P<0.001 |

Table 5.14 Summary of Hypothesis Tests

|  |  |  |  |
| --- | --- | --- | --- |
| Hypotheses | | Path | Supported |
| H1 | Business alignment positively affects organizational support to ISM. | BA→BS | Yes |
| H2 | Business alignment positively affects organization’s IT competence. | BA→IC | Yes |
| H3 | Business alignment contributes to greater organizational awareness of information security risks and controls. | BA→OA | Yes |
| H4 | Organizational support raises organizational awareness of information security risks and controls. | OS→OA | Yes |
| H5 | Organizational support positively affects of information security controls. | OS→SC | Yes |
| H6 | IT competences positively affect information security controls. | IC→SC | Yes |
| H7 | Organizational awareness positively affects information security controls. | OA→SC | Yes |
| H8 | Organizational support positively influences the performance of ISM. | OS→IP | Yes |
| H9 | Organizational awareness positively influences the performance of ISM. | OA→IP | Yes |
| H10 | Effective security controls positively influences the performance of ISM. | SC→IP | Yes |

The third measure employed to evaluate the structural model was the Goodness of Fit (GoF) index, which is defined as the “geometric mean of the average communality and average R2 for all endogenous constructs” (Akter et al., 2011, p.3). The GoF index is used as a global fit measure for PLS models and can be applied to both reflective and formative latent variables (Vinzi et al., 2010). The suggested cut off value for communality is 0.50 and different values of GoF represent different effect sizes of R2 (i.e. small effect size if 0.10≤ GoF < 0.25; medium effect size if 0.25≤GoF < 0.36; large effect size if GoF  0.36) (Wetzels et al., 2009). The GoF value obtained for the research model was 0.58, exceeding the 0.36 threshold of large effect size of R2. This result indicates good performance of the research model.

The last analysis for evaluating the structural model was the effect size of each path in the model, which measures the impact of a particular independent variable on a dependent variable and can be determined by its value (Chin, 1998). The following criteria can be used to interpret the effect sizes: 1) for a small effect size, 0.02 < *f* 2 ≤ 0.15; 2) for a medium effect size, 0.15 < *f* 2 ≤ 0.35, and 3) for a large effect size, *f* 2 > 0.35 (Chin, 1998; Cohen, 1988). The results obtained from WarpPLS 4.0 analysis[[7]](#footnote-8) are summarized in Table 5.15. Except that security controls development has only a small effect on ISM performance, all other paths have medium to large effect sizes.

Table 5.15 Path Effect Size Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| **Dependent Variable** | **Independent Variable** | ***f* 2** | **Effect Size** |
| ISM Performance  (IP) | Organizational Support  (OS) | 0.20 | Medium |
| Organizational Awareness  (OA) | 0.28 | Medium |
| Security Controls Development  (SC) | 0.10 | Small |
| Security Controls  (SC) | Organizational Support  (OS) | 0.28 | Medium |
| Organizational Awareness  (OA) | 0.20 | Medium |
| IT Competence  (IC) | 0.16 | Medium |
| Organizational Awareness  (OA) | Business Alignment  (BA) | 0.23 | Medium |
| Organizational Support  (OS) | 0.36 | Large |
| Organizational Support  (OS) | Business Alignment  (BA) | 0.51 | Large |
| IT Competence  (IC) | Business Alignment  (BA) | 0.39 | Large |

## Post Hoc Analysis

As some demographic questions and control variables were included in the questionnaire, these variables were tested for their potential influence on the endogenous constructs in the research model. There are four single-indicator control variables: industry, organization size, standard, and domestic. Industry represents the industry type for the respondent’s organization (Manufacturing=1, Retail and distribution=2, Financial Services=3, Technology=4, Health=5, Telecommunication=6, Travel, leisure and entertainment=7, Education=8, Utilities, energy and mining=9, Government=10, Other=11). Organization size was coded depending on how many employees were in the respondent’s organization (Employees less than 50 = 1, Employees between 51 and 200 = 2, Employees between 201 and 500 = 3, Employees above 500 = 4). Information Security Standard or “Standard” was coded as binary to stand for whether the organization had applied any national or international information security standard (No =1, Yes = 2). The Domestic variable represents whether the organization is domestic or international. It was also coded as binary (Domestic =1, International = 2).

These four control variables were included one by one in the PLS model, by linking one control variable to each endogenous variable in the model at one time. The significance of those paths was analyzed and the results are shown in Table 5.16. Organization size had a positive impact on organizational support and security controls development, suggesting that managers in bigger organizations perceived more organizational support and better security controls development. Standard had a positive impact on organizational support, indicating that organizations that had already applied information security standards obtained better organization support. All other paths were not significant.

Table 5.16 Control Variable Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Variable** | **Endogenous Construct** | **Path Coefficient** | **Significance** |
| Industry | Organizational Support (OS) | -0.03 | n.s. |
| Organizational Awareness (OA) | -0.01 | n.s. |
| IT Competence (IC) | -0.06 | n.s. |
| Security Controls (SC) | -0.09 | n.s. |
| ISM Performance (IP) | -0.09 | n.s. |
| Organization Size | Organizational Support (OS) | 0.12 | P<0.05 |
| Organizational Awareness (OA) | 0.03 | n.s. |
| IT Competence (IC) | 0.04 | n.s. |
| Security Controls(SC) | 0.11 | P<0.05 |
| ISM Performance (IP) | -0.02 | n.s. |
| Standard | Organizational Support (OS) | 0.12 | P<0.05 |
| Organizational Awareness (OA) | 0.04 | n.s. |
| IT Competence (IC) | 0.06 | n.s. |
| Security Controls (SC) | 0.05 | n.s. |
| ISM Performance (IP) | 0.08 | n.s. |
| Domestic | Organizational Support (OS) | -0.02 | n.s. |
| Organizational Awareness (OA) | 0.00 | n.s. |
| IT Competence (IC) | 0.01 | n.s. |
| Security Controls (SC) | -0.01 | n.s. |
| ISM Performance (IP) | 0.05 | n.s. |

Notes: n.s. = not significant.

In order to determine the magnitude of the impact of control variables on endogenous constructs, their effect sizes were examined. All the control variables with significant paths were added to the research model at the same time. As shown in Table 5.17, the results indicated that all the control variables had a small effect size. Furthermore, the addition of control variables did not change the hypothesized relationships in the research model. The final analysis results were summarized in Table 5.18.

Table 5.17 Path Effect Sizes Analysis for Control Variables

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Variable** | **Endogenous Construct** | ***f* 2** | **Effect Size** |
| Organization Size | Organizational Support  (OS) | 0.04 | Small |
| Security Controls  (SC) | 0.01 | Small |
| Standard | Organizational Support  (OS) | 0.03 | Small |

Table 5.18 Path Analysis with Control Variables

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dependent Variable** | **Independent Variable** | **Path Coefficient** | **Significance** | ***f* 2** | **Effect Size** | **R2** |
| ISM Performance  (IP) | Organizational Support  (OS) | 0.29 | P<0.001 | 0.20 | Medium | 0.57 |
| Organizational Awareness  (OA) | 0.39 | P<0.001 | 0.28 | Medium |
| Security Controls  (SC) | 0.15 | P<0.01 | 0.10 | Small |
| Security Controls  (SC) | Organizational Support  (OS) | 0.34 | P<0.001 | 0.25 | Medium | 0.64 |
| Organizational Awareness  (OA) | 0.28 | P<0.001 | 0.20 | Medium |
| IT Competence  (IC) | 0.24 | P<0.001 | 0.16 | Medium |
| Organization Size\* | 0.11 | P<0.05 | 0.03 | Small |
| Organizational Awareness  (OA) | Business Alignment  (BA) | 0.34 | P<0.001 | 0.23 | Medium | 0.59 |
| Organizational Support  (OS) | 0.50 | P<0.001 | 0.36 | Large |
| Organizational Support  (OS) | Business Alignment  (BA) | 0.66 | P<0.001 | 0.47 | Large | 0.53 |
| Organization Size\* | 0.11 | P<0.05 | 0.04 | Small |
| Standard\* | 0.11 | P<0.05 | 0.03 | Small |
| IT Competence  (IC) | Business Alignment  (BA) | 0.62 | P<0.001 | 0.39 | Large | 0.39 |

\*Control Variable

## Summary

In this chapter, the procedures applied to data collection and data analyses were presented. Before testing the proposed research model, the data were first screened and demographic statistics were summarized. It was also verified that common method bias is not a problem in the current study. The research model was tested using the PLS technique, with an emphasis on the measurement model and structural model. The reliability and validity of the constructs were verified in the PLS measurement model. The structural model suggested that all proposed hypotheses were supported by the data analysis. Finally, post hoc analyses were presented to examine the influence of the control variable.

# Discussion and Conclusions

The results of the data analyses show that the theoretical model is successful in capturing the main antecedents of ISM performance. An organization’s ISM performance is significantly influenced by the organization’s security controls, organizational support, and organizational awareness. In addition, an organization’s security controls development is influenced by the organization’s organizational support, organizational awareness and IT competence, which in turn are all influenced by business alignment. Organizational support also has a significant influence on organizational awareness. In the rest of this chapter, all key findings are further discussed in detail. The theoretical contributions and practical implications of this study are presented, and limitations and future research opportunities are also outlined. Finally, conclusions to this chapter and this dissertation are presented.

## Key Findings

As the proposed research model was tested and all hypotheses were supported by data, the three proposed research questions were answered. Detailed findings regarding the research questions are presented below.

### Measurement of ISM Performance

The first research question of this study is “how to measure ISM performance”. Based on the framework provided by the BSC model (Herath et al., 2010; Huang et al., 2006), ISM performance was measured by four items which represent four perspectives of ISM performance: business value, internal process, user orientation, and future readiness. The four items are: (1) IP\_1, the extent to which the benefit of ISM is greater than cost; (2) IP\_2, the extent to which employees comply with information security policies; (3) IP\_3, the extent to which information security policies are effective and efficient; and (4) IP\_4, the extent to which the organization’s ISM is positioned to meet future needs.

