2015

Intrinsic Motivation and Information Systems Security Policy Compliance in Organizations

Yurita Yakimin Abdul Talib
Virginia Commonwealth University

Intrinsic Motivation and Information Systems Security Policy Compliance in Organizations

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctoral of Philosophy in Business at Virginia Commonwealth University

by

Yurita Yakimin Abdul Talib

Chair : Professor Gurpreet Dhillon

Information Systems Department, School of Business

Virginia Commonwealth University
Richmond, Virginia
2015

Dedication

I dedicate this dissertation to my loving family. Without the enduring love, sacrifice, and unwavering emotional support from my husband, Hisham, and my children, Fitri, Fahmi and Aisyah, the pursuit of my doctorate degree would not have been possible. Primarily, I would like to express gratitude to my husband for his incredible support during this journey. Thank you for keeping me sane during my tenure at VCU. I am also grateful for the endless prayers, doa, and encouragement I received from my father, my mother, and my siblings. This accomplishment is just as much yours as it is mine.

I love you all. `

Yurita Yakimin Abdul Talib

Acknowledgement

First and foremost, I would like to thank Allah S.W.T, the Almighty. You have given me the strength to believe in myself and pursue my dreams. I could never have done this without Him.

It is with immense pleasure to express my sincere and deep sense of gratitude to my supervisor and my dissertation Chair, Dr. Gurpreet Dhillon, for his faith in me, and his efforts to advise and support me throughout the three years of my dissertation endeavor. Not only did he supervise my progress, but he also provided mentorship regarding topics outside of academia.

I am also thankful for the guidance from my committee members, Dr. Manoj Thomas, Dr. Richard Redmond, Dr. Sven Kepes, and Dr. Victoria Yoon. Each member contributed to the completion of my dissertation. I want to express special appreciation to Dr. Sven Kepes for all of the time he sacrificed helping me understand new methodology. He spent countless hours reviewing and contributing his intellectual discourse.

I cherish the friendships I made at VCU, and I would like to take this opportunity to thank all of them. My friends consistently provided encouragement and motivation that I needed to graduate. I would also like to thank my dearest Malaysian friends in Northern Virginia, Washington DC, and Maryland for giving my family and me a second home. I embrace all of my friendships that we built based on love, sincerity, and honesty. I love you all.

Finally, I express my gratitude to my employer, Universiti Utara Malaysia (UUM), and the staff for their help and co-operation. I also extend my appreciation to the Ministry of Education, Government of Malaysia, for their scholarships.

Table of content

List of figures

List of tables

Abstract

Intrinsic Motivation and Information Systems Security Policy Compliance in Organizations

by Yurita Yakimin Abdul Talib

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctoral of Philosophy in Business at Virginia Commonwealth University

Virginia Commonwealth University, 2015

Chair: Professor Gurpreet Dhillon
Department of Information Systems, School of Business

Incidents of computer abuse, proprietary information leaks and other security lapses have been on the increase. Most often, such security lapses are attributed to internal employees in organizations subverting established organizational IS security policy. As employee compliance with IS security policy is the key to escalating IS security breaches, understanding employee motivation for following IS security policy is critical. In addition to several types of extrinsic motives noted in prior studies, including sanctions, rewards, and social pressures, this study adds that an important contributing intrinsic factor is empowerment. Per Thomas and Velthouse's (1990) intrinsic motivation model, empowerment is the positive feelings derived from IS security task assessments. Through survey data collected from 289 participants, the study assesses how

dimensions of psychological empowerment (i.e., competence, meaning, impact, and choice) as derived from IS security task may impact the IS security performance of the participants, measured by their compliance with IS security policy. The study demonstrates that the competence and meaning dimensions of psychological empowerment have a positive impact on participants' IS security policy compliance intention, while impact has a marginal negative influence on compliance. Furthermore, dimensions of psychological empowerment can be predicted by structural empowerment facets, particularly IS security education, training, and awareness (SETA), access to IS security strategy and goals, and participation in IS security decision-making. In addition, the competence and meaning dimensions of psychological empowerment may act as mediators for the relations between structural empowerment and participants' IS security policy compliance. Theoretical contributions, managerial implications, and directions for future research of this study will be discussed.

Keywords: IS security policy compliance, intrinsic motivation, psychological empowerment, structural empowerment

.

Chapter 1. Introduction

1.1 Overview

This study concerns employee information systems (IS) security policy compliance in organizations. IS security policy compliance is the act or process of conformity to official requirements, including disposition to yield to others (Herath and Rao, 2009a; Bulgurcu et al., 2010). The consequences of not complying with IS security policy may include insider security breaches, which pose a significant threat. Over the years, a large body of researchers has attempted to understand the motivations that influence IS security policy compliance. A general conclusion of prior research is that extrinsic motivational factors are the main reasons for an individual to engage in acts that lead to compliance with IS security policy (e.g., Straub, 1990; Pahnila et al., 2007; Bulgurcu et al., 2010).

There have been some studies that point to the importance of intrinsic motivational factors with respect to IS security policy compliance (e.g., Herath and Rao, 2009a; Son, 2011). Such studies are, however, limited and lack theoretical support. Responding to the limited body of work in this area, this research attempts to fill the gap in the body of literature besides heeding to the various calls for undertaking research in the area of intrinsic motivation for IS security policy compliance (see Herath and Rao, 2009a; Son, 2011; Padayachee, 2012). The intrinsic motivation model from Thomas and Velthouse (1990) is used to investigate the influence of four dimensions of psychological empowerment (perceptions of competence, meaning, impact, and choice) on IS security policy compliance. In addition, intrinsic motivation theorists have argued

that feelings of empowerment not only arise from the innate part of individuals and derived from a task, but also driven by factors external to the individuals (Deci and Ryan, 1985; Conger and Kanungo, 1988; Thomas and Velthouse, 1990). Prior studies in IS security compliance have suggested various external factors and strategies, such as training, task design, and etc, to enhance an employee intrinsic motivation (Herath and Rao, 2009a; Bulgurcu et al., 2010; Son, 2011). However, rather than exploring the range of strategies empirically, the studies simply acknowledged their importance. This current study extends prior research to explore the factors that enhance individual intrinsic motivation.

This chapter is organized as follows. Section 1.2 provides the definitions of important concepts. Section 1.3 addresses the research problem, specific research questions, and contributions of the study, as well as the overall organization of the dissertation.

1.2 Definitions

In recent years, the term IS security policy compliance has received a great amount of attention from researchers and practitioners alike (Straub, 1990; Siponen et al., 2007; Herath and Rao, 2009a; Myyry et al., 2009). This section explores the concept of IS security policy compliance in organizations. Two classes of definitions form the basis for developing an understanding of IS security policy compliance, specifically information systems security and information systems security policy.

Information Systems Security

IS security refers to a range of activities to control and manage potential threats to data or information. Such controls help ensure confidentiality, integrity, and availability of data (Loch et al., 1992). Dhillon (2007) considered IS security at three levels of control: technical, formal,

and informal. He argues that any discordance between the three levels may result in potential security issues.

Technical controls aim at securing the hardware, software, and information held in the computer systems. Dhillon (2007) identified six categories of threats to the hardware, software, and the data which reside in computer systems that may lead to a compromise – modification, destruction, disclosure, interception, interruption, and fabrication. Thus, in protecting technical systems, controls are normally assigned in the area of access control and authentication (Dhillon, 2007). This might include the application of smart card technology, or the development of block ciphers, voice analysis, and digital signature. These technology-oriented security controls have generally helped the organizations to safeguard sensitive information.

However, IS security problems cannot be dealt by mere technical controls. For instance, perpetrators may find it easier to procure information from documents left in the garbage rather than electronically via computer systems (Dhillon, 2007). Technological controls require support from formal controls. Formal controls refer to a proper security responsibility and authority structures, establishment of all-encompassing strategy and policy, and adequate business processes. Furthermore, identifying roles and the right people in an organization is needed to ensure that responsibility, strategy and policy, and business processes are sustained (Dhillon, 2007).

Even formal controls (i.e., the rules and procedures) cannot work on their own (Bulgurcu et al., 2010). In order to ensure that formal controls work, it is essential that people adopt and accept them (Dhillon, 2007; Bulgurcu et al., 2010). The process of adopting formal controls involves communication amongst individuals in an organization. Such communication may be formal or informal. Good communication ensures that controls get socialized into an

organization. Balancing the values and attitudes of employees and ensuring the general integrity of the edifice is at the heart of the socialization process.

IS Security Policy

IS security policy is a part of the formal control structure. A policy sketches the security roles and responsibilities, and standard operating procedures for protecting the information resources of a firm (Dhillon, 1997; Bulgurcu et al., 2010). Hence, IS security policy is defined as a baseline statement of the IS security tasks or IS security-related activities that employees should do to ensure the information of their organizations is protected. The IS security tasks include the appropriate use of computer and network resources, good password habits, frequently backing up files, checking for encryptions, manual virus-check, not sharing the computer with others, locking the computer, and etc. (Albrechtsen and Hovden, 2010; Dhillon, 2007; Herath and Rao, 2009a). Typically, IS security policies are informed by current practices of a firm; however, various international standards are increasingly used as a basis for defining practices. The US National Institute of Standards and Technology (NIST) 800 series documents have been extensively used to define security policies. Various other standards such as ISO 17799 (now ISO 27002) and GASSP (Generally Accepted Security System Principles) also exist.

The essence of most standards has been succinctly captured by Kwok and Longley (1999) in their classic Handbook of Information Security where they note that any IS security policies should include the following:

- Definition of information security;
- Statement of management's intention supporting the goals and principles of information security;

- Explanation of the specific security policies, principles, standards, and compliance requirements; and
- Definition of general and specific responsibilities for all aspects of information security explanation of the process for reporting suspected security incidents

IS Security Policy Compliance

IS security policy compliance refers to the act of an individual carrying out IS security tasks to maintain IS security, as stipulated by IS security policies (Chan et al., 2005; Herath and Rao, 2009b). IS security tasks that employees required to perform demand additional time and effort (Bulgurcu et al., 2010). A study by Albrechtsen (2007) discovered that employees may choose not to perform many IS security tasks for reasons of convenience. The employees prioritize other work tasks more than their IS security tasks (Herath and Rao, 2009a). It follows that to comply with IS security policy means investing more effort and time to execute or implement the IS security tasks.

1.3. Research problem, questions and contributions

Past research has argued that employee compliance with organizational IS security policy is motivated by two types of factors, extrinsic and intrinsic (Herath and Rao, 2009a; Son, 2011; Padayachee, 2012). *Extrinsic factors* include sanctions (Bulgurcu et al., 2010), rewards (Boss et al., 2009), social pressure (Herath and Rao, 2009a), and social climate (Chan et al., 2005). Although extrinsic motivation explains employee IS security policy compliance, it is not without limitations. For instance, the observed result of the extrinsic motivation is not always consistent with theory, largely because individuals are able to neutralize or justify their potentially actions (Siponen and Vance, 2010). Neutralization refers to psychological techniques, such as defense of necessity, denial of injury, and denial of responsibility, which people use to enable themselves to

commit rule breaking or wrongdoing actions (Sykes and Matza, 1957). One problematic issue is that neutralization is unobservable (Albrecth et al., 2004). Since neutralization is unobservable, it becomes difficult to remedy it. Furthermore, individuals who feel controlled or oppressed by the external forces (e.g., sanctions, rewards, social pressure) might not fully endorse the behavior and are predicted to show poor persistence in performing a related task (Deci et al., 1999). Thus, organizations might only gain a temporary IS security advantage, if any, through extrinsic mechanisms.

Intrinsic factors may also explain employee IS security policy compliance behavior. For instance, perceived effectiveness of the IS security tasks (Herath and Rao, 2009a), perceived self-efficacy to execute IS security tasks (Rhee et al., 2009), and perceived ownership of IS (Anderson and Agarwal, 2010) influence individuals to take IS security actions. It is an individual's innate desire to act and/or intrinsic values derived from the IS security tasks that motivates him/her to carry out IS security actions. In fact, the intrinsic factors are stronger predictors of IS security behavior that the extrinsic factors (Son, 2011). Intrinsic motivation models (e.g., Hackman and Oldham, 1980; Deci and Ryan, 1985; Thomas and Velthouse, 1990) provide the logical backdrop for the argument that intrinsic motivation could influence individuals to expend time and energy to perform a specific task. However, there is a paucity of research examining the relations between intrinsic factors and employees IS security behavior. There are two primary motivations which influence IS security behavior—extrinsic and intrinsic: the latter is deserving of greater empirical attention (Herath and Rao, 2009a; Son, 2011; Padayachee, 2012).

To examine the relations between intrinsic motivation and IS security policy compliance behavior, this study draws upon Thomas and Velthouse's (1990) intrinsic motivation model.

Thomas and Velthouse (1990) noted that "intrinsic motivation involves positively valued experiences that the individual derives directly from the task" (p. 688). The principle of the model is on task assessments regarding four dimensions of psychological empowerment: perceived competence, meaning, impact, and choice. That is, an individual feels empowered if he/she perceives that he/she has the capability to perform task activities skillfully and successfully, if the value of the task is consistent with his/her personal beliefs, if he/she can make a significant difference or contribute to the organization if he/she executes the task, and finally, if he/she feels autonomy in the tasks.

Prior studies have argued that feelings of empowerment exerts influence on individuals to put more effort to execute and perform the task well (Hackman and Oldham, 1980; Deci and Ryan, 1985; Thomas and Velthouse, 1990; Spreitzer et al., 1997; Kraimer et al., 1999; Liden et al., 2000). While empirical studies have found that these four dimensions are capturing an essence of the psychological empowerment construct (Spreitzer, 1995a; Kraimer et al., 1999), researchers have argued that it is also crucial to tease apart which psychological empowerment dimensions actually drive the associations with outcomes (Spreitzer et al., 1997; Kraimer et al., 1999; Maynard et al., 2012). In fact, studies have found that each dimension contributes to different outcomes (Spreitzer et al., 1997; Kraimer et al., 1999). This study extends prior research by examining which dimensions of psychological empowerment can best explain employees' compliance with IS security policy. This study also not only responds to the gaps in the IS security literature, but also the empowerment literature by investigating the influences of each dimension of psychological empowerment on IS security policy compliance.

In addition, this study seeks to investigate factors that drive individuals' intrinsic motivation. Intrinsic motivation theorists have argued that feelings of empowerment are not only

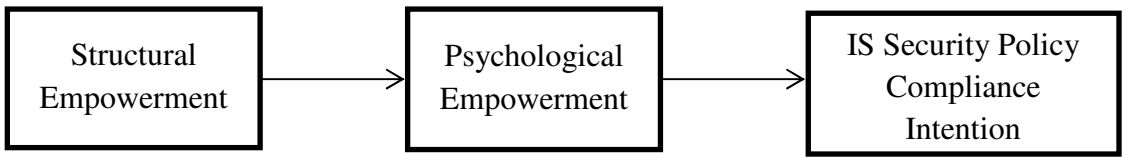
emerge from individuals' assessment of their tasks, but also from factors external to the individuals (Deci and Ryan, 1985; Conger and Kanungo, 1988; Thomas and Velthouse, 1990). Ryan and Deci (2000) called for additional research to investigate factors that enhance individuals intrinsic motivation. This has not been investigated within the IS security behavior literature. Therefore, this study seeks to answer this call by examining several organizational factors, which are expected to influence individuals' feelings of empowerment. Specifically, this study investigates the impact of structural empowerment on psychological empowerment.

Structural empowerment refers to conditions or practices where an organization provides all levels of employees with more access to power tools—defined as opportunity, resources, information, and support (Kanter, 1977). Prior studies have provided strong evidence that structural empowerment drives individual psychological empowerment (Spreitzer, 1996; Siu et al., 2005; Wallach and Mueller, 2006; Zhang and Bartol, 2010; Seibert et al., 2011). In the literature, empowerment work practices have been discussed extensively and various elements of structural empowerment have been suggested, such as training, participation in decision-making, and access to information (Spreitzer, 1996; Zacharatos et al., 2005; Seibert et al., 2011; Maynard et al., 2012). Often, these practices are 'bundled' together into one construct, making it difficult to identify which element of structural empowerment is actually associated with psychological empowerment (Maynard et al., 2012). Therefore, Maynard et al. (2012) called for future research to conduct in-depth considerations of the associations between various elements of structural empowerment on the dimensions of psychological empowerment. Thus, this study examines how empowerment work practices in terms of security education, training, and awareness (SETA) programs, access to organizational IS security strategy and goals, and participation in IS security decision-making, predict the four dimensions of psychological empowerment.