It was found that all these measurements of ISM performance are reliable and valid. All indicator loadings (IP\_1, 0.64; IP\_2, 0.63; IP\_3, 70; IP\_4, 0.65) were greater than 0.40, and all the corrected item-total correlations (IP\_1, 0.60; IP\_2, 0.59; IP\_3, 65; IP\_4, 0.61) were greater than 0.50. These indicate that all the four items of ISM performance are reliable. The Cronbach’s alpha of the construct ISM performance, was 0.77. And the composite reliability value of ISM performance was 0.85. These suggest that ISM performance is reliable as a reflective construct. Further, the AVE of ISM performance was 0.59. ISM performance was validated by examining the convergent and discriminant validity of the construct.

The results from the model support the application of the BSC framework for measuring ISM performance. The multiple performance measures are a mix of common measures and measures unique to the strategy, which measure ISM performance from a management view, end-user view, operation-based view, and innovation and learning view. This indicates that a BSC framework, which is widely used to measure common organization performance, is also suited to measuring intangible assets such as information security management. This finding is consistent with recommendations in prior IS research (Herath et al., 2010; Huang et al., 2006).

Although the four items reflect the four basic perspectives of the BSC model, they are less complicated than the items recommended by the literature (Herath et al., 2010; Huang et al., 2006). In order to explore further measurement development for study, each of the four perspectives was developed as a reflective construct and used to replace ISM performance in alternative PLS models. The four alternative dependent variables are business value of ISM, user orientation of ISM, internal process performance of ISM and future readiness of ISM. All these constructs were operationalized with three measurement items (see Table 4.1).

The four alternative models were tested separately. All the model test results are shown in Appendix 6. For the assessment of business value of ISM, the model accounted for 56 percent of the variance. All paths in the model were significant at the 0.001 level. For the assessment of user orientation of ISM, the model accounted for 46 percent of variance. All paths in the model were significant at the 0.001 level, except the effect of organizational support on user orientation of ISM and the effect of security controls development on user orientation of ISM, which were both significant at the 0.01 level. For the assessment of internal process performance of ISM, the model accounted for 57 percent of the variance. All paths in the model were significant at the 0.001 level. For the assessment of future readiness of ISM, the model accounted for 57 percent of the variance. All paths in the model were significant at the 0.001 level, except the relationship between security controls development and future readiness of ISM, which was significant at the 0.05 level.

In all these alternative models, all the hypotheses were still supported. This may suggest that measurement of the four perspectives reflects measurement of ISM performance. The BSC framework is therefore appropriate for measuring ISM performance. This answers the first research question of this study.

### Antecedents of ISM Performance

As predicted by the research model, an organization’s ISM performance is influenced by the organization’s security controls, organizational support and organizational awareness. The research model’s explanatory power was strong, as 57% of the variance in ISM performance was explained by the model. All these three causal relationships were significant at the 0.01 level.

These results suggest that the more organizational support is provided in an organization, the more effective information security becomes. The relationship between organizational support and ISM performance had a statistically significant beta coefficient of 0.29 (p<0.001), with a medium effect size (*f* 2=0.20). Organizational support includes top management commitment, sufficient resources (especially funding) allocation, and formal structuring for information security management. This finding is basically consistent with prior research in the IS security literature. For example, it was posited that support from senior management through system resource provision provides ISM with a solid foundation to succeed (Datta and Banerjee, 2011). More resources spent on information security management could prevent security incidents (Werlinger et al., 2009). Effective organizational structuring was found to help address the importance of information security at the organizational level and thus improve the effectiveness and efficiency of security management (Boss et al., 2009; Kayworth and Whitten, 2010; Straub, 1988; Straub and Collins, 1990).

These results also suggest that the more that employees are aware of the information security risks, policies, procedures and countermeasures that exist in an organization, the better information security management performance the organization achieves. The relationship between organizational awareness and ISM performance had a statistically significant beta coefficient of 0.39 (p<0.001), with a medium effect size (*f*2=0.28). Organizational awareness represents employee knowledge of potential security threats and their negative consequences, and their knowledge of the organization’s information security policies, procedures, or countermeasures. Such knowledge mainly comes from the organization’s security education and training programs. This finding appears to echo relevant research in the IS security literature as well. For example, it was empirically found that employee awareness of security threats and the severity of these threats would help to encourage employee intentions to comply with security policies and thus improve security management performance (Siponen et al., 2009). Spears and Barki (2010) posited that organizational awareness of security risks and controls would enable the organization to improve effectiveness and efficiency in the security management system.

In addition, it was found that better designed and implemented information security controls will result in better information security management performance. This relationship had a statistically significant beta coefficient of 0.15 (p<0.005), with a small effect size (*f*2=0.10). Security controls development includes the design and implementation of a formal risk management program and formal security policies. The application of specific information security standards is also included. Compared to the other two antecedents, this factor has a smaller effect on ISM performance. It seems that managers perceived organizational support and organizational awareness to be more important than security controls development on ISM performance.

Taken together, the significant influence of these three factors suggests that three paths may lead to ISM success. The first path is from the organizational support. When top management commits more support to ISM, the organization’s security management will be more effective. The second path is from employee awareness of information security. Through organizational education and training programs, employees can receive more knowledge about security risks and countermeasures. Such knowledge will help employees to realize the importance of ISM and comply with security policies effectively. These two paths are both related to human factors. The third path is from the organization’s security measures. Well implemented risk management and security policies will lead to more successful information security management. Perhaps the most interesting findings of this study about the antecedents of ISM performance are the strong and significant effects of organizational support and organizational awareness in comparison to the relatively small impact of security controls development. This may be explained by the great impact of human factors on organizational behavior. Behavioral research literature has emphasized the important role human factors play in IS security management (Culnan et al., 2008; Guo et al., 2011). Without support from the management and employees, even perfectly developed security measures may not be implemented or performed perfectly. These empirical findings suggest that human factors have more influence on ISM performance than security measures.

These findings answer the second research question of this study, “What critical factors make ISM effective?” They also partly answer the third research question, “How do these factors contribute to the success of ISM?”

### Antecedents of Security Controls

An organization’s security controls include technical controls, operation controls and management controls. Security controls development represents identifying, implementing and maintaining security control sets. The results indicate that security controls development is significantly influenced by organizational support, organizational awareness and the organization’s IT competence. The model explained 63% of the variance in security controls development. All these three causal relationships were significant at the 0.001 level.

The relationship between organizational support and security controls had a statistically significant beta coefficient of 0.38 (p<0.001), with a medium effect size (*f* 2=0.28). This suggests that better organizational support leads to better improvement in security controls. Security controls development is a dynamic process, which is complicated and resource-intensive. Organizational support can guarantee necessary resources for the development process and thus facilitate the development of security control sets. The relationship between organizational awareness and security controls also had a statistically significant beta coefficient of 0.27 (p<0.001), with a medium effect size (*f*2=0.20). This suggests that the more organizational awareness is achieved, the more helpful it is to develop security controls. Through appropriate training and regular updates in organizational policies and procedures, employees are able to understand information security threats and security policies in the course of their normal work. Further, employees can provide feedback to current policies and procedures, which will help improve security controls. These findings are in line with results from prior literature (Barlette and Fomin, 2009; Kayworth and Whitten, 2010; Spears and Barki, 2010).

In addition, it was found that an organization’s IT competence had a significant influence on the organization’s security controls. This relationship had a statistical beta coefficient of 0.23 (p<0.001), with a medium effect size (*f* 2=0.16). An organization’s IT competence includes the organization’s IT resources, IT staff’s IT capability and end users’ IT capability. These factors are a substantial basis for the organization to utilize information technologies and skills to develop measures to cope with security threats. Specifically, IT competence is indispensable to the implementation of technical security controls and operational security controls.

Overall, the significant influence of these three antecedents suggests that all organizational factors, human factors and technical factors work together to facilitate the organization’s security controls, which also mediates these factors’ impact on ISM performance. These findings also partly answer the third research question, “How do these factors contribute to the success of ISM?”

### Other Relationships

The data analysis reveals that business alignment has a significant effect on several antecedents of ISM performance. It was found that business alignment had the strongest relationship with organizational support. This path achieved a statistical significance at the 0.001 level and its beta coefficient was 0.71. This relationship had a large effect size (*f 2*=0.51). This indicates that a better fit between the information security objectives and the business objectives leads to a higher level of organizational support. When information security objectives are aligned with the organization’s business strategy, mutual understanding can be achieved between top management and ISM planners. Top management can then be convinced about the importance of information security resulting in better support for ISM processes within the business framework. This empirical finding is consistent with many recommendations in prior IS security literature (Chang et al., 2011; Johnston and Hale, 2009; Kayworth and Whitten, 2010; Ma et al., 2009).

Another strong path is between business alignment and IT competence. This relationship had a significant statistical beta coefficient of 0.62 (p<0.001), which also had a large effect size (*f* 2=0.39). This indicates that business alignment has a very strong impact on the organization’s IT competence. An organization’s IT competences include IT resources and operations, which are the technical foundation of ISM. The acquisition and deployment of IT resources needs to be positioned at the organization’s strategic level. When information security objectives are aligned with the organization’s business strategy, collaborative efforts between information security objectives and business strategies facilitate resource acquisition and other IT competence achievement.

Business alignment also has a significant impact on organizational awareness. This relationship had a statistical beta coefficient of 0.34 (p<0.001), with a medium effect size (*f*2=0.23). This suggests that better business alignment contributes to greater organizational awareness of information security risks and controls. As security policies and procedures gained alignment with the business environment, organizational awareness of security risks and controls increases. In addition, organizational awareness is significantly influenced by organizational support. The path had a large effect size (*f*2=0.36), with a statistical beta coefficient of 0.49 (p<0.001), suggesting that organizational awareness can be greatly increased by organizational support. Prior literature has pointed out that organizationally sponsored security awareness, training, and education programs are the primary formal mechanisms to increase the overall awareness and understanding of information security (Culnan et al., 2008; Kayworth and Whitten, 2010; Ma et al., 2009; Siponen et al., 2009; Werlinger et al., 2009). Support from top management facilitates the organizational training and education programs, which in turn boost organizational awareness.

These findings clearly indicate the importance of business alignment to ISM success. Although it has been emphasized by several previous studies that information security objectives and activities must be aligned with business objectives and requirements (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), no research has empirically examined the effects of business alignment. This study empirically verifies that business alignment significantly influences organizational support, IT competence, and organizational awareness. In turn, these factors mediate the effect of business alignment on security controls development and finally, on ISM performance.

The findings in this section also partly answer the third research question, “How do these factors contribute to the success of ISM?”

### Warped Relationships

From the bivariate data plot diagrams (see Appendix 5), we found that not all the relationships proposed in this study are linear. Given the built-in capabilities for handling nonlinearity in software WarpPLS 4.0, all relationships were automatically warped to the best fit. The relationships between independent variables and dependent variables can then be demonstrated more accurately and clearly. Such nonlinear models reduce the risk of systematically misestimating the impact of independent variables on user perceptions or behaviors (Guo et al., 2011).

From the ten plot diagrams in Appendix 5, we can see that all the curves are steeper in the left bottom corner than the upper right corner. This means that, when the independent variable’s value is small, its effect on the dependent variable is stronger and more obvious. As the independent variable’s value increase, the curve becomes flatter which means the effect becomes weaker. For example, as the value of organizational support increases, the β value of the curve decreases from 0.77 to 0.23. Compared to the result that greater organizational support may lead to better ISM performance, it is more likely that failure in organizational support will cause failures in ISM performance. As seen in Appendix 5, such tendencies exist in all the causal relationships in this research model.

### Control Factors

Four control variables (industry, organization size, standard, and domestic) were tested in the PLS model. It was found that the organization’s industry had no significant impact on the research model’s results. “Domestic”, which represents whether the organization is domestic or international, had no significant influence either. This suggests that none of the relationships in this research model are influenced by the organization’s industry type, or by whether the organization is domestic or international.

However, organization size was found to have a positive impact on organizational support and security controls. The path from organization size to organizational support had a small effect size (*f* 2=0.04), with a statistical beta coefficient of 0.12 (p<0.05). The path from organization size to security controls also had a small effect size (*f* 2=0.01), with a statistical beta coefficient of 0.11 (p<0.05). This suggests that larger organizations may obtain more organizational support and better security controls than smaller organizations. In larger organizations, there may be more formal strategic planning and more formal organizational structures, in which information security management can be positioned at a higher and organization-wide level and thus receive more organizational support. Further, it is more possible for a bigger organization to have formal department/professionals and processes for developing information security controls.

Another control variable, “standard” (whether the organization had applied any national or international information security standard), was also found to have a positive impact on organizational support. This relationship had a statistical beta coefficient of 0.12 (p<0.05), with a small effect size (*f*2=0.03). This relationship suggests that organizations that have already applied information security standards have better organizational support than those that have not applied information security standards. The possible explanation is that security standards may have a requirement for top management commitment, resource allocation and a formal security structure. The application of a security standard represents a commitment of the organization to adhere to that standard. The application of a security standard needs and facilitates organizational support.

The research model was tested again after adding the two control variables (“organization size” and “standard”) with significant paths to the PLS model. The addition of these control variables did not change the hypothesized relationships in the research model, indicating that the control variables did not alter the conclusions derived from the hypotheses of this study. By controlling the effect of organization size and standards application, the proposed research model is validated.

## Contributions

Findings from this study provide important contributions to both theory and practice. Details are presented below.

### Theoretical Contributions

First, this study developed a theoretical model on the critical success factors of organizational information security management. This addresses information security issues at the organizational level, from a strategic management perspective. The relevant critical success factors were well-identified and measured and how these factors contribute to ISM success was empirically tested. To the best of the researcher’s knowledge, this is the first comprehensive critical success factor model in the field of information security management.

Second, this study contributes to the advancement of the ISM literature by developing and validating an ISM performance construct. In this study, ISM performance is measured based on Herath et al.’s (2010) balanced scorecard model. Measurement from four perspectives assesses ISM performance both strategically and operationally, providing a comprehensive solution to the need for such a measure. Furthermore, this construct and its measurement items have been empirically validated in this study, which answers the call for empirical investigation of ISM performance.

Third, this study also contributes to the advancement of the information security management literature by reviewing the most influential information security management standards and trying to validate some basic performance evaluation of the standard. Information security standards provide a common basis for organizations to develop, implement, and measure security management practice. However, scholars have argued that the standards have an unsound basis since they are fostered by an appeal to common practice without having been validated (Siponen and Willison, 2009). This study reviews one international information security standard and combines its guidelines with the IS security literature in order to determine the critical success factors of ISM performance. Through an empirical study, all critical factors have been validated and their effects on ISM performance have also been validated. This study fills the gap between the academic literature and practical standards with its empirical verification.

Fourth, from a methodology perspective, this study has developed and validated new measurement scales for several constructs, including organizational support, organizational awareness, security controls development, and ISM performance. Satisfactory levels of psychometric properties have been achieved in the constructs developed for the model. The validated scales can provide some valuable input for future research on information security management at the organizational level.

Fifth, this study provides empirical evidence that human factors may be more important than security controls for organization’s ISM success. One of the findings of this study is that organizational support and organizational awareness have more significant effects on ISM performance than security controls do. Behavioral research literature has emphasized the important role human factors play in IS security management (Culnan et al., 2008; Guo et al., 2011; Hu et al., 2012). However, no research has compared the relative significance of human factors and security controls. Well implemented risk management and security policies should lead to more successful information security management. Nevertheless, without support from the management and employees, even perfectly developed security measures may not be implemented or performed perfectly. This study empirically proves the more significant importance of human factors.

Lastly, this study contributes to the literature by conducting empirical behavioral research on information security in organizational settings. In the IS security field, individual employee security behaviors such as security policy violation and compliance have been widely studied. However, information security research is one of the most intrusive types of organization research resulting in a serious lack of empirical research in the area of information security management (Kotulic and Clark, 2004). Kotulic and Clark (2004) found that empirical study of ISM at the organizational level was difficult, even when considerable time and effort were expended in attempting to validate proposed conceptual models. Very few empirical studies on organizational ISM can be found in the current literature. The organizational level information security domain may prove in the future to be one of the most critical areas of research necessary for supporting the viability of the organization (Kotulic and Clark, 2004). This study has made considerable progress in this critical area and hopefully can provide useful reference material for future organizational level information security research.

### Implications for Practice

This study also provides organizations’ management with important implications. Even having applied information security standards, many organizations may not be able to distinguish the critical factors and less important factors for ISM success. Information security standards are too complicated for general managers to learn and to guide their practice. Therefore, practitioners need simple and clear guidelines to achieve ISM success. This study identifies several organizational factors that are critical to the organization’s ISM success. And, all these factors’ effects have been empirically verified. Thus, the findings of this study can offer practical guide to organizations’ ISM practice.

First of all, business alignment was found to be the most influential factor in its significant impact on other organizational factors and in turn on ISM success. The results of this study imply that business alignment is the solid foundation of any information security management practice. On the one hand, IS managers or security managers should realize that information security objectives and activities must be aligned with business objectives and requirements. Therefore, when any security management activity or policy is designed or developed, it should be based on business objectives, values, or needs, as opposed to being technology asset focused. On the other hand, the organization’s top management should realize that the aim of ISM is to support organizational objectives, although it may consume organizational resources. It is the responsibility of both the business and the security function, to determine an acceptable level of this alignment. Only collaborative efforts between information security managers and business managers can align ISM practices with the business strategies of the organization.

Secondly, this study indicates that organizational support is one critical success factor which has significant influence on organizational awareness, the development of the organization’s security controls, and the organization’s ISM performance. To achieve ISM success, organizations must provide organizational support to ISM activities, through top management support, commitment of resources, and organizational structuring. Top management should support information security as an important enterprise-wide function and should stress the importance of security to other groups within the organization. Management must consider and allocate sufficient resources (e.g., staff, time, funding, information, methods used in safety works, facilities, tools, machines, etc.) to carry out day-to-day activities to accomplish both short-term and long-term information security goals. Moreover, top management should play the most important role in developing formal organizational structures for information security management, which supports reporting, communication, authority and work flow for ISM. A formal ISM structure can help facilitate organizational integration to achieve security goals and further address the importance of information security at the organizational level. Management must actively support security efforts at all strategic and functional levels.

Thirdly, the results of this study show that organizational awareness significantly influences the organization’s security controls development and ISM performance. In particular, it has the most impact on ISM performance, with a larger effect size than other antecedents of ISM performance. Top management of an organization should recognize the importance of organizational awareness, which means that all employees must be made aware of possible security threats and security controls. Organizationally sponsored security awareness, training, and education program, which is the primary way of communicating information security policies, procedures, and requirements across the organization, should be provided to all employees in order to improve their knowledge and skills on information security at work. A good training program can include courses, regular updates, collateral material such as posters and a system of rewards and penalties for desirable and undesirable behavior (Ma et al., 2009). Employee security awareness can be increased by being trained with verbal persuasion, possible security breach examples, information security mentoring, and the process of designing security policies. In addition, an organization should facilitate an organizational culture that is positive towards carrying out ISM, by building shared values, beliefs and norms for ISM practices.

Fourthly, IT competence is a very important issue which plays a significant role in information security management. Though technological factors are usually less emphasized in current security behavioral research, they are still critical to ISM success. Technologies are used to sustain the security of information. ISM implementation is a top-down process that needs technological IT resources and operations. To strengthen the management of information security, an organization must enhance the IT competences which represent the organization’s integrated and interrelated capabilities of IT elements. Specifically, the following elements should be implemented within the organization: (1) IT resources (e.g., networks, hardware, software, outsourcing, etc.) are available and flexible; (2) IT staff (both inbound and outsourced) is knowledgeable and capable of developing and maintaining information security technologies; and (3) end users of IT systems follow sound operational processes.

Fifthly, to achieve an acceptable level of information security, an appropriate set of security controls must be identified, implemented and maintained within the organization. A comprehensive set of security controls can be recommended to assure ISM success within an organization: (1) Technical controls, such as firewalls, antivirus software, intrusion detection, and encryption techniques, etc; (2) Operational controls, such as physical access controls, backup capabilities, and protection from environmental hazards, etc; (3) Management controls, such as usage policies and business continuity planning. Organizational management should realize that security controls development is a very complicated and resource-intensive process, including risk management, security policies implementation, and standards applications. These processes may require special resources and expertise. It is interesting to note that, as shown by the results of this study, security controls development has less effect on ISM performance than the other two organizational factors. This finding is a reminder to organizations: even with well-developed security controls, ISM success may not be achieved if there is no organizational support and organizational awareness within the organization.