Structural empowerment is associated with psychological empowerment. In turn, both are related to performance-related outcomes at various levels (i.e., individual, team, or unit). This notion has been supported in numerous studies (Spreitzer, 2007; Maynard et al., 2012). This means that psychological empowerment serves as a mediator between structural empowerment and behavioral outcomes. Nielsen (1986) claimed that changing the organizational structural context is not enough to change individual behavior; ultimately, an individual feeling of empowerment is necessary to influence such behaviors (cf. Spreitzer, 1995b). Consistent with

Figure 0.1: Conceptual Model

psychological empowerment on the relations between elements of structural empowerment and IS security policy compliance intentions. Figure 1.1 displays the conceptual structure of this study.



Given the background and overview of the research problem, this study aims to extend the knowledge about employee IS security policy compliance by investigating the influence of psychological empowerment. In summary, this study addresses the following research questions:

1) What is the impact of employees' psychological empowerment, particularly perceptions of competence, meaning, impact, and choice, on IS security policy compliance intentions?
2) How do elements of structural empowerment, including IS security education, training, and awareness (SETA), access to information regarding IS security strategy

and goals, and participation in IS security decision-making, enhance the dimensions of psychological empowerment with respect to IS security?

3) How do dimensions of psychological empowerment mediate the relations among elements of structural empowerment and IS security policy compliance intentions?

To address these questions, this study aims to develop a conceptual research framework that evaluates employees IS security policy compliance intentions based on Thomas and Velthouse's (1990) intrinsic motivation model and Kanter's (1977) structural empowerment theory. A cross-sectional survey of individuals working in a broad spectrum of firms in the United States (US) is used to provide empirical support.

The study will contribute to both researchers and practitioners for several reasons. First, from a theoretical standpoint, an adoption of Thomas and Velthouse's (1990) intrinsic motivation theory in IS security context is new. The study will enrich the current body of knowledge on factors that improve IS security behavior at the workplace. From a practical perspective, the results may be able to help in defining the best practices for managing employee behavior with respect to IS security. Finally, the findings are hoping to offer valuable guidelines for designing and implementation of IS security program in an organization.

The following paragraph outlines the structure of the dissertation and gives a brief summary of each of the remaining chapters. This dissertation is organized into seven chapters. Following an introduction, the second chapter reviews the literature in the area of employee IS security policy compliance. Self-determination theory is used as a conceptual map. In particular, research related to extrinsic and intrinsic motivation and their impact on employee security behavior is reviewed, and the gaps are identified. Further, the theoretical foundation of the study is also discussed. The third chapter presents the research hypotheses. The potential antecedents

influencing an employee compliance with IS security policy are identified and relevant hypotheses are developed. The fourth chapter sketches the research methodology used to conduct this research (e.g, data collection approaches and procedures). The fifth chapter presents the analysis and the results of the study. The sixth chapter analyzes and synthesizes the findings in the previous chapter. The final chapter provides the conclusion of the study that includes a review of the findings, a discussion of the practical and theoretical implications of the study, along with a discussion of the limitations and possible future research directions.

Chapter 2. Literature Review

2.1 Introduction

The expectations of an IS security policy do not necessarily translate into desirable security actions (Bulgurcu et al., 2010). For instance, a survey by Ponemon (2009) found that while more than 71% of respondents were aware of their organizational password sharing security policy, 47% admitted sharing passwords with coworkers. This type of disconnect between IS security responsibilities and real-world practices poses a significant challenge for managing IS security breaches. The consequences of such breaches can be significant. In fact, recent Computer Security Institute (CSI) industry surveys have shown how insider IS security breaches are a prevalent problem and are more costly to handle than outsider IS security breaches (Richardson, 2011). It is therefore important to investigate the factors that motivate employees to execute the IS security tasks as prescribed in the IS security policies (Straub, 1990; Herath and Rao, 2009a; Bulgurcu et al., 2010).

This section of the dissertation begins with a review of the current body of literature regarding IS security policy compliance behaviors. Two orientations of motivation have emerged within the IS security policy compliance literature to explain types of motivation for compliance. Motivation may be intrinsic or extrinsic. As a result of the review of both orientations, it has been discovered that the intrinsic motivation perspective remains under-researched (Herath and Rao, 2009b; Padayachee, 2012). Thus, drawing upon the intrinsic motivation model of Thomas and Velthouse (1990), a logical argument explaining how and why intrinsic factors can serve as

mechanisms to encourage IS security policies compliance is discussed. Next, based on Kanter's (1977) structural empowerment model, potential drivers to enhance intrinsic motivation are discussed.

2.2 Motivations for IS security policy compliance

A person who feels impetus or inspirational to act is considered motivated (Deci and Ryan, 2000). Ryan and Deci (2000), in their self-determination theory (SDT), organized the distinction of factors to motivate people to take action into two paradigms, extrinsic and intrinsic motivation. The term 'extrinsic motivation' (Ryan and Deci, 2000) refers to "doing something because it leads to a separable outcome" (p. 55). It relates to an individual's belief that he/she will attain some separable outcome or instrumental value when carrying out specific activity. For example, employees who perform a IS security task due to fear of sanctions for not doing it are extrinsically motivated, they perform the task in order to attain the separable outcome of avoiding sanctions (Straub, 1990).

Intrinsic motivation has been surmised by Broedling (1977) as a "catchall explanation whenever behaviors occur which cannot be clearly linked to external outcomes" (p. 268). Deci and Ryan (2009) further stated that the definition of intrinsic motivation is based on two axioms. First, intrinsic motivation exists within individuals, suggesting that an individual's motivation to act comes from intrinsic regulation or from the self, not from others (Deci and Ryan, 2000). Second, intrinsic motivation exists within the relations between individuals and tasks, suggesting that engagement in an activity may be rewarding in itself. Intrinsic motivation is based on an assessment of how the task engagement provides satisfaction or fulfillment of innate psychological needs or desires (Ryan and Deci, 2000). In other words, the reward is in the activity itself (Deci and Ryan, 2009). For instance, employees who use computer software in the

workplace due to the inherit enjoyment of using it are intrinsically motivated (Davis et al., 1992). In the following section, extrinsic and intrinsic motivation for IS security policy compliance are reviewed.

Extrinsic motivation and IS security policy compliance

One extrinsic motivator for IS security policies compliance which has received a great deal of attention in the scientific literature is *sanctions*. A sanction is described as a negative stimulus or a negative incentive to discourage individuals from performing acts or taking decisions that are not aligned with organizational goals. Straub (1990) explained that the concept of sanction is derived from from general deterrence theory (GDT) and is used by traditional disciplinary systems to intimidate employees. In the IS security literature, a sanction is classified into the two subcategories of certainty and severity. Certainty of a sanction refers to the possibility that an employee's wrongdoing act will be caught, whereas severity of sanction denotes the degree of punishment if caught (Nagin, 1975). The concept of sanctions assumes humans to be fundamentally rational; hence, the theory argues that people are less likely to perform deviant acts if they believe the risk of being punished is high and the punishment severe (Nagin, 1975).

GDT has had significant influence amongst the IS security scholars (Straub, 1990; Siponen et al., 2007; Myyry et al., 2009; Bulgurcu et al., 2010; Chen et al., 2012). Straub (1990) conducted an empirical field study among 1,211 employees from multiple organizations to identify strategies for reducing computer abuse. The results suggested that when the certainty and severity of sanctions for violations are clearly stated and communicated, employees are highly motivated to use computers appropriately. Similarly, in the context of IS security compliance, Siponen et al. (2007) integrated GDT, protection motivation theory (PMT), and the

theory of reasoned action (TRA) to investigate the impact of sanctions on adherence to IS security policies. The study consisted of 917 employees in four Finnish organizations. They found that sanctions had a significant impact on actual compliance with IS security policies.

In addition, Bulgurcu et al. (2010) adopted the rational choice theory (RCT) to examine how individuals make decisions when facing choices in terms of compliance or noncompliance. The theory purports that employees make decisions based on an overall assessment of the consequences of the decision (e.g., compliance with IS security policies). In their study, one assessment of consequences used was the cost of noncompliance. The authors postulated that an employee's belief about the cost of noncompliance were shaped by sanctions. They measured sanctions as tangible or intangible penalties, monetary or nonmonetary penalties, and unfavorable personal mention in oral or written assessment reports. Bulgurcu et al. (2010) predicted that sanctions would drive an employee's belief about the cost of noncompliance, which then influences decisions to comply. Based on data collected from 464 employees in the US who had some familiarity with the requirements of their organizational IS security policies, their general ideas and predictions were supported.

Monitoring

Organizations have responded to an increase in insider security breaches through the implementation of control-based monitoring to increase compliance with rules and regulations (Urbaczewski and Jessup, 2002), despite concerns for cost, privacy, trust, performance, productivity, and satisfaction (Stanton and Weiss, 2000; Mirchandani and Motwani, 2003; Sipior and Ward, 2009; Smith and Tabak, 2009). A 2010 Cyber Security Watch survey found that 64% of organizations monitor employee Internet connections, whereas 46% and 32% of organizations monitor the online activities of suspicious and disgruntled employees, respectively (CSO, 2010).

Knowing that information is easily transmitted electronically, organizations have increased monitoring of e-mails to prevent the possibility of leaking trade secrets and business strategies (Dominique, 1999).

Monitoring techniques range from the evaluation of employee security behaviors to the electronic surveillance of computer, e-mail, and Internet activities (Straub and Nance, 1990; Ariss, 2002; Siau et al., 2002; Stanton et al., 2005; Boss et al., 2009; Smith and Tabak, 2009). Evaluation refers to the application of a feedback system on the output by means of audit and performance evaluations (Kirby and Davis, 1998; Stanton and Weiss, 2000; Urbaczewski and Jessup, 2002; Boss et al., 2009). Evaluation uses data to determine whether an employee has appropriately performed the required security practices and procedures as prescribed in the IS security policies (Kirsch, 2004). Unless constant evaluation of employee security behaviors is established, the existence of IS security policies remains meaningless (Boss et al., 2009). For instance, an IS security auditor may use a server log to track employee IS security online activities or employers can physically examine any employees' computer system (Boss et al., 2009).

Dhillon (2001) stated that informal evaluations, such as interpreting employee behavioral changes, may also be useful in establishing adequate checks and balances. Within the IS security literature, the evaluation of employee security behavior is based on the belief that when employees realize that their IS security activities are being monitored and assessed for compliance, this knowledge creates a sense of social pressure on them to conform to desired behavior (Wathne and Heide, 2000; Boss et al., 2009). A study conducted by Boss et al. (2009), used 1698 valid responses from all levels of employees at one organization in the US to examine the association between evaluation and IS security compliance behaviors. This results suggested

that evaluation makes employees feel that the IS security policies is mandatory; hence, it positively impacts their compliance behaviors.

Studies have also focused on electronic surveillance systems to monitor employee usage of the Internet and e-mail at the workplace (Straub, 1990; Ariss, 2002; Siau et al., 2002; Tabak and Smith, 2005). Typically, employers monitor Internet usage to control non-essential browsing, reduce bandwidth abuse, and eliminate downloads of pirated software (Siau et al., 2002). E-mail usage is typically scrutinized to prevent wrongful transmitting of confidential organizational data (such as trade secret and business strategies), e-mail spamming, and downloading of potential viruses (Siau et al., 2002).

D'Arcy et al. (2009), in a study involving 269 employees from eight organizations in the US, found that when computer monitoring is known to be in place, incidents of IS misuse drop significantly. Prior to this study, Straub (1990) found a positive association between monitoring and the frequency of changing one's password. Employees tended to comply with a password security policy because they knew that they are being monitored. Other research has supported the idea that monitoring activities of deviant behaviors increases the perception of sanctions and punitive consequences. Fears of sanctions should motivate potential deviants to comply with the rules and policies (Straub and Nance, 1990; Tyler and Blader, 2005; D'Arcy et al., 2009).

Rewards

A reward is an element of positive control, which is implemented with the goal of encouraging conformity with the desired behaviors (Boss et al., 2009). Rewards have two general categories: (1) tangible, such as financial remuneration, medals, and awards, and (2) intangible, such as job advancement, recognition, and praise by peers (Pahnila et al., 2007; Bulgurcu et al., 2010). In the IS security setting, employees are encouraged to comply with IS

security policies when they are sufficiently motivated to attain rewards and recognitions. Rewards also signal to employees that conformance with IS security policies is mandatory (Boss et al., 2009). Such IS security policies are not accorded much importance by employees in the absence of any reward for compliance (Boss et al., 2009).

Stanton et al. (2005) discovered that rewards show a positive correlation with password-related security behaviors, such as changing passwords more frequently and choosing stronger passwords. Similarly, Bulgurcu et al. (2010) postulated that, based on RCT, the perception of benefits of compliance is shaped by a reward system. They described rewards as tangible or intangible compensation which an organization provides in return for compliance with the requirements of IS security policies. Rewards included salary raises, awards, promotions, and personal appreciation in either oral or written form. Their study, based on a sample size of 474 respondents from varying organizations, showed that rewards were positively correlated with IS security policies compliance. Thus, rewards may be used as an effective means for increasing motivation for IS security policies compliance.

Social Pressures

Individuals may also be motivated to perform actions to avoid guilt and anxiety or to gain pride and ego-enhancements (Ryan and Deci, 2000). This indicates that the motivation for individuals to perform a specific action may be the desire to maintain a feeling of self-worth and self-esteem. This is associated to the pressures individuals receive from their social interaction with the organizational members to perform the behavior in question (Venkatesh and Brown, 2001). Social pressures exerted by subjective norms (perceived expectation) and descriptive norms (observation) should positively influence IS security compliance intentions (Herath and Rao, 2009a).

Normative beliefs are based on the beliefs as to whether or not significant others expect the individual to perform a specific behavior (Ajzen, 1991). This indicates that a message about expectations from one member's social network is able to influence another member's behavior. In the IS security setting, examples of normative beliefs are the expectations of superiors, IT management, and peers in IS departments on IS security policies compliance (Herath and Rao, 2009a). A study has shown that if an employee believes that others expect IS security policy compliance from him or her, then that individual will comply (Herath and Rao, 2009a). Simply put, the possibility of gaining approval from others motivates individuals to perform IS security compliant behaviors.

Descriptive norms concern observations of behaviors demonstrated by others (Leach, 2003), and they are strongly influenced by the behavior of others. New or existing employees who need to conform with their organizational norms tend to build their IS security behaviors according to the IS security practices and behaviors demonstrated by senior management and peers (Leach, 2003). Chan et al. (2005) examined how perceptions of descriptive norms derive from the observation of organizational management, direct supervisor's, and peers' IS security behaviors. Management behaviors include the routine actions of management as observed by individual employees. Such behaviors and practices include outlining written IS security policies and providing training and awareness programs. These actions demonstrate to employees that the organization stresses the importance of good IS security. Direct supervisory behaviors and practices are measured by the repeated actions of supervisors as observed by the individual employee. Since supervisors have the most contact with subordinates, they are the ideal candidates for communicating and enforcing organizational goals. Thus, employees who observe their supervisors giving greater emphasis to prescribed IS security procedures tend to be inclined

to carry out the same behaviors. Peer socialization refers to observation of peer behaviors (Chan et al., 2005). This view holds that an individual's decision to perform a certain behavior is based on the observation that others are doing it. In other words, employees' reciprocate the behavior of others because they believe they need to do what many others do. Chan et al. (2005) provided evidence that management practices, supervisory practices, and peer behaviors do influence employees' compliant behavior. Similarly, Herath and Rao (2009a) found that if employees see their coworkers routinely following IS security rules, they are motivated to perform the same behaviors and, thus, follow the IS security rules as well.

Intrinsic motivation and IS security policy compliance

In recognizing the importance of intrinsic incentives, IS security researchers have incorporated feelings of competence (Chan et al., 2005; Workman et al., 2008; Herath and Rao, 2009b; Rhee et al., 2009), feelings of contribution from one's IS security actions (Herath and Rao, 2009a), and feelings of value congruence and legitimacy (Son, 2011) in their models.