Finally, management should understand the importance of security standards applications. Information security standards offer guidelines to organizations to help maintain an acceptable level of information security. In this study, only 32% of the participants indicated that their organizations applied some kind of security standard, so most organizations have not realized the usefulness of security standards. Some guidelines for security standards have been empirically verified in this study. The results of this study also show that standard applications may influence the organization’s organizational support, which in turn influences ISM performance. Therefore, organizational management can consider applying security standards as a very useful form of information security control.

## Limitations

As with any research project, several limitations should be taken into account for the interpretation of the findings of this study.

The first limitation is that the measurement of ISM performance is subjective. This study applies the BSC framework to measure ISM performance. Ideally, performance measures for the BSC model should be as objective, verifiable and auditable as possible. However, since it is very difficult for the researcher to collect objective data from organizations, this ISM performance model uses subjective measures which collect data on participant perceptions instead of objective measures. This may weaken the measurement power of the BSC framework. Nevertheless, as the difficulties of attempting to gain data about the actions of an organization have been recognized by IS security researchers (Kotulic and Clark, 2004), some scholars have argued that subjective measures are often unavoidable and can be necessarily involved in the measurement (Herath et al., 2010).

The second limitation is self-reporting by survey participants which is the single source of measurement data. Although statistical tests did rule out any significant influence of common method bias in this study, such bias may still possibly be present. Multiple sources of measurement may help alleviate this problem and further validate the causal relationships. Furthermore, if objective measures can be obtained for the dependent variable (ISM performance) as mentioned above, there should be no such problem.

The third limitation is that the results of this study may not be generalized to organizations in countries outside North America. The participants of this study were mainly from North America, where organizational cultures and employee behaviors may be very different from those in other countries. Even in North America, there is a difference in national policies on information security between the U.S. and Canada. For instance, in the U.S., firms are fined heavily if they have security breaches, whereas in Canada they are not. This might have an effect on how seriously firms regard the development of ISM policies. Thus it is expected that social cultural factors may affect how organization and people perceive and respond to organizational information security management activities. Future studies can expand the research model proposed in this study to organizations in other countries with different cultures.

Fourth, most (68%) of the respondents did not have security standards implemented in their organizations. This may affect the measure of security controls, as these respondents may not know the security standards and their impacts. However, it is the fact that only a small proportion of organizations invests in information security standards. A survey was conducted at the end of year 2013 by PWC team and it reported that only 25% of the respondent organizations invested in full implementation of at least one standard[[8]](#footnote-9). This rate is very close to our survey result. Future research should investigate the factors that affect the adoption of security standard and test its impact on ISM performance by comparison of those that have applied security standards and those that have not applied security standards.

The final limitation is that this study reviewed only one information security standard. Security standards provide organizations with practical guidelines but lack empirical verification. One purpose of this study was to find empirical support for practical security standards. One of the most widely used information security standard, Code of Practice for Information Security Management, was chosen as a sample standard. The exclusion of other security standards may miss some critical success factors, and the resulting empirical verification may have less generalizability. Future research should include additional security standards.

## Future Research

According to the findings and limitations of this study, there are several opportunities to conduct future research in information security management area. First, evidence-based ISM performance measurement can be a source of further studies. How to assess the performance of ISM activities is very important to IS security research at the organizational level, whereas effective measurement has not been developed or verified in prior literature. This study demonstrates that the BSC framework provides comprehensive and suitable dimensions to measure ISM performance. However, due to limitations in obtaining objective data from actual organizations, this study could not assess ISM performance with objective data. To better verify the appropriateness of using the BSC model to assess ISM performance, future research can make more efforts to gather objective measurements to test this proposed model.

The second opportunity for future research is to investigate the effects of failure in the CSFs. This study has demonstrated that improvement in critical success factors facilitates improvement in ISM performance. Although we expect that the failure of any success factors we identified may lead to the failure of ISM, this has not been empirically verified yet. We also do not know if there are other factors that may lead to ISM failure. For instance, Fowler and Horan (2008) pointed out that information systems success and failure are not necessary two sides of one coin. Their exploratory study showed that not all of but only four of the six factors associated with the success of the investigated IS were related to the factors identified from the literature as being associated with IS failure. Thus, future study can extend current research to examine the factors that may lead to failure in the organization’s ISM performance such as security breach .

Finally, new methodology can be applied to study the critical success factors of ISM performance for future research. As little empirical research has been done on organizational information security management, more rigorous qualitative and quantitative empirical studies are needed in this area. Case studies are a widely accepted methodology for exploratory and theory-building research (Yin, 2013). These can also be used in explanatory research to test theory or to develop causal explanations (Myers, 2013). A case study is an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident (Yin, 2013). Future research could use case studies to crystallize the identified critical success factors and their impacts on ISM. Companies should be carefully selected for possible case studies based on their representativeness. Interviews should be conducted with the key personnel of IS security management and the importance and relevance of each CSF discussed with these participants. Interviewees would be asked to consider different factors about different aspects of information security management when expressing their points of view. In particular, we can collect data through case studies to study what factors actually lead to the failure of ISM. Findings from such case studies could definitely enrich our understanding and provide insight to the issues of information security management.

## Conclusions

The current study aimed to answer the following research questions: (1) How to measure ISM performance? (2) What critical factors make ISM effective? And, (3) how do these factors contribute to the success of ISM? To achieve this end, this study constructed a theoretical model to investigate the main factors that contribute to successful information security management. By reviewing the ISM standards and literature in the IS field, five critical success factors were identified and the relationships between these factors and ISM performance were examined and validated empirically. Results from this study suggest that the proposed theoretical model has high explanatory power. The research model suggests 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 successful information security management.

Findings from this study provide important contributions to both research and practice. This study contributes to the literature by proposing a theoretical model to examine the effects of critical organizational factors on organizational ISM performance, and empirically validating this proposed model, providing a theoretical extension of the Spears and Barki (2010) model. This study contributes to the advancement of the ISM literature by developing and validating an ISM performance construct, reviewing the most influential information security management standard, and trying to validate some basic guidelines of the standard. Furthermore, from a methodology perspective, this study develops and validates new measurement scales for several constructs.

From a practice point of view, the results of this study suggest that organizational ISM success depends on several critical factors such as business alignment, organizational support, organizational awareness, IT competence, and security controls development. These critical success factors must be evaluated by organizational management in order to better implement information security management in the organization. Moreover, management must develop an understanding of the importance of applying security standards within the organization.

This study provides recommendations for future research avenues. First, future research can make more effort towards using objective measurement to assess ISM performance. Second, future research may explore more critical factors of ISM success and include more relationships in order to get a complete picture of the mechanism that leads to ISM success. Third, the current proposed theoretical model can be conducted in different countries from North America. Finally, new methodologies can be applied in future research to study the critical success factors of ISM performance.

# 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.

Akter, S., D'Ambra, J., and Ray, P. 2011. "An Evaluation of Pls Based Complex Models: The Roles of Power Analysis, Predictive Relevance and Gof Index," *AMCIS 2011 Proceedings - All Submissions* (Paper 151).

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp 613-643

Applegate, L. M., McFarlan, F. W., and McKenney, J. L. 1996. *Corporate Information Systems Management: The Issues Facing Senior Executives*, Irwin: Chicago.

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.

Bano, M., and Zowghi, D. 2015. "A Systematic Review on the Relationship between User Involvement and System Success," *Information and Software Technology* (58), pp 148-169.

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.

Baskerville, R. 1993. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys* (25:4), pp 375-414.

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.

Bhattacherjee, A. 2001. "Understanding Information Systems Continuance: An Expectation-Confirmation Model," *MIS Quarterly* (25:3), pp 351-370.

Boggs, W. B. 2004. "Tqm and Organizational Culture: A Case Study," *The Quality Management Journal* (11:2), pp 42-52.

Bollen, K., and Lennox, R. 1991. "Conventional Wisdom on Measurement: A Structural Equation Perspective," *Psychological Bulletin* (110:2), pp 305-314.

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.

Bremser, W. G., and Chung, Q. 2005. "A Framework for Performance Measurement in the E-Business Environment," *Electronic Commerce Research and Application* ( 4), pp 395-412.

Browne, P. 1979. *Security: Checkllst for Computer Center Self-Audits*, AFIPS Press: Arlington, Va.

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.

Chin, W. W. 1998. "The Partial Least Squares Approach to Structural Equation Modeling," in *Modern Methods for Business Research* G. a. Marcoulides (ed.), lawrence Erlbaum: Mahwah, NJ, pp. 295-336.

Chin, W. W. 2010. "How to Write up and Report Pls Analyses," in *Handbook of Partial Least Squares: Concepts, Methods and Applications,* V. E. Vinzi, W. W. Chin, J. Henseler and H. Wang (eds.), Springer-Verlag: Berlin Heidelberg, pp. 655-690.

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.

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*, Hillsdale: NJ.

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.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp 79–98.

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.

Deal, T., and Kennedy, A. 1982. *Corporate Culture: The Rites and Rituals of Corporate Life*, Addison-Wesley: New York, NY.

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.

Denison, D. R., Haaland, S., and Goelzer, P. 2004. "Corporate Culture and Organizational Effectiveness: Is Asia Different from the Rest of the World?," *Organizational Dynamics* (33:1), pp 98-109.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in Is Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* (11:2), pp 127-153.

Dhillon, G., and Torkzadeh, G. 2006. "Value‐Focused Assessment of Information System Security in Organizations," *Information Systems Journal* (16:3), pp 293-314.

Diamantopoulos, A., and Siguaw, J. A. 2006. "Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration," *British Journal of Management Decision* (17), pp 263-282.

Diamantopoulos, A., and Winklhofer, H. M. 2001. "Index Construction with Formative Indicators: An Alternative to Scale Development," *Journal of Marketing Research* (38:May), pp 259-277.

Doherty, N. F., and Fulford, H. 2005. "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," *Information Resources Management Journal* (18:4), pp 21-39.

Douglas, M. 1985. *Measuring Culture: A Paradigm for the Analysis of Social Organization*, Columbia University Press: New York, NY.

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>.

Falk, R. F., and Miller, N. B. 1992. *A Primer for Soft Modeling*, University of Akron Press: Akron, OH.

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp 39-50.

Fowler, J. J., and Horan, P. 2008. "Are Information Systems’ Success and Failure Factors Related? An Exploratory Study," in *End-User Computing: Concepts, Methodologies, Tools, and Applications* S. Clarke (ed.), Hershey, PA: IGI Global.

Gefen, D., Straub, D., and Boudreau, M. C. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the association for information systems* (4:1), pp 2-77.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly., C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), pp 203-236.

Hanseth, O., and Braa, K. 2001. "Hunting for the Treasure at the End of the Rainbow: Standardizing Corporate It Infrastructure," *Computer Supported Cooperative Work (CSCW)* (10:3-4), pp 261-292.

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.

Hong, K. S., Chi, Y. P., Chao, L. R., and Tang, J. H. 2003. "An Integrated System Theory of Information Security Management," *Information Management & Computer Security* (11:5), pp 243-248.

Hoyt, D. 1973. *Computer Securlty Handbook*, Macmdlan: New York.

Hsu, C. W. 2009. "Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in an Organization," *European Journal of Information Systems* (18:2), pp 140-150.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), pp 615-660.

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.

Hutt, A., Bosworth, S., and Hoyt, D., eds. 1988. *Computer Securzty Handbook*, (2d ed.) Macmdlan: New York.

IBM 1972. *Secure Automated Facilities Environment Study 3, Part 2*, Armonk: NY.

ISO 2005. "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.

Jarvis, C. B., MacKenzie, S. B., and Podsakoff, P. M. 2003. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *Journal of Consumer Research* (30:199-218).

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

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp 549-566.

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.

Kaplan, R. S., and Norton, D. P. 1992. "The Balanced Scorecard-Measures That Drive Performance," *Harvard Business Review* (70), pp 71-79.

Kaplan, R. S., and Norton, D. P. 1993. "Putting the Balanced Scorecard to Work," *Harvard Business Review* (Sept–Oct ), pp 134-147.

Kaplan, R. S., and Norton, D. P. 2004. "The Strategy Map: Guide to Aligning Intangible Asset," *Strategy & Leadership* (32:5), pp 10-17.

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.

Keeney, R. L. 1994. "Creativity in Decision Making with Value-Focused Thinking," *Sloan Management Review* (35), pp 33-41.

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.

Kock, N. 2013. *Warppls 4.0*, ScriptWarp Systems: Laredo, Texas.

Kotulic, A. G., and Clark, J. G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:5), pp 597-607.

Krauss, L. 1972. *Safe: Security Audit and Field Evaluatlon for Computer Facilities and Information Systems*, Amacon: New York.

Krauss, L. 1980. *Safe: Security Audit and Field Evaluatlon for Computer Facilities and Information Systems. Revised Ed.*, Amacon: New York.

Krosnick, J. A. 1991. "Response Strategies for Coping with the Cognitive Demands of Attitude Measures in Surveys," *Applied cognitive psychology* (5:3), pp 213-236.

Lee, S., and Ahn, H. 2008. "Assessment of Process Improvement from Organizational Change," *Information & Management* (45:5), pp 270-280.

Lee, Y., and Larsen, K. R. 2009. "Threat or Coping Appraisal: Determinants of Smb Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18), pp 177-187.

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp 71-90.

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., and Pearson, J. M. 2005. "Iso 17799: "Best Practices" In Information Security Management? ," *Communications of the Association for Information Systems* (15:5), pp 577-591.

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.

MacCallum, R. C., and Browne, M. W. 1993. "The Use of Causal Indicators in Covariance Structure Models: Some Practical Issues," *Psychological Bulletin* (114:3), pp 533-541.

Malhotra, N. K., Kim, S. S., and Patil, A. 2006. "Common Method Variance in Is Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management Science* (52:12), pp 1865-1883.

Marr, B., and Schiuma, G. 2003. "Business Performance Measurement - Past, Present and Future," *Management Decision* (41), pp 680-687.

Martin, C., Bulkan, A., and Klempt, P. 2011. "Security Excellence from a Total Quality Management Approach," *Total Quality Management* (22:3), pp 345–371.

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.

Massetti, B., and Zmud, R. W. 1996. "Measuring the Extent of Edi Usage in Complex Organizations: Strategies and Illustrative Examples," *MIS Quarterly* (20:3), pp 331-345.

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

Meyers, L. S., Gamst, G., and Guarino, A. 2006. *Applied Multivariate Research: Design and Interpretation*, Thousand Oaks, CA: Sage.

Miles, R. E., Snow, C. C., Meyer, A. D., and Coleman, H. J. 1978. "Organizational Strategy, Structure, and Process," *Academy of Management Review* (3:3), pp 546-562.

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.

Myers, M. D. 2013. *Qualitative Research in Business and Management*, Sage: London.

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

Nunnally, J. 1987. *Psychometric Theory*, McGrawHill: New York.

Orlikowski, W. J., and Gash, D. C. 1994. "Technological Frames: Making Sense of Information Technology in Organisations," *ACM Transactions on Information Systems* (12), pp 174-207.

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

Parker, D. B. 2006. "Why Information Security Is Still a Folk Art," *Communications of the ACM* (49:10), p 11.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (31:4), pp 623-656.

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

Podasakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp 879-903.

Podsakoff, P. M., MacKenzie, S. B., and Podsakoff, N. P. 2012. "Sources of Method Bias in Social Science Research and Recommendations on How to Control It," *Annual review of psychology* (63:539-569).

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.

Rossiter, J. R. 2002. "The C-Oar-Se Procedure for Scale Development in Marketing," *International Journal of Research in Marketing* (19), pp 305-335.

Sabherwal, R., and Chan, Y. E. 2001. "Alignment between Business and Is Strategies: A Study of Prospectors, Analyzers, and Defenders," *Information systems research* (12:1), pp 11-33.

Saint-Germain, R. 2005. "Information Security Management Best Practice Based on Iso/Iec 17799," *The Information Management Journal* (July/August ), pp 60-66.

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

Schumacher, M. 2002. "Security Patterns and Security Standards," Proceedings of the 7th European conference on pattern languages of programs (EuroPloP), Irsee, Germany, 2002.

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

Simpson, B., and Wilson, M. 1999. "Shared Cognition: Mapping Commonality and Individuality," *Advances in Qualitative Organizational Research* (2), pp 73-96.

Singh, A. N., and Gupta, M. P. 2014. "Identifying Factors of “Organizational Information Security Management” " *Journal of Enterprise Information Management Decision* (27:5), pp 644-667.

Siponen, M. 2006. "Information Security Standards Focus on the Existence of Process, Not Its Content," *Communications of the ACM* (49:8), pp 97-100.

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., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp 487-502.

Siponen, M., and Willison, R. 2009. "Information Security Management Standards: Problems and Solutions," *Information & Management* (46:5), pp 267-270.

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

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

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. 2005. " A Holistic Risk Analysis Method for Identifying Information Security Risks," in *Security Management, Integrity, and Internal Control in Information Systems,* P. Dowland, S. Furnell, B. Thuraisingham and X. S. Wang (eds.), Springer: New York, pp. 185-202.

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

Spender, J. C. 1998. "The Dynamics of Individual and Organizational Knowledge," in *Managerial and Organizational Cognition,* C. Eden and J. C. Spender (eds.), Sage: London, UK, pp. 13-39.

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., Boudreau, M., and Gefen, D. 2004. "Validation Guidelines for Is Positivist Research," *Communications of the Associations of Information Systems* (13), pp 380-427.

Straub, D. W., and Burton-Jones, A. 2007. "Veni, Vidi, Vici: Breaking the Tam Logjam," *Journal of the Association for Information Systems* (8:4), pp 223-229.

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

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

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

Suh, B., and Han, I. 2003. "The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce," *International Journal of electronic commerce* (7:3), pp 135-161.

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

van Wesse, R., Yang, X., and de Vries, H. J. 2011. "Implementing International Standards for Information Security Management in China and Europe: A Comparative Multi-Case Study," *Technology Analysis & Strategic Management* (23:8), pp 865–879.

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

Vinzi, V. E., Trinchera, L., and Amato, S. 2010. "Pls Path Modeling: From Foundations to Recent Developments and Open Issues for Model Assessment and Improvement," in *Handbook of Partial Least Squares: Concepts, Methods and Application,* V. E. Vinzi, W. W. Chin, J. Henseler and H. Wang (eds.), Springer: Berlin Heidelberg, pp. 47-82.

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.

von Solms, R., and von Solms, S. H. B. 2006. "Information Security Governance: A Model Based on the Direct–Control Cycle," *Computers & Security* (25:6), pp 408-412.

Vroom, C., and Von Solms, R. 2004. "Towards Information Security Behavioural Compliance," *Computers & Security* (23:3), pp 191-198.

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.

Wetzels, M., Odekerken-Schröder, G., and van Oppen, C. 2009. "Using Pls Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration," *MIS Quarterly* (33:1), pp 177-195.

Wheeler, B. C. 2002. "Nebic: A Dynamic Capabilities Theory for Assessing Net-Enablement," *Information Systems Research* (13), pp 125-146.

Wiander, T. 2007. "Implementing the Iso/Iec 17799 Standard in Practice - Findings from Small and Medium Sized Software Organizations," Proceedings of the 5th international conference on Standardization, Innovation and Information Technology (SIIT 2007), Calgary, Canada., 2007.

Yeh, Y.-J., Lai, S.-Q., and Ho, C.-T. 2006. "Knowledge Management Enablers: A Case Study," *Industrial Management & Data Systems* (106:6), pp 793-810.

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.

Yin, R. K. 2013. *Case Study Research: Design and Methods*, Sage publications: CA.

1. Informed Consent Form

**Purpose of the Study**

This research aims to apply critical success factor (CSF) approach to study information security management (ISM) from organizational level. More specifically, this paper tries to answer the following research question: What critical factors make ISM effective and how these factors contribute to the success of ISM?

**Procedures involved in the Research**

You will be asked to complete a questionnaire asking for items such as your opinions about how to evaluate organizations’ information security management program and what socio-organizational factors lead to the success.

**Potential Harms, Risks or Discomforts**

There are no conceivable physical, psychological, emotional, financial, or social risks associated with the survey questionnaire.

**Potential Benefits to the Participants and/or Society**

Organizations’ managers may benefit from this research. 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, once completed with empirical validation, this study can provide managers with a way of evaluating the reliability or objectivity of the claimed best practices in practical standards and guidelines.

**Confidentiality**

Anything that you say or do in the study will not be told to anyone else. Anything that we find out about you that could identify you will not be published or told to anyone else, unless we get your permission. Your privacy will be respected. We will not be asking you to provide your name or any personal information other than some demographic information. If you are interested in knowing summary information about the results of the study, your name and contact information will be used only for sending the results. All research data will be kept for 2 years and then be deleted.