Perceived competence

Competence or self-efficacy refers to an individual's belief in his/her capability to perform a specific task (Bandura, 1977). Self-efficacy theory argues that individuals with low self-efficacy on a specific task tend to avoid that task. Self-efficacy regarding IS security tasks have been widely studied (e.g., Chan et al., 2005; Workman et al., 2008; Herath and Rao, 2009b; Rhee et al., 2009). Chan et al. (2005) examined the causal role of employee self-efficacy and IS security compliant behavior in IT intensive organizations in the logistics and petrochemical industries. This study indicated that employees' belief in their efficacy in IS security influenced their decision to perform (or not perform) IS security related tasks, particularly those prescribed

through organizational IS security policies. Chan et al.'s (2005) results indicated that self-efficacy perceptions are an important determinant of performance related to a specific task.

Self-efficacy beliefs also affect individual efforts and persistence efforts related to a specific task. Rhee et al. (2009) showed that self-efficacy in IS security influences individuals' intention to strengthen IS security efforts, both in terms of security technology use and security-conscious behavior. Furthermore, self-efficacy influenced individuals' intention to continue their IS security efforts. That is, they tend to agree to strengthen their knowledge about IS security, enforce IS security procedures, and add extra IS security measures in the future. The results suggest that if employees have high levels of IS security self-efficacy, they will increase compliance-related behaviors.

Perceived effectiveness

Herath and Rao (2009a) examined how intrinsic incentives affect employee compliance behavior. This study considered intrinsic incentive in term of feeling of contribution from one's action. Herath and Rao (2009a) postulated that if employees believe that their IS security actions or behaviors can contribute to the betterment of the organization, it is likely that they will carry out the actions. Their web-based survey was carried out in collaboration with Cyber Task Force, Buffalo Division, the Federal Bureau of Investigation (FBI), and involved 312 employees from 77 organizations across the US. Herath and Rao's (2009a) results indicated that employees adopt a favorable IS security compliance behaviors if they believe that their IS security actions are effective. Thus, intrinsic motivation, measured by perceived effectiveness of IS security actions predicted employees intention to comply with IS security policies.

Beliefs about organization

Son (2011) suggested that employees' assessment of their employer may be an important source of intrinsic motivation to follow rules. Drawing upon the work by Tyler and Blader (1995), Son (2011) specified two specific employer assessment conditions: perceived value congruence and perceived legitimacy. Perceived value congruence refers to the alignment between individuals and organizational IS security values (Son, 2011). Son (2011) posited that individuals (and organizations) tend to cooperate when their belief systems match. Thus, when employees perceive their values are in congruence with the organization's values, they tend to commit and maintain a long-lasting relation. However, if there is a lack of alignment, chances are that an individual is not loyal to the organization and, thus, poses a security risk. In the context of IS security policy compliance, if employees feel that their IS security value system is in congruence with that of the organization, there is a higher chance of IS security policy compliance. Perceived legitimacy refers to employees' assessment of the IS security policy in terms of its appropriateness and desirability (Son, 2011). Son (2011) purported that it is important for organisation to achieve legitimacy in order to influence the organisational members behaviors. The results of his study indicated that both perceived value congruence and legitimacy were positively related to IS security compliance behaviors. Thus, employees innate desires and preferences for legitimacy and value congruence of the IS security were found to influence thier IS security behaviors.

Another strand of research has focused on the assessment of an asset as a source of individual intrinsic motivation to perform a desired behavior. Specifically, this stream of research is based on individual assessment of psychological ownership of an asset. The logical argument is that rational people will not destroy or take unnecessary action against something

that belongs to them. As much as possible, such people will protect what belongs to them. In the context of IS security behavior related to home computing, Anderson and Agarwal (2010) investigated the impact of feelings of ownership of the Internet and the computer on behavioral intentions to protect the Internet and one's computer. They found that an individual's level of psychological ownership towards the Internet and computer does influence IS security behavior. Table 0.1 presents a summary of seminal work in the two paradigms, dominated by the extrinsic motivation paradigm.

Table 0.1: Extrinsic and intrinsic motivation of IS security policy compliance

Motivation	Factors	Description	Theory Used	Some Seminal Papers
EXTRINSIC	Sanctions	I comply with security policies to avoid penalties.	General Deterrence Theory (GDT); Agency Theory	Bulgurcu et al., 2010; Pahnila et al., 2007; Straub, 1990
	Monitoring	I comply with security policies because I know my activities is being monitored.	Control Theory	Boss et al., 2009; Stanton and Weiss, 2000; D'Arcy et al., 2009; Straub, 1990
	Rewards	I comply with security policies to attain rewards.	Rational Choice Theory; Theory of Planned Behavior	Boss et al., 2009; Bulgurcu et al., 2010; Stanton et al., 2005
	Normative Beliefs	I comply with security policies because I belief that significant others (superiors, IT management and peers in IS departments) expect me to comply.	Protection Motivation Theory	Bulgurcu et al., 2010; Herath and Rao, 2009; Pahnila et al., 2007
	Social Climate / Observation	I comply with security policies because I observe that my management, supervisors and colleagues give great emphasis to prescribed security procedures.	Protection Motivation Theory	(Chan et al., 2005; Herath and Rao, 2009; Leach, 2003)
INTRINSIC	Perceived Effectiveness	I comply with security policies because I perceive that my security actions will help for the betterment of my organization.		Herath and Rao, 2009
	Perceived Self-Efficacy	I comply with security policies because I perceive that I have the skills or competency to perform the security activities.	Self-efficacy theory	(Chan et al., 2005; Rhee et al., 2009; Workman et al., 2008)
	Perceived Value Congruence	I comply with security policies because I perceive that the security values/goals are congruence with my values.		Son, 2011
	Perceived Ownership	I comply with security policies because I perceive that I own the assets (computer and the Internet).		Anderson and Argawal, 2010

Extrinsic or intrinsic motivation?

Herath and Rao (2009a) examined the influence of variables under both extrinsic and intrinsic motivation models of IS security policy compliance intentions. They reported that employees' intrinsic motivation, measured by perceived effectiveness, predicted IS security compliance intentions (β = .22, p < .05). The extrinsic motivation model, measured by severity

of penalty, certainty of detection, peer behavior, and normative beliefs, was partially supported. Overall, Herath and Rao's (2009a) findings suggested that both intrinsic and extrinsic motivators may influence the IS security behaviors of employees. However, the study did not predict the magnitude of contribution for each model (i.e., the extrinsic and the intrinsic motivation model).

Recent work by Son (2011) examined the impact of perceived certainty and severity of sanctions (i.e., the extrinsic motivation model), and perceived legitimacy and perceived value congruence (i.e., the intrinsic motivation model) of IS security policy compliance among employees in the US. Both extrinsic and intrinsic models were assessed for their significance. The results of Son's (2011) study showed that factors that rooted in the intrinsic motivation model were significantly related to IS security policy compliance (β = .36 and .26, $p < .05$). However, contrary to expectations, both extrinsic factors were not significant (β = .05 and .06, $p > .1$). More interestingly, Son (2011) predicted that both the extrinsic and intrinsic motivation models will explain significantly more employees' IS security policy compliance than would variables from either the extrinsic or intrinsic motivation model. His results showe that the extrinsic model explained 16% and the intrinsic model explained 41% of variance of IS security policies compliance behaviors. By simultaneously testing the relations between the extrinsic factors, intrinsic factors, and IS security policy compliance intention, the model explained a substantial amount of variance of IS security policies compliance behavior (R^2 = .42). Son's (2011) results showed that the contribution of the intrinsic motivation model exceeded that of the extrinsic motivation. He proposed that intrinsic motivation may generate alternative explanations and solutions for compliance with organizational IS security policy. Thus, organizations should increase their emphasis on intrinsic motivation-based approaches, and rely less on extrinsic-based approaches (Son, 2011).

Summary

In sum, IS security policy compliance research has witnessed the rise of the extrinsic motivation argument. Scholars considering extrinsic factors to be important in ensuring compliance have largely examined the four dimensions of sanctions, rewards, monitoring, and social pressures. It goes without saying that individual compliance with IS security policy can be explained with respect to the extent of sanctions or rewards, how well they are being monitored, and what their social pressures might be.

Although most past and current research in IS security policy compliance has focused mainly on employees' value of extrinsic rewards (see Table 0.1) employees tend to value both intrinsic and extrinsic rewards (Herath and Rao, 2009a). Intrinsic motivational factors such as self-efficacy, psychological ownership, perceived effectiveness, and perceived value congruence influence employees' decisions to comply with IS security policy. Interestingly, a recent study provided empirical evidence that the intrinsic factors could explain more of the variance in IS security policy compliance than extrinsic factors (Son, 2011). This suggests that the factors constituting intrinsic motivation to comply with IS security policy are certainly promising. Unfortunately, relatively little research has been conducted within the intrinsic motivation paradigm. Hence, calls have be made to investigate other intrinsic factors (Herath and Rao, 2009a; Son, 2011; Padayachee, 2012).

Further, Herath and Rao (2009a) and Son (2011) have acknowleged few strategies or drivers, such as IS security training, and IS security climate, to enhance employees' intrinsic motivation. However, eventually no empirical research has investigated the drivers to enhance employees' intrinsic motivation. As a result, this study investigates the impact of psychological empowerment, a factor rooted in intrinsic motivation model, on IS security policies compliance

intentions, and explores the antecedents of psychological empowerment. The following section describes the theoretical foundation of this study.

2.3 Theoretical foundation

Based on the gap described above, this section seeks to explain individuals' intrinsic motivation to comply with IS security policy. In doing so, the present study incorporates the conceptual ideas of Thomas and Velthouse's (1990) intrinsic motivation/empowerment model, as well as Kanter's (1977) structural empowerment theory.

Thomas and Velthouse's Intrinsic Motivation/Empowerment Model

Although there are various definitions of intrinsic motivation, Thomas and Velthouse (1990) defined it as "positively valued experiences that the individual derives directly from the task" or "those generic conditions by an individual, pertaining directly to the task, that produce motivation and satisfaction" (Thomas and Velthouse, 1990, p. 668). This indicates that a motivation to act occurs within a person and refers to the task itself. Thomas and Velthouse (1990) claimed that a task refers to a set of activities directed towards a purpose. In other words, a task contains both activities and goals. Thus, the design of their model may be applied to various tasks in the work context.

Thomas and Velthouse's model conceptualizes empowerment as intrinsic task motivation. Empowerment refers to a set of cognitions reflecting one's perceptions about their task and their ability to control, shape or influence the task (Thomas and Velthouse, 1990; Spreitzer, 1995b). This contrasts with structural empowerment, which focuses on managerial practices that share power with employees (Spreitzer, 2007). Psychological empowerment is formed based on individuals' assessments or judgments of a task regarding four cognitions: competence, meaning, impact, and choice (Thomas and Velthouse, 1990). Thus, the core of their

model focuses on identifying these cognitions, known as task assessments. In other words, individuals are considered intrinsically motivated whenever they experience these four cognitions from a task, which are described next.

Perceptions of competence

Competence or self-efficacy refers to an assessment of one's own capability to perform a task activities skillfully (Thomas and Velthouse, 1990). Bandura (1995, p. 2) defined self-efficacy as "the belief in one's capabilities to organize and execute the courses of action required to manage prospective situations." Thus, competence relates to an individual's belief regarding whether he/she has the ability to perform a specific task. Self-efficacy theory states that when a person has low self-efficacy regardind a particular skill to execute a specific task, he or she will avoid such a tasks where this skill is required (Bandura, 1977).

Perceptions of meaning

Meaning refers to judgments of the value of a task goals with individual's own goals and standards (Thomas and Velthouse, 1990). A feeling of meaningfulness materializes if there is a fit between the task objectives and employees own beliefs, values, and behaviors (Spreitzer, 1995a). This is analogous to Hackman and Oldham's (1980) concept of *experience meaningfulness of the work.* Experiencing work as meaningful indicates the degree to which a person believes that the work objective or purpose is significant in one's own value system (Hackman and Oldham, 1980). Thus, the cognitive assessment of task meaningfulness relates to an individuals' belief concerning whether a given task is trivial or not. If a task is important or meaningful to individuals, they will invest their energy to accomplish the goal of the task (Thomas and Velthouse, 1990). In contrast, individuals who perceive that a task is meaningless tend to be apathetic and detached from said task (Thomas and Velthouse, 1990).

Perceptions of impact

Impact refers to judgments concerning how a behavior or an action regarding a task may make a significant difference to the organization in terms of accomplishing the goal of the task (Thomas and Velthouse, 1990). Thus, the cognitive assessment of impact relates to an individual's belief regarding whether he/she can contribute to the organization by performing or executing a specific task. If individuals are aware that the results of their action will benefit others, it encourages them to invest their time and energy to perform the task (Thomas and Velthouse, 1990). This is analogous to the *knowledge of results* in Hackman and Oldham's (1980) model. According to Hackman and Oldham (1980), knowledge of the results indicates that individuals know about the outcomes of their work activities. If they know that the impact of their work will be beneficial and significant, they become intrinsically motivated to perform said activity well (Hackman and Oldham, 1980).

Perceptions of choice/self-determination

Choice involves a causal responsibility for a person's actions (Thomas and Velthouse, 1990). Thomas (2009) asserted that a "sense of choice also gives you a feeling of ownership" (p. 54). A cognitive assessment of choice is based on whether people believe that they have autonomy or experience self-determination in how they perform a given task (Ryan and Deci, 2000; Deci and Ryan, 2009). In other words, cognitions of choice means believing that one has control or discretion in initiating and regulating a specific task, and has the authority to make decisions related to the task. When individuals experience a sense of choice over their task, they feel personal responsibility concerning the outcomes of their task (Oldham and Hackman, 1980), hence they will put more effort in the task (Thomas and Velthouse, 1990). Together, Thomas and Velthouse (1990) stated that experiencing empowerment is derived directly from a task manifest

in cognitions of competence, meaning, impact, and choice. In other words, individuals feel empowered if they are confident they have the skills and ability to do their task well, the task is important to them, they have freedom to make decisions regarding the task, and believe that they can have an impact on task outcomes.

Measuring psychological empowerment

Psychological empowerment is an overall construct or "gestalt" of four dimensions, viz. perceptions of competence, meaning, impact, and choice (Spreitzer 1995a). This indicates that psychological empowerment is a four-dimensional construct. This further suggests that the overall degree of psychological empowerment is limited if one of the dimensions is low or absent (Thomas and Velthouse, 1990; Spreitzer, 1995a). For instance, although people may believe they can have an impact and that they have discretion to make decisions, if they do not feel they have skill to perform the task competently or lack of sense of meaning concerning the task, they will not feel empowered (Spreitzer, 1995a). Spreitzer (1995a) developed a single 12-item (3 items per dimension) to measure psychological empowerment. Her measure has been used predominantly in empirical research in various settings (Spreitzer, 2007). The measurement of psychological empowerment assumes that empowerment is continuous, using a 7-point Likert scale.

Spreitzer (1995a) found support for the idea that all four dimensions may be loaded onto a single second-order psychological empowerment construct. Further, Kraimer et al. (1999) performed a second-order confirmatory factor analysis (CFA) and found support for the notion that psychological empowerment is made up of the four cognitions. The fit statistics indicated that the one-factor model (all 12 empowerment items were hypothesized to represent a single construct) provided a much worse fit than the four-factor model. Thus, the results provided

support for the convergent and discriminant validity for Spreitzer's (1995a) multidimensional construct of psychological empowerment. Empirical evidence across various fields, and across both cultures and work contexts has supported Spreitzer's (1995a) findings (e.g., Spreitzer, 1995b, Spreitzer, 1996, Chen and Klimoski, 2003; Carless, 2004; Alge et al., 2006; Zhang and Bartol, 2010; Ford and Tetrick, 2011).

Although the four-dimensional measure of psychological empowerment was supported in the literature, a meta-analysis concluded that the factor loadings were not consistent either across dimensions or samples (Maynard et al., 2012). This suggests that there is scientific merit to assess the dimensions separately (Maynard et al., 2012). Spreitzer et al. (2007) posited that these different dimensions may predict different outcomes, and are influenced by different antecedents. Some researchers have investigated how each of the four dimensions of psychological empowerment predicted different outcomes and is influenced by different factors (Spreitzer et al., 1997; Kraimer et al., 1999, Liden et al., 2000; Wat and Shaffer, 2005; Logan and Ganster, 2007). For instance, several studies have investigated the influence of perceived meaningfulness of a job on positive work outcomes (Spreitzer et al., 1997; Kraimer et al., 1999; Liden et al., 2000; Wat and Shaffer, 2005). Wat and Shaffer (2005) conducted a survey to assess how supervisors and subordinates perceptions of meaning of their work affects their organizational citizenship behavior (OCB). Using a sample from investment banks in Hong Kong, they found that perceived meaning was related to courtesy behavior, a dimension of OCB. Wat and Shaffer (2005) explained that when task values are consistent with individuals' values, they feel a commitment to and involvement with the goals. In addition, Wat and Shaffer (2005) found that the self-determination dimension relates to altruism or helping behavaior. In a cross-sectional study among mid-level employees in manufacturing industry, Spreitzer et al. (1997)

assessed how job satisfaction, job strain, and task performance are affected by perceptions of impact of one's job. This results indicated that perceptions of impact best predict task performance, and not significantly related to job satisfaction and job strain. However, they found that perceptions of competence were related to satisfaction and negative to job strain (Spreitzer et al., 1997).