**Participation**

Your participation in this study is voluntary. If you decide to participate, you can decide to stop at any time, even after signing the consent form or part-way through the study. If you decide to stop participating, there will be no consequences to you.

In cases of survey withdrawal, any data you have provided to that point before submitting will be destroyed unless you indicate otherwise. Once you have submitted your responses for this anonymous survey, your data will be put into a database and will not be identifiable to you. This means that once you have submitted your survey, your responses cannot be withdrawn from the study because I will not be able to identify which data is yours. If you do not want to answer some of the questions you do not have to, but you can still be in the study.

**Information about the Study Results**

I expect to have this study completed by approximately one year. If you would like a brief summary of the results, please let me know how you would like it sent to you.

**Questions about the Study**

If you have questions or need more information about the study itself, please contact me at:

Zhiling Tu

DeGroote School of Business,McMaster University

Hamilton, Ontario, Canada.

Tel: (905) 525-9140 ext. 26034

tuz3@mcmaster.ca

This study has been reviewed by the McMaster University Research Ethics Board and received ethics clearance. If you have concerns or questions about your rights as a participant or about the way the study is conducted, please contact:

McMaster Research Ethics Secretariat

Telephone: (905) 525-9140 ext. 23142

c/o Research Office for Administrative Development and Support

E-mail: [ethicsoffice@mcmaster.ca](mailto:ethicsoffice@mcmaster.ca)

I have read, understood, and printed a copy of, the above consent form and desire of my own free will to participate in this study.

○ Yes

○ No

1. Survey Questionnaire

A Study of Critical Success Factors of Information Security Management

Thank you for taking time to complete this survey, which has two parts: 1) general information about your organization; 2) your perceptions about your organization’s information security management.

You can withdraw anytime as you wish without any consequence. In cases of withdrawal, any data you have provided to that point before submitting will be destroyed unless you indicate otherwise. Once you have submitted your responses for this anonymous survey, your data will be put into a database and will not be identifiable to you. This means that once you have submitted your survey, your responses cannot be withdrawn from the study because I will not be able to identify which data is yours. If you do not want to answer some of the questions you do not have to, but you can still be in the study.

Screening Question:

Are you working as information security officer or involved with decision making regarding your whole company's information security?

* Yes
* No

PART 1: Information about Your organization

1. What industry is your organization in?

* Manufacturing
* Marketing
* Finance
* Information Technology
* Hospital
* Telecommunication
* Tourism
* Education
* Entertainment
* Service
* Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Please specify)

1. How many employees in your organization?

* 1-50
* 51-200
* 201-500
* Above 500

1. What is the position of your current job?

* Chief Information Officer (CIO)
* Chief Security Officer (CSO)
* IT manager
* Information security manager
* Senior IT staff
* Other \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Please specify)

1. Has your organization applied any national or international information security standard

* No
* Yes

Please specify the name of the standard: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Where is your organization?

* North America
* Asia
* Europe
* South America
* Africa
* Other (Please specify): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Your organization is:

* Domestic
* International

PART 2: Information about Your Organization’s Information Security Management (ISM)

Please indicate the extent (on a 1-to-5 scale) to which you agree with the statements.

1. My organization’s information security management objectives reflect business objectives.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. My organization’s security policies and controls are based on business objectives, value, or needs.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, business users routinely contribute a business perspective to information security management.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, top management actively supports information security management as a vital enterprise-wide function.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, sufficient funding and resources are allocated to information security management.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. A formal organizational unit for information security is established within my organization.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, information security educational and training programs are provided to employees periodically.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, employees are aware of potential security threats and understand the need for information security management.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, employees are aware of policies, procedures, or countermeasures for information security.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, employees exhibit a sense of being proactive in protecting information security.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. My organization’s IT resources (e.g., networks, hardware, software, outsourcing, etc.) are available and flexible.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, IT staff (both inbound and outsourced) is knowledgeable and capable of developing and maintaining information security technologies.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. If you are still reading, please select “Neither Agree nor Disagree”. (Screening Question)

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, end users of IT systems follow sound operation processes.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, a formal risk management program has been designed and implemented.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, formal security policies have been defined and implemented.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, specific information security standards have been applied to enhance information security management.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. My organization’s information security management program has been useful and security deficiencies have been decreased.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. My organization’s information security management has increased the efficiency of controlling information security threats.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. I am satisfied with my organization’s information security management program.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. My organization’s information security management is cost-effective, i.e., the cost is justified by the potential benefit.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. My organization’s information security management has contributed value to organization as whole.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, top management is satisfied with the implementation of information security management.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, employees comply with information security policies.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. In my organization, employees have contributed to strengthening transaction security.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. If you are still reading, please select "Disagree". (Screening Question)

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. Customers are satisfied with my organization’s information security practices.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. The processes of planning and implementing information security management have been improved in my organization.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. My organization’s information security policies are effective and efficient to protect information asset.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. Information security standards compliance in my organization has been improved.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. My organization’s information security management program provides continuing information security training to employees.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. My organization’s information security management program prepares for potential changes and challenges, such as social networking, BYOD (Bring Your Own Device), and outsourcing.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

1. My organization’s information security management program is positioned to meet future needs.

* Strongly Disagree
* Disagree
* Neither Agree Nor Disagree
* Agree
* Strongly Agree
* Not Applicable

**Thank you very much for your participation!** [End of questionnaire.]

1. Interview Questions

A Study of Critical Success Factors of Information Security Management

Information about these interview questions: This gives you an idea what I would like to learn about the information security management in your organization. Interviews will be one-to-one and will be open-ended (not just “yes or no” answers). Because of this, the exact wording may change a little. Sometimes I will use other short questions to make sure I understand what you told me or if I need more information when we are talking such as: “So, you are saying that …?), to get more information (“Please tell me more?”), or to learn what you think or feel about something (“Why do you think that is…?”).

1) Information about you: Your job position now? Your position in information security management in your organization

2) Please tell me about your organization’s current information security policies and measures to protect information security.

3) What issues do you most concern about the information security in your organization? Please tell me more about why you think that.

3) How do you measure the performance of your organization’s information security management?

4) What factors do you think are critical to the success of your organization’s information security management? Please tell me more about why you think that?

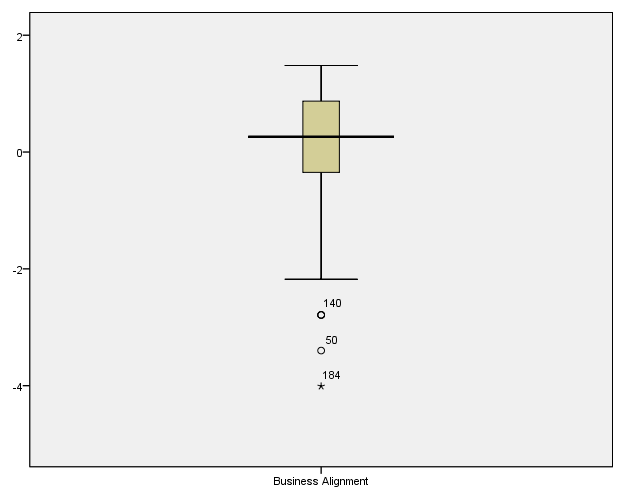
5) What aspects do you think can be improved for your organization’s information security management?

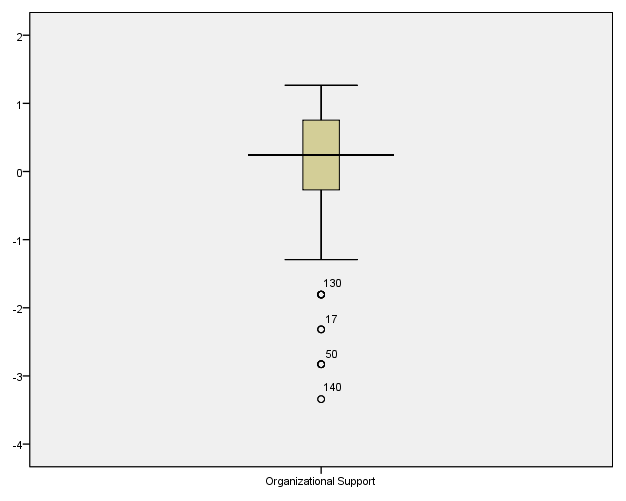
6) What do you think about the relationships between information security management and business objectives, top management, employees, technologies, or customers?

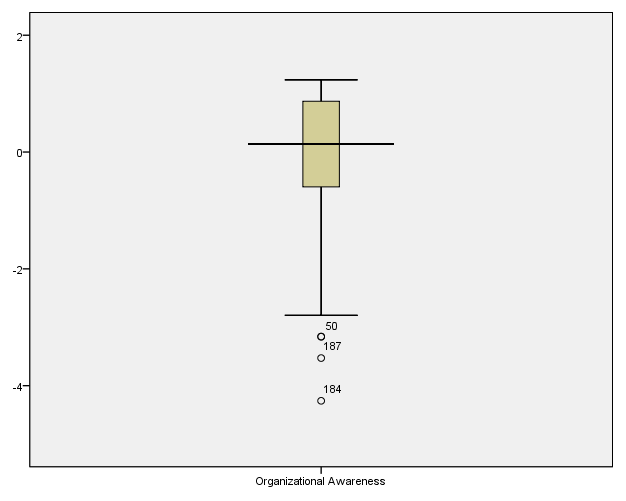
7) Do you think it is important for academics to do research on organization’s information security management? Do you have any suggestions to our study?