While this perspective has not received due attention in the literature, Maynard et al. (2012) has called for research to determine the influence that the four dimensions have on various outcomes. This study seeks to answer the call by investigating the association between dimensions of psychological empowerment and individuals performance, in a context of IS security.

Individual performance-related outcomes of psychological empowerment

Findings across a wide range of studies showed that psychological empowerment influences various outcomes, including organizational level performance, team level performance, individual attitudes, individual behaviors, individual performance, and many others (Spreitzer et al., 2007; Chen and Klimoski, 2003; Zhang and Bartol, 2010; Ford and Tetrick, 2011). Meta-analytic evidence has supported this (Seibert et al., 2011; Maynard et al., 2012). The scope of the literature review is limited to individual level performance-related outcomes as this study focuses on individuals' IS security policy compliance behaviors. To comply means to exert energy to perform the IS security tasks in order to achieve the organizational IS security objectives. Thomas and Velthouse's (1990) intrinsic motivation theory postulates that the level of psychological empowerment is likely to affect outcomes, such as *active and concentration of energy upon task.* Active and concentration of energy upon task can be described as putting more "effort" or "working hard" towards accomplishing the goals of the task (Thomas and Velthouse,

1990). This indicates that the stronger the cognitions of competence, meaning, impact, and choice deriving from a task, the greater the individuals' motivation to invest more energy in behaviors towards achieving that task. Related outcomes include individual task performance, work effort, task or work effectiveness, and organizational citizenship behavior (OCB) (Spreitzer et al., 1997; Wat and Shaffer, 2005; Ke and Zhang, 2011; Campbell et al., 2003; Chen and Klimoski, 2003). The following section reviews the influence of different dimensions of psychological empowerment on individual performance-related outcomes.

Spreitzer et al. (1997) investigated the impact of each of the dimensions of psychological empowerment on employee work effectiveness. Effectiveness may be described as the degree to which individuals fulfill or exceed work role expectations. Their results showed that individuals who experience a stronger sense of competence and impact in the workplace tend to be more effective on the job (Spreitzer et al., 1997). Spreitzer et al.'s (1997) findings suggest that employees may see that their effort has made a difference (based on their prior performance) and feel that they can have an impact. In addition, the findings indicate that competence is necessary for employee effectiveness. Thus, employees who feel empowered in terms of impact and competence on the job are more motivated to invest their energy in the job and perform effectively.

Perceived competence increases task performance and goals accomplishment by increasing task effort and persistence (Bandura, 1977). That is, the stronger the perceived competence, the more persistence and active employees efforts. Task effort may be described as the amount of energy employees expend when carrying out their job. Rhee et al. (2009) showed that self-efficacy in IS security influences individual intention to strengthen their IS security efforts, both in terms of security technology use and IS security-conscious behaviors.

Furthermore, their results showed that perceived self-efficacy influenced individuals' intention to continue their IS security efforts. That is, higher efficacious employees tend to strengthen their IS security behaviors, enforce IS security procedures, and add additional security measures in the future. In another research, Kraimer et al. (1999) found that perceived meaningful of a job was related to employees' intention to stay longer in the job. Individuals who found their job meaningful are likely to be motivated to continue putting more effort into their current job. Thus, employees who find meaning in their work tend to engage in a high level of sustained work effort.

In addition, the meaning dimension of empowerment has been found to result in task performance (Ke and Zhang, 2011), as individuals reported more value and worth in the task they were required to complete. Employee task performance describes individual behaviors that are aimed at achieving firm goals (Campbell et al., 1993). In other words, task performance reflects behaviors that employees engage in to accomplish desired organizational objectives. Wat and Shaffer (2005) conducted a study to assess how supervisors and subordinates perceptions of meaning of their work affects their organizational citizenship behaviors (OCB). They found that perceived meaning was related to courtesy behavior, a dimension of OCB. Wat and Shaffer (2005) explained that because the work values are consistent with individuals' values, they feel a commitment to and involvement with the work goals. Therefore, individuals with higher levels of meaningfulness related to the work may engage in behaviors that helps their organization to achieve specified goals.

In sum, the reviewed studies provide support for the notion that the perceptions of competence, meaning, impact, and choice drive individuals to expend effort to perform a related task, as well as to achieve goal of the task.

Antecedences of psychological empowerment

Theories have documented the need of drivers to enhance one's intrinsic motivation related to his/her task or job (Hackman and Oldham, 1980; Deci and Ryan, 1985; Thomas and Velthouse, 1990). For example, Hackman and Oldham (1980) posited that enhancing intrinsic motivation concerns the properties of the job itself. Hackman and Oldham's job characteristics model suggests five job characteristics, namely skill variety, task identity, task significance, autonomy, and feedback from a job, as antecedents to influence one's intrinsic motivation. Similarly, Thomas and Velthouse (1990) contended that an individual's work environment is an important factor that can influence the level of intrinsic motivation.

In a study of the intrinsic motivation behind IS security policy compliance, Bulgurcu et al. (2010) suggested that an organization may use external instrumentals, such as training, to influence employees' perceptions of intrinsic benefits. Similarly, Son (2011) stated that an organization can implement training and education programs, and tighten the connection between the objective of the IS security policy and employees internal value to drive employees' intrinsic motivation. Furthermore, Herath and Rao (2009a) have suggested to enhance appropriate IS security climate in order to improve employees perceived effectiveness of their IS security tasks. Rather than exploring the range of external factors, these studies simply acknowledged their importance. Hence, it is imperative to explore the antecedents to influence employees' intrinsic motivation, specifically their psychological empowerment.

Thus far, a broad range of antecedents of psychological empowerment has been reported in the organizational literature. These include job characteristics, structural empowerment, and leadership style (Spreitzer, 1995b; 1996; Kraimer et al., 1999; Liden et al., 2000; Hon and Rensvold, 2006; Logan and Ganster, 2007). For instance, Kraimer et al. (1999) linked Hackman

and Oldham's (1980) five job characteristics to the four dimensions of empowerment. Kraimer et al. (1999) found that job meaningfulness was related to perceptions of meaning, task feedback was related to perceptions of impact and competence, and job autonomy was related to the experience of self-determination. The role of leadership may also influence one's feelings of empowerment. For instance, transformational leadership, leader-member exchange (LMX), and trust in one's leader were associated with feelings of empowerment among subordinates (Kark et al., 2003; Avolio et al., 2004; Ergeneli et al., 2007). Specifically, this current study focuses on structural empowerment, based on Kanter's (1977) structural empowerment theory. The argument is that, when management transfers power to subordinates, feeling of empowerment should follow.

Kanter's Structural Empowerment Theory

Although several researchers have explored the conception of structural empowerment, Kanter (1977) identified it first. Structural empowerment refers to conditions or practices where an organization provides subordinates with an amount of power. According to Kanter, power is derived from the structural conditions in an organization, not inherent from personality traits or effects of socialization. Thus, the focus of Kanter's theory is on the employees' perception of the work conditions, rather than the individuals, which determine what happened.

Kanter (1977) discussed several practices that indicate structural empowerment: (1) access to opportunity, (2) access to information, and (3) participation in decision-making. First, *access to opportunity* relates to job or task conditions that provide individuals with chances for growth and development within the organization, as well as chances to develop their skills, abilities, and knowledge. Access to opportunity allows an individual to learn about skills and the economies of the larger organization (Lawler, 1986). Lancshinger (1996) defined *access to*

opportunity as opportunities for growth and movement within an organization as well as opportunities to enhance and develop one's knowledge and skills. This could be achieved through training and education programs. Educational efforts contribute to individuals' intrinsic motivation by increasing the belief in their capability to perform task activities skillfully (Thomas and Velthouse, 1990; Spreitzer et al., 2007). According to Gist and Mitchell (1992), attempts to improve sense of competence or self-efficacy should involve some formal training. In addition, a training program that provides information on the effectiveness of performance (task feedback) should enhance individuals' belief about the impact of their work activities (Hackman and Oldham, 1980).

Liao et al. (2009) argued that if management invests in training programs, it may enhance employees' human capital, employees' knowledge, skills and abilities (KSAs) to provide quality service to customers. In return, the KSAs acquired through the training may positively influence employees' confidence in their competence in service delivery. The study showed that high performance work systems (HPWS), which include training programs was positively related to cognitions of empowerment. Bonias et al. (2010) found support for Liao et al's (2009) results in the context of quality care to patients in hospitals. Bonias et al.'s (2010) study showed that training, part of a HPWS, was positively associated to the dimensions of psychological empowerment – perceptions of competence, meaning, impact, and choice. Logan and Ganster (2007) conducted a field experiment that tested the effects of an empowerment intervention (i.e. training) among unit managers of a large trucking company in the USA. However, their results were contrary to the hypothesis, as training had a negative significant effect on the participants' sense of competence. This indicates that although training leads to increases in KSAs, it can also reduce the participants' perceived level of competence.

Second, Kanter (1977) posited that *access to information* refers to ability to obtain knowledge and information necessary to carry out an individual's task as well as information concerning what is going on in the larger organization. In her second edition of the book, she posited that "to be empowering, top management must make more information available to more people at more levels through more devices" (Kanter, 1986 p.5). Lancshinger (1996) referred to access to information as having information regarding organizational goals and policy changes. More specifically, previous researchers have focused on information regarding the mission and future direction of the organization (Lawler, 1992; Spreitzer, 1995b, 1996; Bordin et al., 2006). Access to information related to goals and strategic directions allows an individual to see the "big picture", which creates an understanding on how his or her work contributes to the firm's goals (Bowen and Lawler, 1992). Thus, such an individual will be able to make better decisions related to his/ her task.

Quinn and Spreitzer (1997) conducted interviews with 12 senior executives in a manufacturing company. The results of the interviews showed that empowerment is about delegation and accountability. It is a process in which top management develops a clear organizational mission, along with a vision and values, and communicates said vision to the members of the organization (Quinn and Spreitzer, 1997). They found that providing a clear vision allows people in the organization to feel highly empowered, as they understand top management's vision and strategic direction of the organization. With an understanding of the vision and the direction of the organization, they experience enhanced levels of confidence and the ability to act without waiting for approval from a supervisor. Earlier, Lawler (1992) posited that accessing organization's mission contributes to individuals' intrinsic motivation by increasing the belief in their ability to make and influence decisions that are congruent with the

organizational goals and mission. In addition, studies found that access to information may help employees to perceive a given job or task as meaningful and important, because they see and understand how their task can contribute to the goals (Spreitzer, 1995a; Liao et al., 2009).

Third, Kanter's (1977) theory also suggests an empowerment through participation. This indicates that employees are able to provide inputs and influence over decisions. Inputs in this context consist of strategic and day-to-day operational decisions related to their job or task. Knoop (1995) stated that participation is the act of sharing decision-making with others to achieve organizational goals. As employees are at the operational level, they know better how specific actions related to their job or task affect the organization. Employees are also more likely to offer valuable ideas on how operations may be improved. Subsequently, their meaningful suggestions are more likely to be accepted and adopted. Participative climate helps employees to belief that they are an important asset of the organization and that they can make significant impact to the organization (Spreitzer, 1996). Lawler (1992) reasoned that when employees are more involved in the decision-making process concerning organizational tasks, they are more aware of the tasks requirements (i.e. sense of meaningful), and, hence are more likely to take effective actions.

Spreitzer's (1996) study reported that participative organizational climate significantly correlated to individuals' feelings of empowerment. In the context of service industry, Liao et al. (2009) argued that increased decision-making power may enhance employees' confidence in their competence to handle customers. Their findings showed that employee experience with the high performance work system (HPWS), including participation in decision-making, influences one's feelings of empowerment. Bordin et al. (2006) also found support for this argument in the context of white collar IT employees.

In addition, Wallach and Mueller (2006) examined opportunities for employees to participate in decision-making within human service organizations. Their study confirmed earlier findings (e.g., Bordin et al., 2006; Liao et al., 2009) that structures in organization that allow employees to participate in decision-making enhances their psychological empowerment, manifested by four cognitions, competence, meaning, impact and autonomy. However, the study also reported that when controlling for variables such as role ambiguity, peer support, and supervisory working alliances, the relations between participation in decision-making and perceived empowerment did not remain statistically significant.

As shown, many studies have examined the relations between structural empowerment and the psychological empowerment (Spreitzer, 1996; Laschinger et al., 2004; Siu et al., 2005; Wallach and Mueller, 2006). However, most of the studies have conceptualized structural empowerment as a 'bundle' of practices (e.g., Laschinger et al., 2004; Siu et al., 2005) that make it difficult to identify which structural empowerment elements are actually associated with psychological empowerment. Additionally, as Spreitzer's (1996) and Wallach and Mueller's (2006) work has exemplified, psychological empowerment has been conceptualized as a composite of perceptions of competence, meaning, impact, and choice. Again, this makes it difficult to tease apart which dimensions were actually driven by the elements of structural empowerment. Spreitzer (2007) noted that the different dimensions of psychological empowerment may be influenced by different antecedents. Similarly, Maynard et al. (2012) called for future research to take in-depth considerations of the various elements of structural empowerment and their association with the dimensions of psychological empowerment. In response to these notions and calls, this study attempts to investigate the relations among the elements of structural empowerment (i.e., training, access to information regarding strategy and

goals, and participation in decision-making) and the dimensions of psychological empowerment (i.e., perceptions of competence, meaning, impact and choice) in the context of IS security.

The mediating role of psychological empowerment

The concept of psychological empowerment serving as mediator between structural empowerment and individual performance-related outcomes has been repeatedly supported in numerous studies (e.g., Spreitzer, 2007; Maynard et al., 2012). Changing an organizational structural context is not enough to change individual behaviors; ultimately, an individual's sense of empowerment is necessary to influence such behaviors (Nielsen, 1986 cf. Spreitzer, 1995a). For example, Spreitzer (1995b) found that psychological empowerment partially mediated the relation between social structural and innovative behavior. In addition, Liao et al. (2009) found that cognitions of empowerment fully mediate the relations between a HPWS and service performance. Further, Laschinger et al. (2001) found that psychological empowerment mediates the relations between structural empowerment and individual satisfaction. In these studies, both the structural and psychological empowerments were measured as composite constructs.

When considering the dimensions of psychological empowerment independently, Gist and Mitchell (1992) reported that self-efficacy did mediate the effects of training on individual performance. Further, Liden et al. (2000) found that perceived meaning partially mediated the relations between job characteristics and job satisfaction. In a different context, Bonias et al. (2010) tested for a mediating effect of all dimensions of psychological empowerment and found that senses of competence, meaning, and autonomy fully mediated the relations between a HPWS and quality care to patients. This dissertation partly replicates these previous studies, by investigating the mediating role of each individual dimension of psychological empowerment in

the relations between elements of structural empowerment and IS security policy compliance behavior (i.e., individual performance-related outcomes).

2.4 Conclusion

Reviewing what has been discussed thus far in the literature review section, a number of conclusions may be drawn. First, this study classified and identified current research direction in IS security policy compliance research. The views were systematically classified according to Ryan and Deci's (2000) extrinsic-intrinsic motivation framework. The literature review established the dominance of the extrinsic motivation paradigm. There have only been a few attempts diverting from this mainstream view. The limitations of these approaches have led to the emergence of the intrinsic motivation perspective. Drawing upon Thomas and Velthouse's (1990) intrinsic motivation/empowerment model, psychological empowerment is conceptualized as intrinsic motivation, which is formed based on individuals' assessments or judgments of a task regarding four cognitions: competence, meaning, impact, and choice. Empirical studies concluded that the dimensions of psychological empowerment lead to various individual performance-related outcomes, specifically task effort, task performance, and work effectiveness. However, prior studies in the context of IS security have given little focus to the four dimensions of psychological empowerment, except for perceptions of competence. Thus, the current study includes all four dimensions as predictors of IS security compliance intentions.

Second, Thomas and Velthouse's (1990) theory posits that intrinsic motivation should be enhanced or driven by environmental factors. While the IS security compliance literature acknowledged the importance of external factors to influence intrinsic motivation, no study has empirically explore the associations (see Herath and Rao, 2009a; Bulgurcu et al., 2010; Son, 2011). Based on Kanter's structural empowerment theory, studies have found that individuals in

positions with access to power, as measured by opportunities to obtain training, access to information, and participation in decision-making, experience an increase in their psychological empowerment. Although theory and empirical studies have provided support for the assertion that these structural empowerment facets are antecedents of one's psychological empowerment, few studies have investigated the impact of each structural empowerment facet on the dimensions of psychological empowerment. This study seeks to fill that gap in the context of IS security.

Finally, the vast majority of research has considered psychological empowerment as a mediator. This study follows that notion, investigates the mediating role of the dimensions of psychological empowerment on the relations between structural empowerment facets and IS security policy compliance intentions. Accordingly, the next chapter of this study proposes a research framework that incorporates the constructs derived from the two theories, Thomas and Velthouse's (1990) intrinsic motivation model and Kanter's (1977) structural empowerment theory, along with the hypothesized relations.

Chapter 3. Theoretical Model and Hypotheses Development

3.1 Introduction

The previous chapter has reviewed the effects of extrinsic and intrinsic motivation on IS security policy compliance. Although extrinsic motivation dominates the literature, IS security scholars have begun to consider intrinsic motivation as another predictor of IS security policy compliance. Despite the contribution of intrinsic motivation to IS security compliance behaviors, relatively little research has been conducted within this paradigm (Herath and Rao, 2009a; Padayachee, 2012), and there is a lack of theoretically driven approaches. Preston (1991) specifically called upon information systems researchers to investigate the underlying assumptions and theoretical constructs that shape their understanding. Thus, the objective of this study is to develop a comprehensive model of intrinsic motivation and empirically test the role of psychological empowerment (i.e., intrinsic motivation model) in mediating the relations between structural empowerment facets and IS security policy compliance intentions. This study adopts Thomas and Velthouse's (1990) intrinsic motivation model.

This chapter is organized into four sections. Section 3.2 describes how intrinsic motivation theory can be applied in the context of IS security. Section 3.3 presents the development of hypotheses. It is divided into three subsections: influences of psychological empowerment on IS security policy compliance, drivers for psychological empowerment, and psychological empowerment as mediator. Section 3.4 provides the conclusions of this chapter.

3.2 Linking intrinsic motivation theory and IS security policy compliance

Thomas and Velthouse (1990) posited that "intrinsic motivation involves positively valued experiences that the individual derives directly from the task" (p. 688). From the previous chapter, Thomas and Velthouse's (1990) theory proposes that intrinsic motivation is a cognitive assessment of four components of empowerment derived from a specific task: feelings of competence, meaningfulness, impact, and choice of the task. Competence has been defined as the belief in one's capability to perform the task activities skillfully and successfully. For example, individuals with the proper skills in an organization may feel confident about some portion of the IS security task they choose to work on. Cognitive assessment of meaning relates to an individual's belief regarding the value of the task in relation to one's personal beliefs, specifically attitudes and values. In the context of this study, individuals in an organization may identify with protective values and regard their performing IS security-related tasks as meaningful. Impact refers to the belief that one can make a significant difference or contribute to the organization in accomplishing the goal of the task. For instance, individuals in an organization should consider if their IS security actions produce intended effects, such as a reduction in the IS security breaches. Choice refers to a sense of freedom or autonomy to select tasks that makes sense and perform in ways that seem appropriate, and being personally responsible for the results. In the context of IS security, individuals may decide how they want to carry out a given IS security task.

Thomas and Velthouse's (1990) model of intrinsic motivation is grounded on the thesis that individuals' assessment of four dimensions of empowerment exerts influence on that individuals' feeling towards performing the task well (see also Oldham and Hackman, 1980; Deci and Ryan, 1985). Prior studies have examined the direct effects of competence, meaning,

impact, and choice of a task on individuals' performance-related outcomes in organizational contexts (e.g., Spreitzer et al., 1997; Kraimer et al., 1999; Liden et al., 2000), as discussed in previous chapter.

An assessment of positive feelings of competence, meaning, impact and choice of a task, should motivate individuals to initiate actions. Although these feelings are innate to individuals and derived from a specific task, these feelings must be enhanced by external factors (Thomas and Velthouse, 1990; Ryan and Deci, 2000). One way an organization can stimulate these feelings is the provision of structural empowerment. Structural empowerment refers to practices that allow individuals to enhance their knowledge and skills through training and education related to the task, access to information about strategy and goal, and participate in decision-making related to the task (Seibert et al., 2011; Liao et al., 2009; Logan and Ganster, 2007). Educational efforts influence psychological empowerment in terms of increasing individual's belief in his/her capability to perform a specific task skillfully (Thomas and Velthouse, 1990; Spreitzer, 2007). Decision making responsibility related to a task can enhance one's perception of meaningful, autonomy, and impact of the task (Spreitzer, 1996; Hon and Rensvold, 2006; Logan and Ganster, 2007; Seibert et al., 2011). Furthermore, access to information about the strategy and goals has been found to be associated with feelings of competence and meaningfulness of the job (Spreitzer, 1996; Liao et al., 2009).

The notion of individuals' feelings of competence, meaning, impact, and choice of a task can be extended to IS security context for two reasons. First, tasks in IS security are similar to job tasks in organizations, with activities and goals (Thomas and Velthouse, 1990). IS security tasks are defined as activities that protect the organisation's information with the goals of ensuring the confidentiality, integrity, and availability of the information (Loch et al., 1992).

These activities include the appropriate use of computer hardware and software, the appropriate selection of a password, the using and updating of anti-virus software, backing up of data, appropriate use of e-mail and the internet, checking for encryptions, not sharing the computer with others, etc. (Stanton et al., 2005; Albrechtsen, 2007; Dhillon, 2007; Herath and Rao, 2009a). These IS security tasks to protect the information resources of a firm and are typically described in IS security policies, which is part of the formal control structure in an organization (Dhillon, 1997; Bulgurcu et al., 2010). Second, similar to other job tasks (e.g., payroll, teaching students, serving customers, and so on) IS security tasks are important to organizations. In order for employees to create value for their organization, they must complete these IS security tasks. For instance, employees that create a strong password help to protect their organization from security threats and vulnerabilities. It is through exerting effort and performing IS security tasks (e.g., complying with the IS security policy) that employees contribute to the organization and other stakeholders.

3.3 The Research Model and Hypotheses

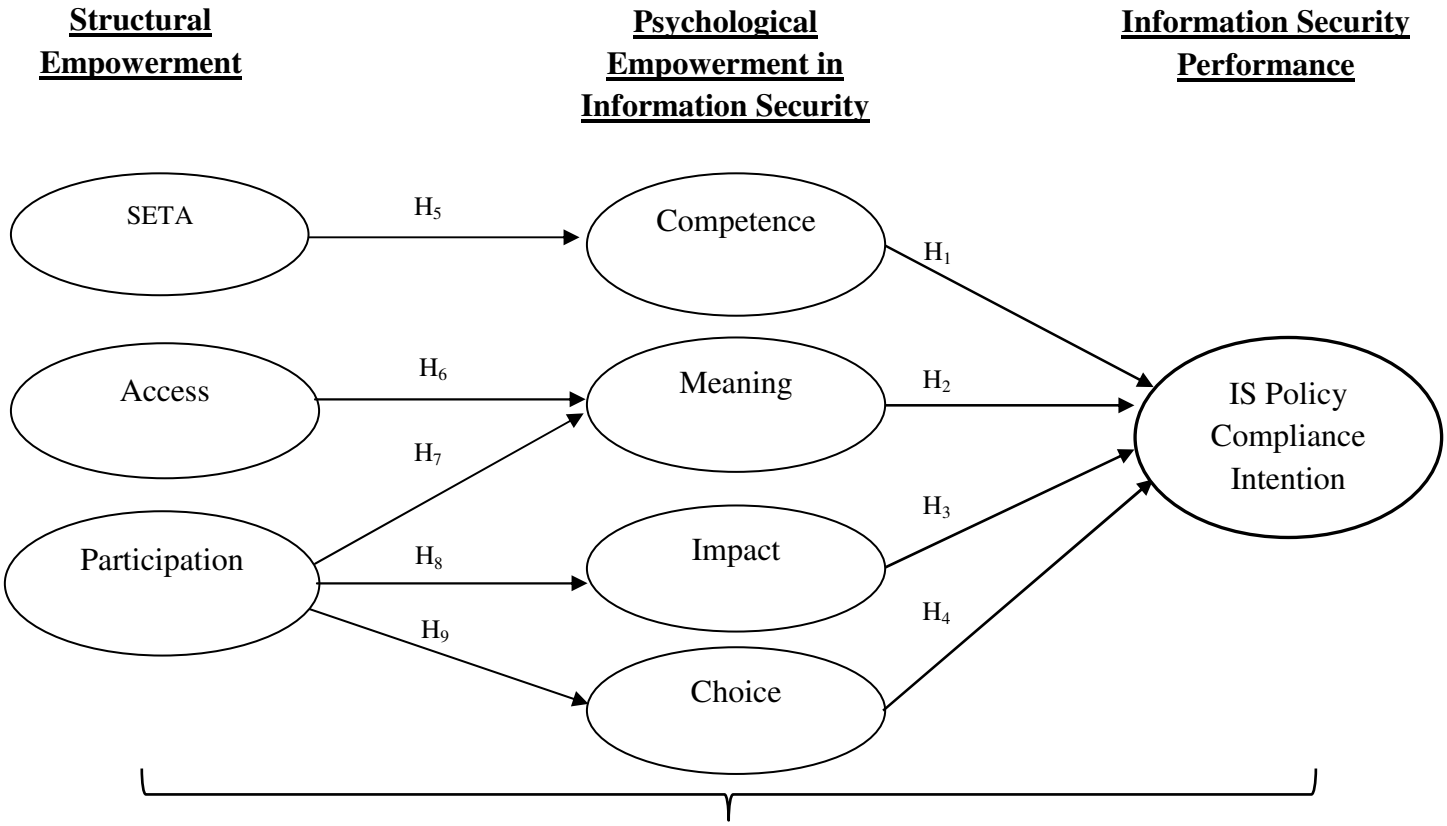
This section is divided into 3 subsections. The first subsection describes psychological empowerment in the context of IS security and how it influences the intention to comply with an IS security policy. The second subsection identifies the drivers that enhance the psychological empowerment of employees. The third section explains the mediating role of psychological empowerment between structural empowerment facets and IS security policy compliance.

Influences of psychological empowerment on IS security policy compliance intentions

Extending Thomas and Velthouse's (1990) intrinsic motivation model to the IS security context, this study contends that psychological empowerment, which is conceptualized as individuals' belief regarding their ability to carry out the IS security tasks, individuals' feelings

of meaningfulness of the IS security tasks, individuals' feelings of impact of their IS security actions, and the freedom individuals' feel in executing the IS security tasks, may help explain individuals' intention to execute and perform IS security efforts (i.e., compliance with IS security policy).

Figure 0.1: Proposed Research Framework



In addition, this study seeks to investigate how individuals' psychological empowerment can be enhanced through structural empowerment. Figure 3.1 illustrates the research framework. It is proposed that employees' innate feelings of competence, meaning, impact, and choice

derived from the IS security tasks influence their intention to comply with the IS security policy. Although these feelings are innate to individuals, they might be enhanced by structural empowerment, through the three following mechanisms: (a) IS security education, training and awareness (SETA), (b) access to IS security strategy and goals, and (c) participation in IS security decision-making. Each of the constructs and its relations are discussed in the following sections.

IS security policy compliance intention can be defined as individuals' intention to perform or execute the IS security tasks in order to protect information and technology resources from potential security breaches (Bulgurcu et al., 2010). That is, individuals intent on strengthening their IS security efforts by investing their time and energy to execute the IS security tasks. Based on the theory of planned behavior (TBP), behavioral intention is a strong indicator of an individual's readiness to perform the actual behavior (Ajzen, 1991). Thus, in this research individuals' intentions to comply with the IS security policy is the dependent variable.

Competence and IS security policy compliance intention

Perceived competence refers to one's ability to perform a task (Bandura, 1977). When individuals perceive that there have the competence and skills regarding a specific task, they will engage and regulate their efforts in the task activities (Bandura, 1977). Further, the intrinsic motivation theory purports that individuals are likely to put more effort and energy towards completion of a task when they feel they are performing the task well (Thomas and Velthouse, 1990).

There is extensive research linking competence or self-efficacy on task-related behaviors and actual performance (e.g., Stajkovic and Luthans, 1996; Hsu and Chiu, 2004; Ke and Zhang, 2011). In a meta-analysis, Stajkovic and Luthans (1996) assessed the impact of competence on

task performance. Task performance was measured by the required acts necessary to perform the task and the product of the task. The meta-analysis of 114 studies concluded that the relations between competence and task performance was significant (Stajkovic and Luthans, 1996). Perceived competence may also provide motivation for employees to engage in IT usage (Hsu and Chiu, 2004; Ke and Zhang, 2011). A study conducted by Hsu and Chiu (2004) showed a significant positive relations between users' confidence in their skills of service on service usage. Further, Ke and Zhang (2011), reported that perceived competence in an open source software (OSS) task was found to be a significant predictor of OSS project participation. These findings suggest that an individual who has confidence in the capability to undertake a task is more likely to take the required associated actions.

With regards to IS security policy compliance, employees who have confidence in their ability to carry out IS security tasks as prescribed in the IS security policy are more likely to have positive feeling towards the IS security tasks. In return, the positive feeling increases their motivation to take acts necessary to perform the IS security tasks. Some empirical studies have examined the influences of perceived competence on IS security behaviors (e.g., Chan et al., 2005; Workman et al., 2008; Herath and Rao, 2009b; Rhee et al., 2009). For instance, Chan et al. (2005) found that employees' belief in their efficacy in IS security influences their decision to perform IS security related activities, particularly those prescribed under an organizational IS policy. More recently, Rhee et al. (2009) demonstrated that self-efficacy in IS security influences individuals' intention to strengthen their security efforts, use security protection software, and other security compliance behaviors.

Consistent with self-efficacy theory, intrinsic motivation theory, and the findings of Chan et al. (2005), Workman et al. (2008), Herath and Rao (2009b), and Rhee et al. (2009), it is

expected that perceived competence of IS security tasks will encourage IS security task performance in the form of IS security policy compliance. That is, employees do not approach IS security tasks devoid of any presumptions about thier ability to successfully perform the tasks. This prediction is formally recognized in the following hypothesis:

> *H_1: Perceived competence in IS security tasks positively affects one's intention to comply with the requirements of the IS security policy*

Meaning and IS security policy compliance intention

Meaning refers to judgments of the value of a task goal or purpose in relation to an individual's own ideals and standards (Thomas and Velthouse, 1990). Theory suggests that individuals are more likely to engage, do well and exert energy into a task if the task activities are meaningful, serve an important purpose, and are in accordance with their own values and goals (Thomas and Velthouse, 1990). Individuals who believe that an assigned task is meaningful are more likely to be motivated to invest their resources to accomplish the goal of the task because by doing so, their goals are met.

Research has provided evidence that meaning is associated with numerous work-related benefits, such as courtesy behavior, higher commitment to work, engagement at work, and work performance (e.g., Liden et al., 2000; Wat and Shaffer, 2005; Wang and Lee, 2009; May et al., 2004). For example, Wat and Shaffer (2005) found that the perceived meaningfulness of a job was a significant predictor of courtesy behaviors, which refer to actions taken to prevent problem with other employees. This suggests that individuals who perceive that their job is meaningful are motivated to engage in behavior that helps organization from work-related problems from occurring, due to their commitment to the goals (Wat and Shaffer, 2005). Further feelings of meaningfulness of a given work activity have been positively linked to employee engagement in the associated work activities (May et al., 2004). A study by Wang and Lee (2009) found an

increased propensity to commit to work when said work was perceived as personally meaningful. Employees who believe that the work activities are personally meaningful were willing to invest themselves more fully in the associated activities.