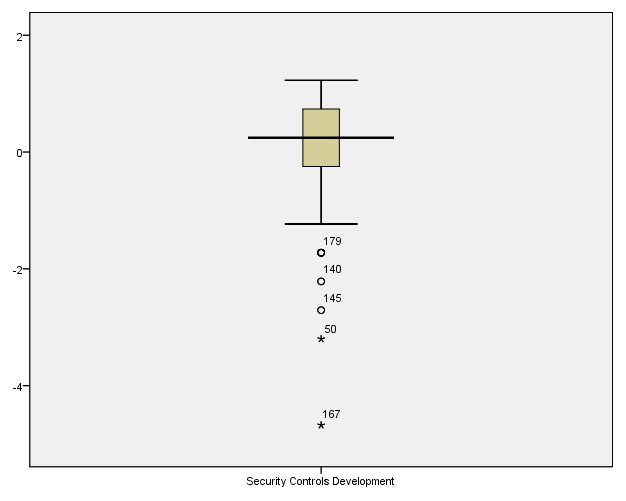
[END]

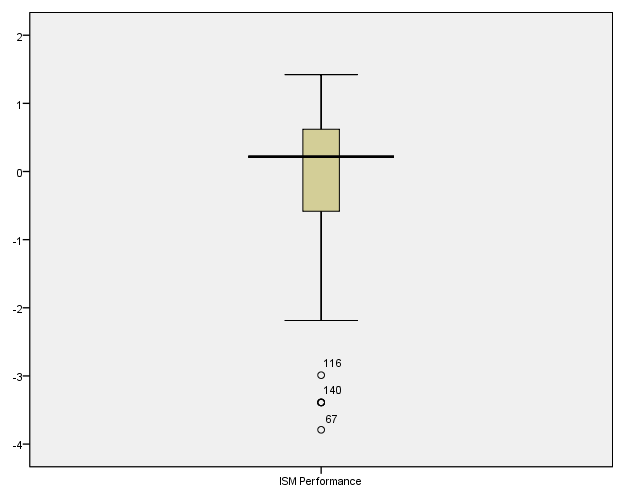
1. Composite/Indicator Box Plots

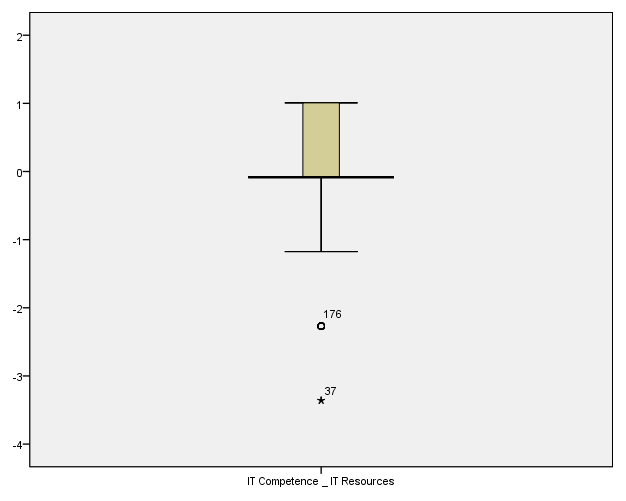


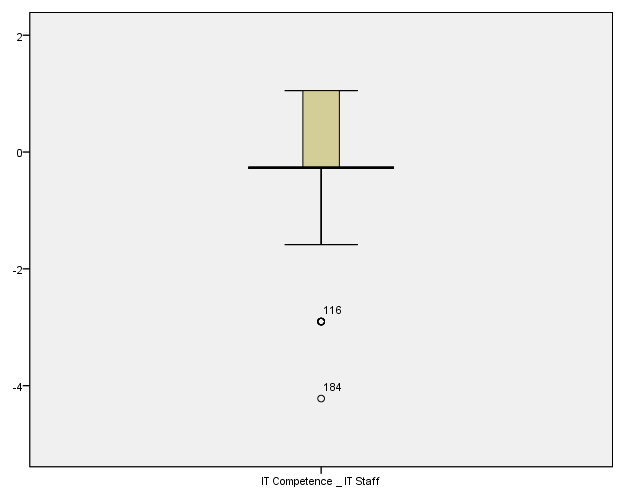


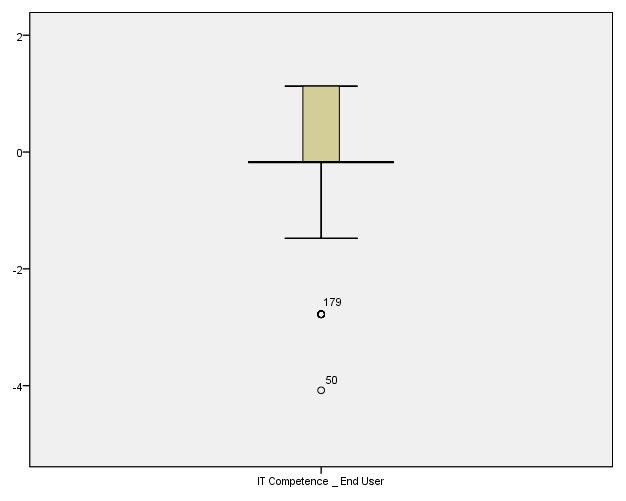










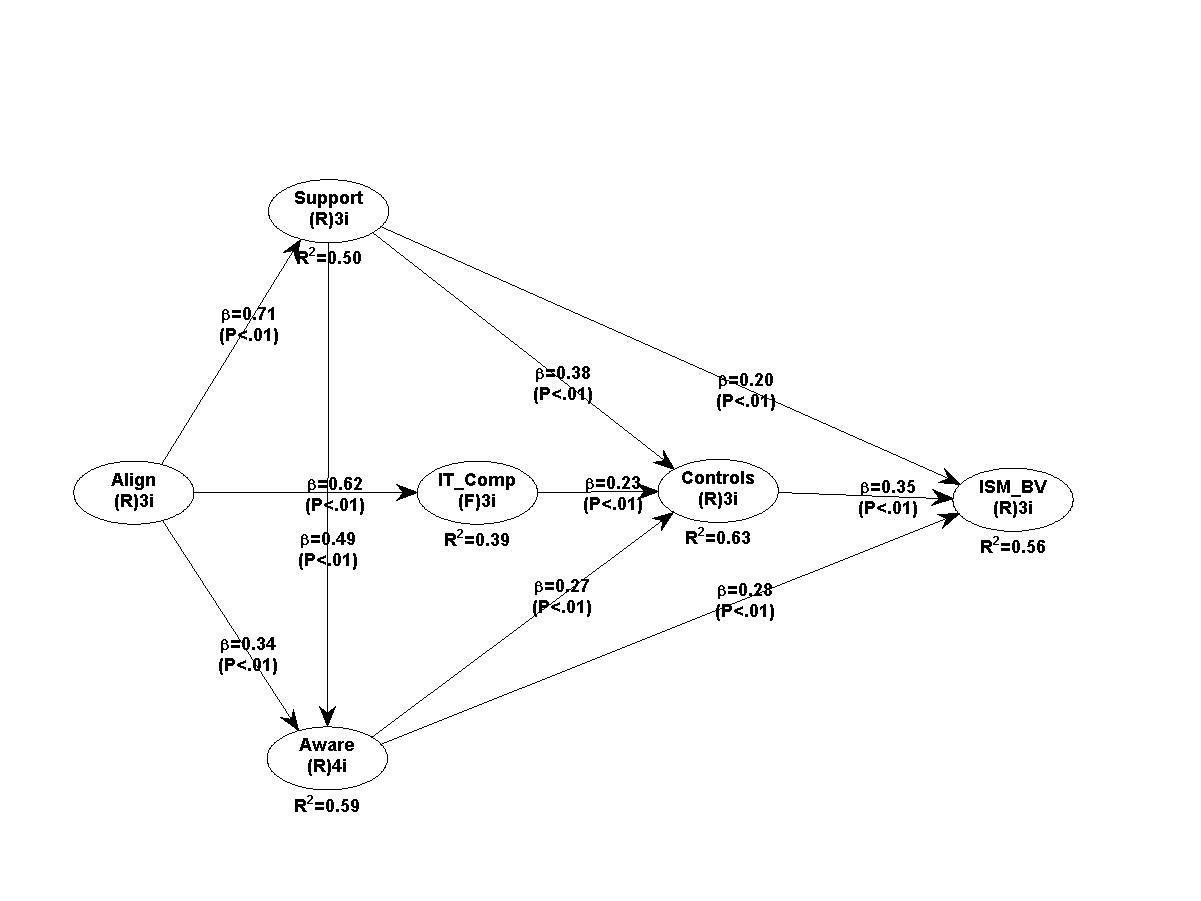


1. Bivariate Data Plots

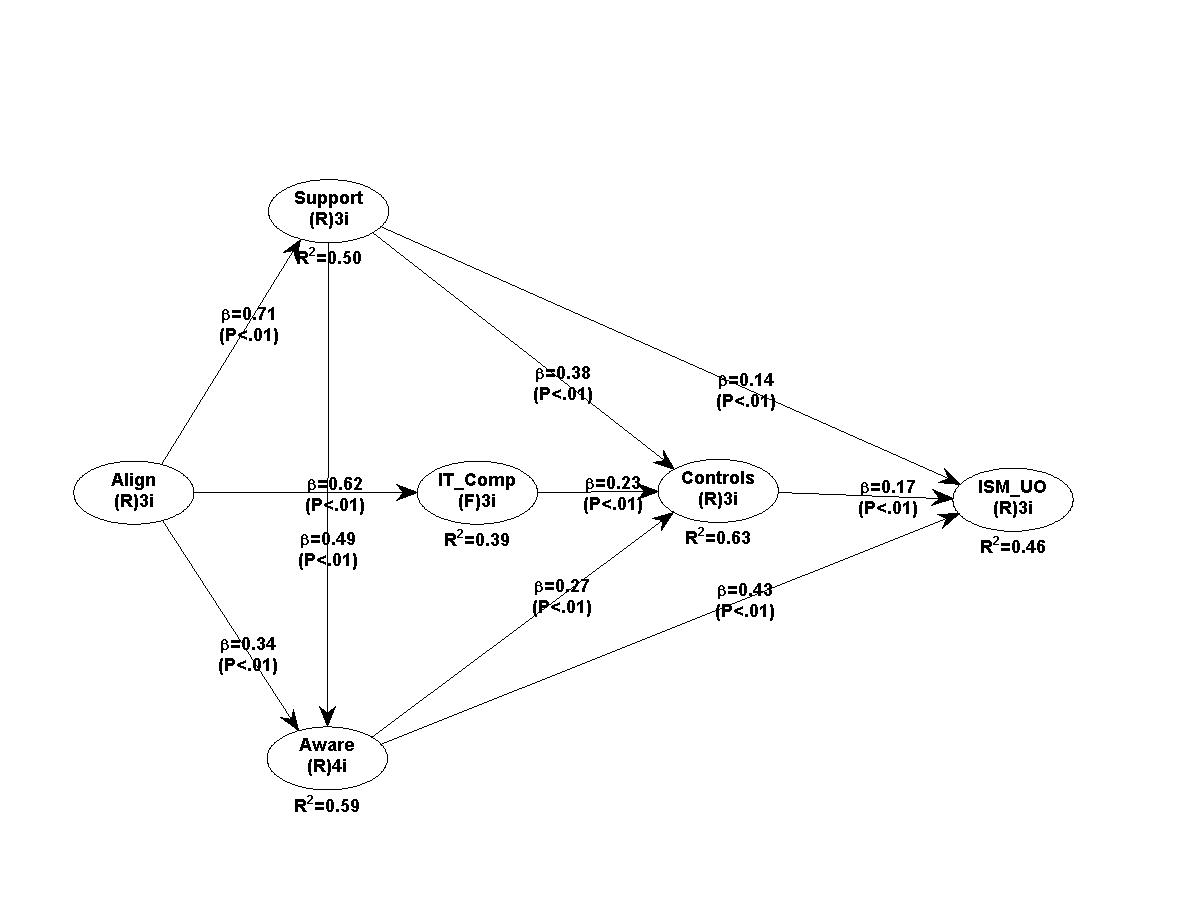
|  |
| --- |
| **Business Alignment 🡪 Organizational Support** |
| final structure model 20150408 BA-OS.jpg |
|  |
| **Business Alignment 🡪 Organizational Awareness** |
| final structure model 20150408 BA-OA.jpg |
|  |
| **Business Alignment 🡪 IT Competence** |
| final structure model 20150408 BA-IC.jpg |
|  |
| **Organizational Support 🡪 Organizational Awareness** |
| final structure model 20150408 OS-OA.jpg |
|  |
| **IT Competence 🡪 Security Controls Development** |
| final structure model 20150408 IC-SC.jpg |
|  |
| **Organizational Support 🡪 Security Controls Development** |
| final structure model 20150408 OS-SC.jpg |
|  |
| **Organizational Awareness 🡪 Security Controls Development** |
| final structure model 20150408 OA-SC.jpg |
|  |
| **Security Controls Development 🡪 ISM Performance** |
| final structure model 20150408 SC-IP.jpg |
|  |
| **Organizational Support 🡪 ISM Performance** |