Regarding IS security policy compliance, employees who perceive that IS security tasks as prescribed in the IS security policy are meaningful, are more likely to engage and perform the tasks. For example, good or poor performance of IS security literally mean the difference between survival and death for the organization (i.e., IS security breach may result in significant loss, both monetary and nonmonetary, to the organization). If employees care about the survival of their organization, they are likely to rate IS security tasks as highly meaningful to them, which should increase intrinsic motivation to act in accordance with IS security policy. This indicates that individuals who believe that IS security tasks serve a purpose, typically to help the organization from IS security-related problems, which is incongruous with their value, are more willing to exert effort into the task. This leads to the following hypothesis:

> *H_2: Perceived meaningfulness of IS tasks positively affects one's intention to comply with the requirements of the IS security policy.*

Impact and IS security policy compliance intention

Impact refers to the belief that one's behavior or act to perform a task can make a significant difference or contribute to an organization, especially in terms of accomplishing the purpose of the task (Thomas and Velthouse, 1990). Per stewardship theory, it is expected that individuals may be motivated to take action for collective benefits, such as for the well-being of the organization, co-workers, and the communities in which they operate (Davis et al., 1997; Donaldson and Davis, 1991). Such individuals engage in activities that are beneficial to others because they believe that their actions will be able to influence and improve the organizational

outcomes (Spreitzer et al., 1997; Herath and Rao, 2009a). Thus, there may also be intrinsic motivation factors (i.e., perceived impact) to arrive at an outcome that benefits others.

Prior data provide evidence of the relations between perceived impact of acts to perform a task and engagement as well as performing well with the task (e.g., Spreitzer et al., 1997; Kraimer et al., 1999; Wang and Lee, 2009; Liao et al., 2009; Herath and Rao, 2009; Agarwal and Anderson, 2010). For example, Spreitzer et al. (1997) found that perceived impact significantly related to work effectiveness, which is the degree to which individuals fulfill or exceed work expectation. Furthermore, an empirical investigation by Kraimer et al. (1999) in the hospital setting found that nurses' belief in the impact of their job tasks influences their commitment to the organization. Commitment refers to a strength of one's involvement with a a particular organization (Porter et al., 1974). These results indicate that individuals are willing to engage and work hard in their job when they believe that their actions provide significant influence to organizational outcomes.

In the IS security context, few researchers have considered a concept similar to perceived impact (Herath and Rao, 2009a; Anderson and Agarwal, 2010). Herath and Rao (2009a) considered perceived effectiveness as the belief of individuals that their IS security action can make a difference and have impact on the overall organizational IS security goal. Anderson and Agarwal (2010) considered perceived citizen efficacy as an individual's belief that one's actions can make a difference in securing the Internet. Taken together, these studies concluded that the relation between perceived impact and IS security behavior and intention to comply with organizational IS security policy was significant. This suggests that individuals with a strong belief that they can engage in IS security actions and behaviors that contribute to the betterment

of others (e.g., organization, society) are more likely to undertake the prescribed and required IS security actions or behaviors.

Consistent with the intrinsic motivation theory, stewardship theory, and the empirical evidence, it is predicted that if employees believe that the IS security actions can have an impact and influence on the organization IS security goals, they are motivated to carry out IS security tasks in the form of the required IS security policy compliance behaviors. For example, if employees believe that by creating a strong password, they will contribute to the IS security goals, such as ensuring confidentiality of the information, they try hard to undertake the password protection task (i.e. complying with password policy). Thus, it can be hypothesized that:

> *H_3: Perceived impact of IS security tasks positively affects one's intention to comply with the requirements of the IS security policies.*

Choice and IS security policy compliance intention

Perceived choice refers to individual' assessment of freedom or experience of self-determination in their actions of a specific task (Deci and Ryan, 1985; Thomas and Velthouse, 1990). According to intrinsic motivation theory, when individuals experience a high degree of choice regarding a task, they are aware that their views and insights related to the task matter (Thomas, 2009). As a result, such individuals will feel a strong sense of ownership of the task and feel a personal responsibility towards the outcomes of their decisions, and, thus, be more likely to put more effort towards accomplishing the goals of the task (Thomas and Velthouse, 1990). Similarly, self-determination theory (SDT) holds that individuals have a psychological need for self-determination. This need motivates individual to engage and accomplish tasks that may provide them with a sense of self-determination (Deci and Ryan, 1985; Ryan and Deci, 2000).

Kraimer et al. (1999) defined self-determination at work as relating to an individual's identification with and involvement in a particular organization. Kraimer et al. (1999) found that individuals who experience a sense of self-determination with their job were more committed to the organization, by means of more involvement with the job. Similarly, Logan and Ganster (2007) reported that self-determination of task significantly related to improved performance of the task. Performance was measured by a composite of the frequency of accidents, breakdowns, and maintenance expenses related to the task. This indicates that employees who experience a high degree of discretion in carrying out their task feel a personal responsibility towards the outcomes of the task. Consequently, they put more effort to improve the performance of the task.

In the IS literature, perceived choice has also been shown to have a significant impact on open source software (OSS) projects (Ke and Zhang, 2011). The authors recorded that individuals with a sense of autonomy in tasks related to an OSS project are more likely to expend high levels of effort on the project tasks. In the context of IS security policy compliance in organizations, if employees believe that their views and insights related to IS security task matter and are the responsible decision makers that regulate their own IS security tasks, they are more likely to carry out the prescribed IS security behaviors. Thus, perceived choice would translate into accomplished IS security tasks by means of the effort expended on the required tasks. Taking into account the above supporting evidence, it is hypothesized that:

> *H_4: Perceived choice of IS security task positively affects one's intention to comply with the requirements of the IS security policies*

As a conclusion thus far, it is predicted that an intrinsically motivated employee anticipates complying with the requirements of the IS security policy when he/she assesses the intrinsic value experience (rewards) in term of feelings of competence, meaningfulness, impact,

and choice, through the IS security task itself. Table 0.1 summarizes the four constructs of psychological empowerment of IS security task and IS security policy compliance intentions.

Table 0.1: Summary of constructs

Construct	Definition	Sources
Sense of Competence	An employee's assessment of personal skills, knowledge, or competency about the IS security task.	Deci and Ryan (1985); Thomas and Velthouse (1990)
Sense of Meaning	An employee's assessment on how the goal or value of the IS security task is significant to their own value.	Hackman and Oldham (1980); Thomas and Velthouse (1990)
Sense of Impact	An employee's assessment on how the IS security task can make a significant difference to the organization in terms of accomplishing the goal of the IS security.	Hackman and Oldham (1980); Thomas and Velthouse (1990)
Sense of Choice (Autonomy)	An employee's assessment of freedom or experience self-determination in the IS security task.	Hackman and Oldham (1980); Deci and Ryan (1985); Thomas and Velthouse (1990)
Intention to comply with IS security policy	An employee's intention to execute the IS security task in order to protect the information and technology resources of the organization from potential security breaches.	Bulgurcu et al. (2009)

Drivers to enhance the psychological empowerment

As previously hypothesized, an employee's perception of intrinsic motivation, operationalized in terms of the four dimensions of psychological empowerment—sense of competence, meaning, impact, and choice of IS security tasks—are antecedents of one's IS security policy compliance intention. This study also investigates how an employee forms these perceptions. Theory and literature have acknowledged that perceptions of psychological

empowerment may be influenced by factors external to individuals (Hackman and Oldham, 1980; Deci and Ryan, 1985: Thomas and Velthouse, 1990; Spreitzer, 1995a). Furthermore, Maynard et al. (2012) urged researchers to determine potential factors that may serve as antecedents to certain dimensions (and not to others) of psychological empowerment. Based on Kanter's (1977) work on structural empowerment, three factors were investigated (a) security education, training and awareness (SETA) programs, (b) access to information about the strategy and goals of organizational IS security, and (c) participation in IS security decision-making. The following section explains how these factors enhance one's intrinsic motivation.

Security Education, Training, and Awareness (SETA) and psychological empowerment

Intrinsic motivation theory purports that educational efforts contribute to individuals' intrinsic motivation in terms of increasing their belief in their capability to perform task activities skillfully (Thomas and Velthouse, 1990; Spreitzer et al., 2007). Further, Bandura (1997) proposed that self-efficacy beliefs are developed through "enactive mastery experiences that serve as indicators of capability; vicarious experiences that alter efficacy beliefs through transmission of competencies and comparisons with the attainments of others; verbal persuasion and other types of social influence that one possesses certain capabilities; and physiological and affective states from which people judge their capableness, strength, and vulnerability to dysfunction" (p. 79). Accordingly, Agarwal et al. (2000) stated that training provides opportunities for enactive mastery through the hands-on experience of a task, vicarious experience by watching others perform a task, verbal persuasion through feedback on one's performance, and psychological and affective states induced by the interaction with a task, such as stress and anxiety.

There is extensive prior research linking training and education, and competence or self-efficacy (e.g., Gist et al., 1989; Agarwal et al., 2000; Liao et al., 2009). In a meta-analysis study, Seibert et al. (2011) examined the impact of training on perceived competence. The authors concluded that employees' feelings of competence in work roles were reflected by enhanced knowledge, skills, and abilities resulting from the training programs. Extensive training may also enhance employees' confidence in their competence in service tasks (Liao et al., 2009). In an experiment with 108 managers and administrators in a university, Gist et al. (1989) found a significant positive relations between training of computer and software, and computer and software self-efficacy. Further, Karsten and Roth (1998) reported that training experience is associated with student perceptions of their ability to use computers effectively. These findings suggest that within a training environment, individuals are progressively provided with greater opportunity for learning, experience, and practice with a particular task, computer or software, and over time, develop self-efficacy regarding the task, computer or software.

In the IS security context, security, education, training and awareness (SETA) programs focus on providing users with general knowledge of IS security environment, along with the skills necessary to perform the required IS security tasks (Whitman et al., 2001; Lee and Lee, 2002; c.f. D'Arcy et al., 2009). The content and scope of the SETA program may vary. For example, SETA programs could include information on day-to-day physical security issues, the certainty and severity of penalties, the range of technical and managerial controls to cope with systems risks, and how this information can be used to take actions (Straub and Welke, 1998; Furnell et al., 2002). From a different perspective, Puhakainen and Siponen (2010) suggested that IS security training should consider the individuals' past knowledge of IS security policy compliance. Irrespective of the specific content of these programs, the main reason for SETA

programs is to review the IS security policies and educate employees on how best to protect organizational information systems (Straub and Welke, 1998, Harris, 2010). This can take the form of various efforts, including reviewing media reports of recent security attacks on other companies and discussing how those companies could have avoided the attacks, showing a security video, a combination of courses, seminars, handouts, directives, reminders, and newsletters (Murray, 1991; Mitnick, 2002).

Three out of the four sources of information that are considered essential to self-efficacy (Bandura, 1977) will be able to obtain from a SETA program. For example, individuals gather personal mastery of IS security via hands-on exercises and activities of IS security or regular demonstration of IS security issues and respective countermeasures. Further, SETA provides opportunities to observe the successes and failures of other IS security behaviors. Consequently, this information provides a guideline to employees against which they compare their own self-efficacy (Gist et al., 1989). In addition, verbal persuasion is regularly delivered in a SETA program. Individuals receive suggestions from instructors that encourage and support their IS security skills and foster a responsible development. Thus, it is expected that self-efficacy in IS security may be developed through the ongoing acquisition of knowledge related to IS security, such as knowledge about IS security issues, the consequences, the controls to cope with the issues, and how to take action when such issues occur through SETA. This leads to the following hypothesis:

> *$H_{5:}$ SETA programs are positively associated with one's perception of competence of IS security tasks*

Access to organizational IS security strategy and goals and psychological empowerment

Hoffman (1994), in the context of emerging information technology (IT), stated that, "to support worker empowerment throughout our enterprise we will be prepared to provide every

worker with all information relevant to that worker's job regardless of its effect on the company as a whole" (Hoffman, 1994, p. 55). Information might include data about a firm's strategy and goals (Lawler, 1992; Spreitzer, 1996). Liao et al. (2009) asserted that an employee's experiences of a HPWS, including information sharing, might assist an employee in perceiving the service tasks as meaningful and important. Information about a strategy or operational goals allows employees to see their work as personally meaningful because they understand how it fits into their organization's goals and strategies (Seibert et al., 2011). In other words, access to information about strategy and goals allows an individual to see the "big picture" and hence creates and understanding on how one's work can contribute to organizational goals (Bowen and Lawler, 1992). The broader research into the effect of access to information regarding organizational strategy and goals supports this view as well. For instance, Spreitzer (1996) showed that providing access to information about the strategy and goals of an organization enhances employee knowledge about the direction of the organization. As a result, employees felf confident in how their work roles can contribute to these goals. In support of this, a meta-analysis by Seibert et al. (2011) concluded that there was a significant relation between HPWS, including sharing of information about organizational strategy and goals and the four dimensions of psychological empowerment.

Accordingly, in the context of this study, access to an organization's IS security strategy and goals denotes the extent to which the work structure provides opportunities for employees to obtain and understand the organization's IS security strategic information, objectives, and goals. This could be accomplished by communicating a IS security policy that consists of the goals regarding IS security (Straub, 1990; Boss et al., 2009). Access to information regarding an IS security strategy and goals should allow individuals to feel informed about where an

organization is headed in the context of IS security. When employees understand the direction in which the organization is heading, they tend to be more aware about how their own IS security tasks contribute to achieving the stated IS security goals. That is, employees acquire a greater sense that the IS security task is meaningful to be executed because they know that their IS security task is supporting the IS security goals and benefit the organization. Thus, access to an organization's IS security strategy and it's associated goals is expected to correlate with perceived meaning. This leads to the following hypothesis:

> *H_6: Access to the organizational IS security strategy and goals is positively associated with one's perceived meaningfulness of IS security task.*

Participation in IS security decision-making and psychological empowerment

Participation in decision-making refers to the act of sharing decision-making with others to achieve organizational goals (Knoop, 1995). Thus, participation in decision-making indicates that employees at all levels are able to provide input and influence over decisions related to a specific task or job (Cotton et al., 1988). In the context of IS security, participation relates to an individual's involvement in the IS security decision-making process. Spears and Barki (2010) defined participation in security risk management (SRM) as a set of activities assigned to individuals during risk assessment, design, and implementation of IS security controls. SRM comprises of strategies, policies, roles, and procedures to manage the security risks (Spears and Barki, 2010). Participation in IS security decision-making should allow individuals to contribute their inputs and thoughts pertinent to the IS security in order to achieve the organizational IS security goals. Fostering participation in decision-making in turn strengthens the motivation of employees to engage in IS security-related behaviors by providing them with the opportunity to attain intrinsic rewards from their work, including a greater experience of self-determination,

meaningfulness, and impact (Scandura et al., 1986; Manz and Sims Jr, 1987; Lawler, 1992; Spreitzer, 1996).

When employees are involved in decision-making processes related to IS security tasks, they have the opportunity to contribute their inputs, such as ideas and thoughts, to accomplish the goals of the IS security policy. Thus, participation allows employees to feel that they have the opportunity for freedom and independence for IS security task-related decisions. Participation is an influential source of self-determination because it provides evidence that ones' inputs, thoughts, contribution, and activities related to their job matter (Lawler, 1992; Spreitzer, 1996). In a case study setting in IS security, Dhillon et al. (2004) found that most employees in an organization did not feel a sense of freedom because they were left out from all major decision-making and had no say on the latest developments related to IS security in the organization.

In addition, greater participation might be the impetus to enhance individuals' feeling of impact (Seibert et al., 2011). When employees participate in the decision-making process related to their IS security task, they have the opportunity to set decisions jointly with the superiors. This likely influences the extent to which employees feel that they can impact their work environment. Spreitzer (1996) provided empirical evidence of the relations between participation in decision-making and perceived impact. The study concluded that participation signals to the employees that they are an important asset of the organization and that they can impact, or make a significant difference to the organization (Spreitzer, 1996). Further, when employees are allowed to participate in the decision-making process related to their IS security task, they have the opportunity to provide input that is consistent with their own values or needs. That is, the IS security task is shaped by their own values and needs. Because of this, they are more likely to perceive that the IS security tasks are meaningful and important. Hon and Rensvold (2006) has

provided evidence showing that participation was strongly related to perceived meaning of a task. Collectively, it is thus expected that if employees involved in decision-making processes related to the IS security tasks, they have opportunities to contribute their input to accomplish the IS security objectives and affect the work environment. Consequently, their perceptions of meaning, impact, and choice of the IS security tasks should be higher. This predicted effect is formally recognized in the following hypotheses:

> *H_7: Participation in IS security decision-making is positively associated with perceived meaning of IS security tasks.*
>
> *H_8: Participation in IS security decision-making is positively associated with perceived impact of IS security tasks.*
>
> *H_9: Participation in IS security decision-making is positively associated with perceived choice of IS security tasks.*

Mediating effect of dimensions of psychological empowerment

The above nine hypotheses combine to form a mediation model. It signifies that the psychological empowerment dimensions (i.e., feelings of competence, meaning, impact, and choice) mediate the relations between the structural empowerment facets (i.e., SETA, access to IS security strategy and goals, and participation in IS security decision-making) and the intention to comply with organizational IS security policy.

In the context of this study, psychological empowerment reflects how individuals feel about their self-determination over their IS security task-related decisions, their IS security task competence, and their sense of meaning and impact of the IS security tasks. Based on the previously presented arguments, it is expected that psychological empowerment is influenced by organizational practices that provide opportunities to nurture self-efficacy through IS security training, get involved in IS security decision-making processes, and access information about the IS security strategy and it's goals. In return, the increased feelings of empowerment that

individuals receive motivate them to perform well with the IS security tasks, measured by their IS security policy compliance intentions.

Prior studies provide evidence that elements of structural empowerment are associated with psychological empowerment, which in turn are related to work related performance (Spreitzer, 2007). For instance, training influences employees' task performance by empowering them to feel competent (Gist and Mitchell, 1992; Seibert et al., 2011). Thus, it is expected that employees develop a sense that their capability to perform IS security-related tasks that increases their IS security task performance as a consequence of SETA programs. Further, access to information can affect task performance through psychological empowerment by giving employees the perception that their work tasks are meaningful (Spreitzer, 1996). In the context of this study, it is predicted that access to IS security strategy and its goals influences employee IS security task performance by empowering employees to feel how their IS security tasks would contribute to achieving the IS security goals. Meta-analytic research has provided evidence that participation in decision-making can motivate employees to perform well through psychological empowerment by giving employees the perception that they have a choice and have an impact in their work (Seibert et al., 2011). Thus, employees feel that the IS security task is self-determined, has meaning, and is impactful when they are involved in the IS security task decision-making process. Consequently, their intention to comply and engage in IS security tasks should increase. Taken together, different dimensions of psychological empowerment may mediate the relations between structural empowerment facets and IS security policy compliance intentions.

H_{10}: Perceived competence mediates the relations between SETA and one's intention to comply with the IS security policy.

H_{11}: Perceived meaning mediates the relations between access to information regarding IS security strategy and goals, and one's intention to comply with the IS security policy.

H_{12a}: Perceived meaning mediates the relations between participation in IS security decision-making, and one's intention to comply with the IS security policy.

H_{12b}: Perceived impact mediates the relations between participation in IS security decision-making, and one's intention to comply with the IS security policy.

H_{12c}: Perceived choice mediates the relations between participation in IS security decision-making, and one's intention to comply with the IS security policy.

3.4 Conclusion

This chapter started by explaining how the theory of intrinsic motivation can be applied to explain IS security policy compliance behavior. Following this discussion, a conceptual framework and specific hypotheses were developed based on Thomas and Velthouse's (1990) intrinsic motivation theory and Kanter's (1977) structural empowerment theory. Table 0.2 summarizes the hypotheses. The proposed conceptual framework will be tested in Chapter 5 using the data gathered in this study.

Table 0.2: Summary of Proposed Hypotheses

Hypotheses	Description
H_1	Perceived competence of IS security task positively affects one's intention to comply with the IS security policies.
H_2	Perceived meaningfulness of IS security task positively affects one's intention to comply with the IS security policies.
H_3	Perceived impact of IS security task positively affects one's intention to comply with the IS security policies.
H_4	Perceived choice of IS security task positively affects one's intention to comply with the IS security policies.
H_5	SETA programs are positively associated with one's perceived competence of IS security task.
H_6	Access to the organizational IS security strategy and goals is positively associated with one's perceived meaningfulness of IS security task.
H_7	Participation in IS security decision making is positively associated with one's perceived meaningfulness of IS security task.
H_8	Participation in IS security decision making is positively associated with one's perceived impact of IS security task.
H_9	Participation in IS security decision making is positively associated with one's perceived freedom of IS security task.
H_{10}	The effect of SETA on one's intention to comply with IS security policies is mediated by perceived competence of IS security task.
H_{11}	The effect of access to IS security strategy and goals on one's intention to comply with IS security policies is mediated by perceived competence and meaningfulness of IS security task.
H_{12a}	The effect of participation in IS security decision making on one's intention to comply with IS security policies is mediated by perceived meaningfulness of IS security task.
H_{12b}	The effect of participation in IS security decision making on one's intention to comply with IS security policies is mediated by perceived impact of IS security task.
H_{12c}	The effect of participation in IS security decision making on one's intention to comply with IS security policies is mediated by perceived choice of IS security task.
H_{13}	The interaction of access to IS security strategy and goals and participation in IS security decision-making is related to perceived meaningfulness of IS security task.

Chapter 4. Research Methodology

4.1 Introduction

The previous chapter has identified the theoretical background of this research and subsequently developed the research framework (see Figure 3.1). The proposed research framework has been designed to explore the relations among structural empowerment facets, psychological empowerment dimensions, and IS security policy compliance intentions. This chapter describes the methodology used to assess the proposed relations. The remainder of this section presents the research population and sample, the data collection procedures, the measures, and the data analysis approach.

4.2 Research population and sample

As the primary thrust of this study is to investigate the relations between individuals' perception of psychological empowerment related to IS security tasks and IS security policy compliance intention at the workplace, employees in different jobs and levels were thought to be appropriate as the target population. The unit of analysis is individual and the convenience-sampling technique was used as the sampling strategy. The convenience sampling is a sampling procedure to obtain people who are easily available (Zikmund, 2000). Specifically, the respondents in this study were MBA, Executive MBA, and Executive MIS students enrolled in two public universities in the US. The rationale of selecting students in the US as a sample are because the researcher herself is a student in the US, which has enabled easy access to the data

sources; and to obtain a larger number of completed questionnaires quickly and economically (Zikmund, 2000). The limitations of using a student sample is discussed later in chapter 7.

Hair et al. (2010) recommended a sample size in the range of 100 to 400 as appropriate to run data using structural equation modeling (SEM). Other researchers have claimed that a sample size of 300 is enough (e.g., Comrey and Lee, 1992; Tabachnick and Fidell, 2001). This, however, is subject to other considerations such as the number of constructs and items (Hair et al., 2010). Nunnally (1978) suggested that in SEM estimation, a good rule is to have at least ten times as many subjects as variables. In MIS research that used SEM, the rule of thumb of 10 cases per indicator in setting a lower bound of sample size was widely used (Westland, 2010). Therefore, this study has attempted to yield approximately 250 or above usable samples in order to satisfy the statistical recommendations of 10 cases per indicator, based on twenty-five items in the questionnaire.

4.3 Data collection procedures

This study is a cross-sectional study because the data was collected at a single point in time. The data were collected using a self-administered survey, where the researcher administered the questionnaires in classes or sent through e-mail to graduate students. Zikmund (2003) stated that self-administered questionnaires could be widely distributed to a large number of respondents with minimal cost compared to other types of data collection. Another strength of this method is that respondent confidentiality and anonymity can be assured (Davis, 2000).

The instructors for the MBA, the Executive MBA, and the Executive MIS programs were contacted to ask for permission to distribute the questionnaire in their classes. Once permission was granted, the researcher attended the classes and explained to the students the purpose of the study. Then, the questionnaire and a cover letter explaining the purpose of the study, the

information about voluntariness, confidentiality, and anonymity were distributed. With the help of the instructors, the questionnaires were collected after class. In addition, the students were able to submit the completed questionnaires in a box at the graduate student office. Some instructors allocated 20 to 30 minutes of the class time for the students to immediately answer the questionnaires. This helped to increase the response rate.

For some classes, a web survey was distributed to students by e-mail sent directly by the instructors. The web survey was prepared using the Google doc survey tool. The e-mail stated the purpose of the study and asked students to complete the survey. The students were able to access the survey through clicking the survey site URL (hyperlink) embedded within the e-mail. In both methods (paper and pencil and electronic), respondents were required to answer a set of exclusion criteria questions to determine whether a person should participate in a research study or whether he/she should be excluded in a systematic review. The exclusion questions were: (1) How long you have been working with the current organization; (2) Is your organization has IS security policy; and (3) Do you aware of the requirements of the IS security policy? This criteria help to identify suitable participants that are currently employed and have knowledge about their organization's IS security policy.

Overall, 410 surveys (paper and pencil and electronic) were distributed to the participants and 326 complete responses were returned within five months. The final response rate for the survey data collection was 79.5%. Detailed response profiles are reported in Chapter 5, in addition to an evaluation of missing data, an assessment of normality, an examination of outliers, and an assessment of common method variance.

4.4 Measurement of constructs

Reliability is a test of the consistency and repeatability of the items to measure a construct (Zikmund, 2003). One of the common methods to assess the reliability of a measure is an average of split-half correlation (i.e., Cronbach's alpha, α) with a cut-off value of .7 (Zikmund, 2003). The following section defines and describes the measures to assess the constructs in the proposed research framework. All measures were adapted from previously validated studies. All the questionnaire items were self-assessments and used seven-point Likert-type scales with anchors ranging from 1 (strongly disagree) to 7 (strongly agree).

IS security policy compliance intentions. IS security policy compliance intentions refer to the extent to which employees intend to perform the IS security tasks in order to protect the information and technology resources of the organization from potential security breaches. The compliant behaviors do not imply that one security behavior is better than the other, but involvement in one or more behaviors can help mitigate security breaches, thus improving organizational IS security performance. Three items were used from Bulgurcu et al. (2010) to measure IS security policy compliance intentions. For instance, respondents were asked how much do they agree or disagree with statements, such as "I intend to comply with the requirements of the IS security policy of my organization," "I intend to protect information and technology resources according to the requirements of the IS security policy of my organization," and "I intend to carry out my responsibilities prescribed in the IS security policy of my organization when I use information and technology." Likert-type scale with response options ranged from (1) strongly disagree to (7) strongly agree. The measure had an acceptable level of internal consistency (α = .75).

Psychological empowerment. In order to assess the appropriateness of using the individual dimensions of psychological empowerment instead of a single, global psychological empowerment construct, consistent with previous research, CFAs was used. These CFAs shown that the hypothesized four-factor model (χ^2 = 91.45 with *df* = 48; RMSEA=.056; SRMR = .047; CFI = .98; NFI = .96) fit the data better than a model with one construct (χ^2 = 111.85 with df = 50; RMSEA=.066; SRMR = .075; CFI = .97; NFI = .95). These results are consistent with previous research that showed that the four dimensions of psychological empowerment are distinct (e.g. Spreitzer et al., 1997; Kraimer et al., 1999). Further, a chi-square difference test was performed and the result confirms that the models are different ($p < .05$). Thus, the four individual facets of psychological empowerment, feelings of competence, meaning, impact, and choice, were used to separately test the hypotheses.

Competence. This measure captures the employees' perception regarding their personal skills and competence about IS security tasks. Specifically, the items represent the extent to which employees feel confidence in their ability to master the skills needed to protect the organizational information. Three items were adapted from Spreitzer (1995a) to measure perceived competence. Respondents were asked how much do they agree or disagree with statements, such as "I am confident about my ability to do my job of securing information and information systems" and "I am self-assured about my capabilities to perform my job of securing information and information systems activities." Likert-type scale with response options ranged from (1) strongly disagree to (7) strongly agree. The scale has a high level of internal consistency reliability (α = .89).

Meaning. Meaning captures the extent to which employees perceive the value of the IS security tasks as significant to their own value. Perceptions of meaning was measured using three

items from Spreitzer (1995a). Respondents were asked to specify the degree to which they agreed or disagreed with a set of statements using a likert-type scale with response options ranged from (1) strongly disagree to (7) strongly agree. Items included, "My work of securing information and information systems is very important to me," "My work of securing information and information systems is personally meaningful to me," and "My work of securing information and information systems is meaningful to me." The scale had a high level of internal consistency reliability (α = .91).

Impact. Perceived impact is an employee's assessment on how performing the IS security tasks can make a significant difference to the organization in terms of accomplishing the goal of IS security. More specifically, this construct captures the extent to which employees feel that their action related to IS security affects the organization. Perceived impact from the employees' perspective was measured using three items from Spreitzer (1995a). As an example, respondents were asked to what degree to which they agreed or disagreed with "my impact of what happens in my department related to IS security is large" and "I have significant influence over what happens in my department related to IS security." Likert-type scale with response options ranged from (1) strongly disagree to (7) strongly agree. The scale had a high level of internal consistency (α = .90).

Choice. Perceived choice is an employee's assessment on how he/she has experience a sense of choice in initiating and regulating the IS security tasks. Perceived choice was measured from the employee perspective, using three items from Spreitzer (1995a). For instance, respondents were asked to specify the degree to which they agree or disagree with a set of statements, such as "I have significant autonomy in determining how I do my job of securing information and information systems" and "I have considerable opportunity for independence

and freedom in how I do my job of securing information and information systems." Likert-type scale with response options ranged from (1) strongly disagree to (7) strongly agree. The scale had an acceptable level of internal consistency (α = .78).

Security education, training and awareness (SETA). The SETA measure was created to assess the employees' perceptions regarding the amount of education, training and awareness of the IS security breaches and the counter-measures the employees receive from the organization. SETA was measured using five items from D'Arcy et al. (2009). Respondents were asked to what degree they agree or disagree with various statements, such as "I receive training to help me improve my awareness of computer and IS security issues," "I am briefed on the consequences of modifying computerized data in an unauthorized way," and "I receive an education on my computer security responsibilities." Likert-type scale with response options ranged from (1) strongly disagree to (7) strongly agree. The scale had an acceptable level of reliability (α = .88).

Access to IS security strategy and goals. Three items, adapted from Spreitzer (1995a), were used to assess employees' perceptions of the extent of access they have to strategic information related to IS security in the organization. As an illustration, respondents were asked to specify the extent to which they agree or disagree with statements, such as "I have access to the strategic information I need to do my job of securing information and information systems well" and "I understand the IS security strategies and goals of the organization." Likert-type scale with response options ranged from (1) strongly disagree to (7) strongly agree. The scale showed an acceptable level of internal consistency (α = .76).

Participation in IS security decision-making. The scale to assess participation in decision-making related to IS security was used to assess employees' perceptions of their

involvement in defining, reviewing or approving IS security control, as well as how well they can contribute to the risk management activities in the organization. Two items to measure participation were adapted from Spears and Barki (2010). Respondents were asked to specify the extent to which they agree or disagree with statements, including "I actively participate in defining, reviewing or approving any IS security controls related to protecting the organization's information" and "In managing risk to information and information systems in my company, I actively perform, or contribute to decision-making in any risk management activities." Likert-type scale with response options ranged from (1) strongly disagree to (7) strongly agree. The scale had an acceptable level of reliability (α = .78). A summary of the variables investigated in this dissertation is included in Table 0.1.

Common method variance

According to Podsakoff et al. (2003, p. 879), "method variance refers to the variance that is attributable to the measurement method rather than to the construct of interest." Common method variance (CMV), one of the sources of measurement errors, can have serious influences on the observed relations between the predictor and outcome variables in organizational and behavioral research (Podsakoff et al., 2003). CMV may occur when data is collected by one method or at a single point of time. When data is collected in such a way, the variance that the items have in common with each other may be due to the collection method, rather than to the relations between the items and their respective constructs or the relations among the constructs. In order to control for CMV, Podsakoff et al. (2003) suggested two techniques: (1) procedural remedies and (2) statistical control.