| final structure model 20150408 OS-IP.jpg |
|  |
| **Organizational Awareness 🡪 ISM Performance** |
| final structure model 20150408 OA-IP.jpg |

1. Alternative Model Test Results

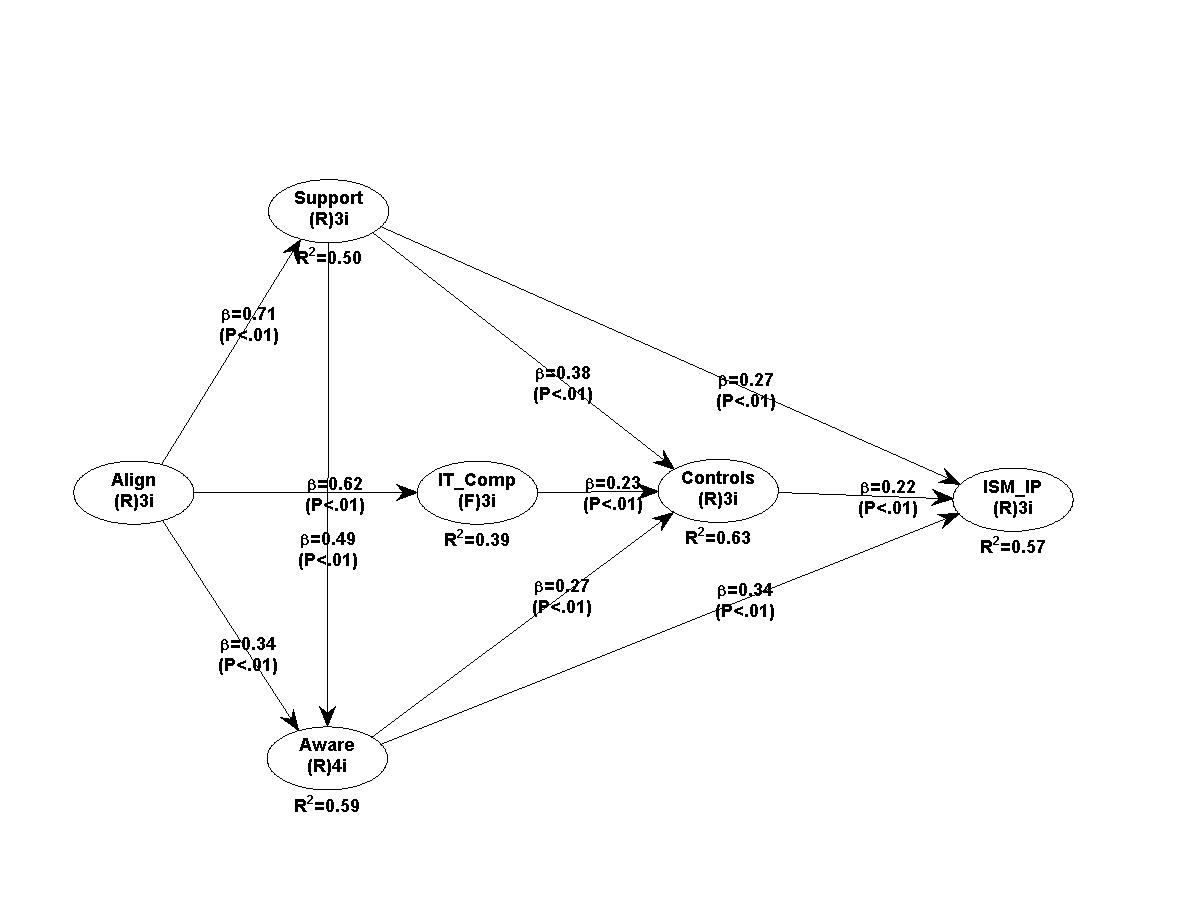
ISM Performance measured by Business Value



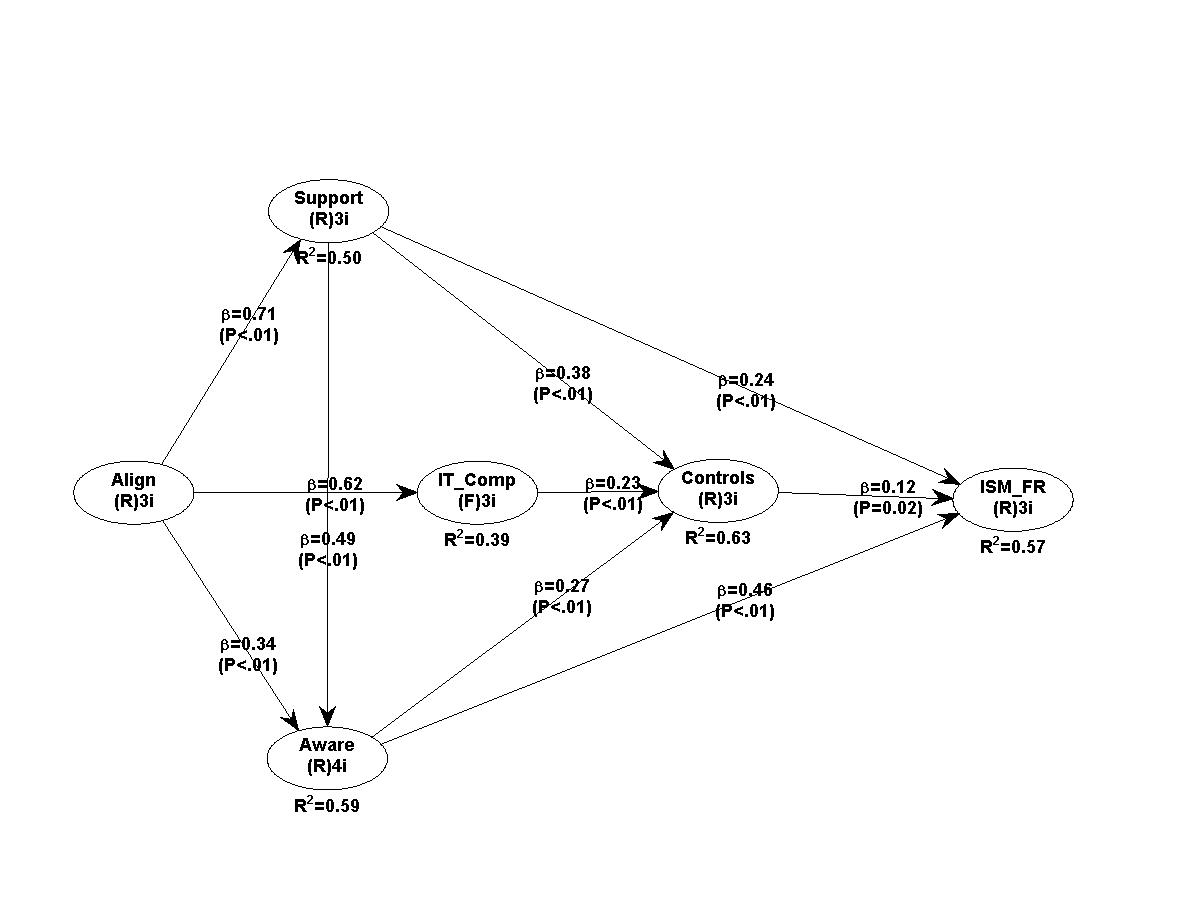
ISM Performance measured by User Orientation



ISM Performance measured by Internal Process



ISM Performance measured by Future Readiness



1. US cybercrime: Rising risks, reduced readiness ---- Key findings from the 2014 US State of Cybercrime Survey, http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf [↑](#footnote-ref-2)
2. “Information technology — Code of practice for information security management” [↑](#footnote-ref-3)
3. www.empanelonline.com. [↑](#footnote-ref-4)
4. www.empanelonline.com [↑](#footnote-ref-5)
5. http://www.scriptwarp.com/warppls/ [↑](#footnote-ref-6)
6. Item loadings in this table correspond to the initial item loadings obtained in a principal component analysis performed in SPSS. [↑](#footnote-ref-7)
7. Unlike other PLS software packages which need the users to calculate values, WarpPLS 4.0 provides users with the values directly. [↑](#footnote-ref-8)
8. https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf [↑](#footnote-ref-9)