Table 0.1: Measurement items and the source

Variable	Item	Source
ISPC1	I intend to comply with the requirements of the ISP of my organization in the future.	Bulgurcu et al. (2010)
ISPC2	I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future.	Bulgurcu et al. (2010)
ISPC3	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future.	Bulgurcu et al. (2010)
PACT1	My impact of what happens in my department related to IS security is large.	Spreitzer (1995a)
PACT2	I have a great deal of control over what happens in my department related to IS security.	Spreitzer (1995a)
PACT3	I have significant influence over what happens in my department related to IS security.	Spreitzer (1995a)
COMP1	I am confident about my ability to do my job of securing information and information systems.	Spreitzer (1995a)
COMP2	I am self-assured about my capabilities to perform my job of securing information and information systems activities.	Spreitzer (1995a)
COMP3	I have mastered the skills necessary for my job of securing information and information systems.	Spreitzer (1995a)
MEAN1	My work of securing information and information systems is very important to me.	Spreitzer (1995a)
MEAN2	My work of securing information and information systems is personally meaningful to me.	Spreitzer (1995a)
MEAN3	My work of securing information and information systems is meaningful to me.	Spreitzer (1995a)
CHOI1	I have significant autonomy in determining how I do my job of securing information and information systems.	Spreitzer (1995a)
CHOI2	I can decide on my own how to go about doing my job of securing information and information systems.	Spreitzer (1995a)
CHOI3	I have considerable opportunity for independence and freedom in how I do my job of securing information and information systems.	Spreitzer (1995a)
SETA1	I receive training to help me improve my awareness of computer and information security issues.	D'Arcy et al. (2009)
SETA2	I receive education on computer software copyright laws.	D'Arcy et al. (2009)
SETA3	I am briefed on the consequences of modifying computerized data in an unauthorized way.	D'Arcy et al. (2009)
SETA4	I receive education on my computer security responsibilities.	D'Arcy et al. (2009)
SETA5	I am briefed on the consequences of accessing computer systems that I am not authorized to use.	D'Arcy et al. (2009)
ACC1	I have access to the strategic information I need to do my job of securing information and information systems well.	Spreitzer (1996)
ACC2	I understand top management's IS security vision of the organization.	Spreitzer (1996)
ACC3	I understand the IS security strategies and goals of the organization.	Spreitzer (1996)
PART1	I actively participate in defining, reviewing or approving any IS security controls related to protecting the organization's information (e.g. access control, separation of duties, employee training on IS security awareness and etc.)	Spears and Barki (2010)
PART2	In managing risk to information and information systems in my company, I actively perform, or contribute to decision-making in any risk management activities (e.g. documenting business processes or transactions for risk evaluation, ensuring key controls exist to mitigate specific types of risks, implementing control and etc.)	Spears and Barki (2010)

Procedural remedies are aiming to minimize or mitigate CMV between predictor and criterion variables through the design of the research. First, CMV can be controlled by obtaining different sources for independent variable (IV) and dependent variables (DV) (Podsakoff et al., 2003). Therefore, the measures for the DV (IS security policy compliance intentions) and the IVs (dimensions of psychological empowerment and structural empowerment) should be collected from different sources. However, this option was not practical for this study due to time and resource constraints. In addition, it might not be appropriate in this research setting because students were used as the respondents. If the data were collected in an actual organizational setting, the researcher could have collected information from the employees (IVs) and management or supervisors (DV).

Podsakoff et al. (2003) suggested a temporal separation in collecting the IV and the DV. To do this, a longitudinal study that involves a series of measurement for a period of time should be used. However, as this research used a cross-sectional design rather than a longitudinal approach, both the IVs and DV were measured at the same point in time, due to time and resources constraints. Another reason for the used of a cross-sectional design was to ensure anonymity of the respondents. If the collection of IVs and DV are separated, researchers need to apply some kind of method to link the data from the different time periods, which can compromise the anonymity. Protection of respondents' anonymity is another method to control for common method variance (Podsakoff et al., 2003). Anonymity allows respondents to answer as honestly as possible. Consequently, they are less likely to respond based on social desirability or what the researcher wants. Thus, this study used this technique wherein respondents' identities were not collected. The counterbalancing question order is another method suggested by Podsakoff et al. (2003) to reduce CMV. This technique requires that the items for the same

construct are not clustered together. This is to reduce the item-context-induced mood state (Podsakoff et al., 2003). This technique was used to reduce CMV. To ensure the items were grouped back into their specific construct for the data analysis purpose, each item was assigned a unique identifier.

Although a substantial effort has been made during the design stage to reduce CMV using two procedural remedies, Podsakoff et al. (2003) suggested that it may be useful to use one of the statistical remedies to minimize, if not totally eliminate, the effect of CMV. Researchers use many statistical remedies to control for CMV, such as Harman's single-factor test, partial correlation procedures designed to control for method biases, controlling for the effects of a single unmeasured latent method factor, and use of multiple-method factors to control method variance etc. (Podsakoff et al., 2003).

Harman's single-factor test is one of the most widely used techniques to address the issue of CMV (Podsakoff et al., 2003). Conventionally, researchers load all the variables in the study into an exploratory factor analysis (EFA) and examine the unrotated factor solution to determine the number of factors that are necessary to account for the variance in the variables (Podsakoff et al., 2003). This technique assumes that CMV exists if a single factor will emerge from the analysis or one general factor will account for the majority of the covariance among the variables (Podsakoff et al., 2003). More recently, some researchers have used confirmatory factor analysis (CFA) as a more sophisticated method to test of the hypothesis that a single factor accounts for all the variance in the data (Iverson and Maguire, 2000; Korsgaard and Roberson, 1995; Mossholder, Bennett, Kemery, and Wesolowski, 1998 cf. Podsakoff et al., 2003). Harman's single-factor was used to statistically assess the possibility the CMV has affected the reported results (see section 5.2).

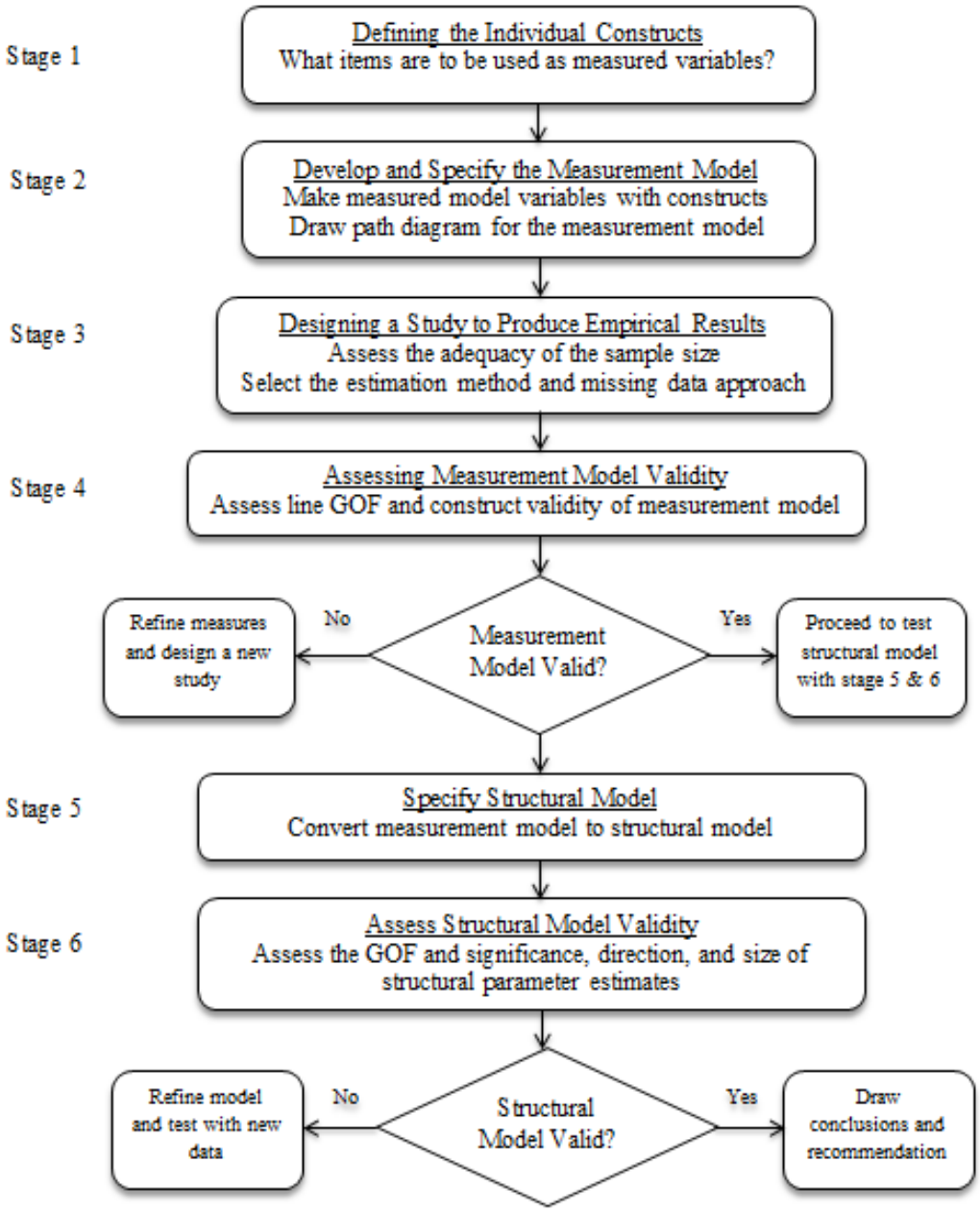
4.5 Analysis of data

Structural equation modeling (SEM) was used to analyze the measurement model and to test the hypotheses of the proposed research model. Empirical studies show that the use of SEM is widespread in information systems research (Gefen et al., 2000). SEM, a multivariate statistical technique, is a powerful quantitative data analytical tool that enables researchers to observe the structural element (path model) and measurement element (factor model) simultaneously (Gefen et al., 2000). Hair et al. (2010) stated that SEM is most appropriate when the research has multiple constructs that can be differentiated as DVs and IVs, and each construct is assessed with multiple items. Unlike other multivariate techniques, SEM can handle constructs that act as the IV in one relations and as the DV in another relations, and the relations can be run simultaneously (Hair et al., 2010). AMOS version 18 was used. Following Hair et al. (2010), this study used the six stage decision process of SEM as shown in Figure 0.1 below.

Stage 1 involves the process of *defining the individual constructs.* At this stage, a researcher operationalizes a construct by selecting scale items and the scale type (Hair et al., 2010). In this study, items and scales were obtained from prior research studies (section 4.4). Stage 2 involves the *development and specification of the measurement model*. A key element in this process is the labeling of indicators, constructs, and error terms, and specifying the relations between items and constructs, and among the constructs (Hair et al., 2010). Using AMOS version 18, a measurement model for this study was developed (see Figure 9.1). The measurement model represents the relations between the latent constructs (unobserved variables) and measured variables (observed variables or indicators). The observed variables are represented by rectangles, constructs are represented by ovals, and measurement error is depicted by small circles.

At stage 3, a researcher is required to discuss the issues of research design and model estimation. In the area of research design, careful consideration should be given to the type of data to be analyzed, impact and remedy of missing data, and impact of sample size (Hair et al., 2010). As recommended by Hair et al. (2010), covariance matrices were used to analyze the data. Next, one must address the issue of missing data, which could affect the generalizability of the obtained results (Hair et al., 2010). A missing data pattern should be identified to determine an appropriate treatment for the missing data. In doing this, the percentage of variables with missing data for each case and the number of cases with missing data for each variable was tabulated. The analysis was performed with the Missing Value Analysis (MVA) module in SPSS. During this analysis, variables and cases that would be possible candidates for deletion were identified, depending on the severity of the missing percentage (Hair et al., 2010). After that, diagnosis for the randomness of the missing data was performed to determine whether the missing data are distributed randomly across the cases and variables (Hair et al., 2010). The analysis of randomness provides insights into the appropriate remedy methods. Hair et al. (2010) suggested four basic methods, namely the complete case approach, all-available approach, imputation approach, and model-based approach. Detailed analysis for missing data is presented in section 5.2.

Figure 0.1: Stages of Structural Equation Modeling



Note: adopted from Hair et al. (2010)

Stage 4 contains a process of assessing the validity of the measurement model. This stage seeks to provide empirical support for the relations between the measured variables and the latent constructs (i.e., the model). SEM uses two tests to achieve this. The first is construct validity and the second is to test for acceptable levels of goodness-of-fit for the measurement model (Hair et

al., 2010). Construct validity is whether the measured variables (items) related to a specific latent construct are really measuring the latent construct as theoretically predicted. Two types of construct validity are convergent validity and discriminant validity. Convergent validity is whether the indicator items of a specific latent construct converge or share a very high proportion of variance. CFA outputs provide a range of information to evaluate convergent validity, such as factor loadings and average variance extracted (AVE). Factor loadings examine the size of loadings of each of the items to the latent construct. A rule of thumb is that standardized loading estimates should be .5 or higher (Hair et al., 2010; Klein, 2011). AVE may be estimated to provide additional information for the convergent validity (Hair et al, 2010). AVE is calculated as the mean variance extracted for the items loading on a construct, with a rule of thumb of .5 or higher (Hair et al, 2010). An AVE of higher than .5 indicate that, on average, more variance in the items explained by the latent construct than error remains in the items (Hair el al., 2010).

Discriminant validity is whether a construct is truly distinct from other constructs in the model. Discriminant validity shows that a construct is unique and captures a phenomenon other constructs do not. For discriminant validity, Fornell and Larcker's (1981) test was conducted. This test compares the square root of average variance extracted (AVE) of each construct with the correlations associated with that construct. AVE is the mean of the variance extracted for the items loading on a construct. To provide evidence that a construct has discriminant validity, the square root AVE should be greater in value than the correlation coefficients. That is, the variance that uniquely belongs to the construct should be greater than the variance shared between the constructs (Hair et al., 2010).

The next step is to assess the overall fit of the measurement model. Evaluation of fit, or goodness-of-fit (GOF), is a comparison between theory and reality by measuring the similarity between the observed (the proposed model) and estimated (the data) covariance matrices among the indicator items. In other words, the purpose of GOF is to check whether the proposed model explains the data or not, and if any modification is needed to improve the model fit (Kline, 2011). Hair et al. (2010) identify three classes of GOF measures:

- Absolute measures
- Incremental measures
- Parsimony fit measures

There are various fit indices produced by SEM (e.g., Chi-Square (χ^2) Statistic, comparative fit index (CFI), root mean square error of approximation (RMSEA), standardized root mean square residual (SRMR) with a different minimum or maximum value of good fit were used as the rule of thumb (Hu and Bentley, 1999; Byrne, 2009; Hair et al. 2010). However, it is unlikely to find research that reports all of those fit indexes. In fact, different fit indices were reported in different research articles in the IS domain (Gefen et al., 2000). Hair et al. (2010) asserted that it is not necessary to report all the indices to provide an assessment of fit, and suggested that researchers should rely on at least one absolute index and one incremental index in addition to the χ^2 Statistic. Kline (2011) advocates the use of the χ^2 test, the RMSEA, the CFI, and the SRMR.

Absolute Fit Indices is the most direct measure to assess on how well a proposed model fits the data (Kline, 2011; Byrne, 2009). The χ^2 statistic is looking for no difference between covariance matrices of the proposed model and the data (i.e., the lower the χ^2 the better) (Hu and Bentler, 1999). A good model fit would provide an insignificant result ($p > .05$), that is, the null hypothesis fails to be rejected (Hu and Bentler, 1999). However, since the mathematical

properties of χ^2 has sample size, the value of χ^2 is affected by the sample size. This means that the greater the sample size, the higher the value of χ^2. Due to the limitation of χ^2 related to sample size, researchers have sought alternative indices to assess model fit. CMIN (χ^2 /*df*) is a statistic that minimizes the impact of sample size on the χ^2 statistic. Although there is no consensus regarding an acceptable ratio for this statistic, a value below 2.0 indicates a very good fit (Byrne, 2009; Kline, 2011).

Another fit measure that can deal with the issue of sample size sensitivity of the χ^2 statistic is the RMSEA. RMSEA adjusts for both model complexity and sample size by including each in its computation (Hair et al., 2010). RMSEA is regarded as the most widely used measure and the most informative fit index (Diamantopoulos and Siguaw, 2000; Hair et al., 2010). Low values indicate a better fit. Hu and Bentley (1999) suggested cut-off value lower than .06 for RMSEA. Still, values as high as .08 may be acceptable (Hu and Bentler, 1999). In addition, Browne and Cudeck (1989) also suggested that values in the range of .05 to .08 indicate a fair fit, and that values greater than .10 indicate poor fit. One of the advantages of RMSEA is that it can report range values for a given level of confidence (e.g. 95% confidence). This study applies the cut-off value of .08.

The root mean square residual (RMR) and SRMR assess to the square root of the difference between the sample covariance matrix and the proposed covariance model. The RMR is an average of the covariance residuals whereas SRMR adjusts for the scale of the covariances (Hair et al., 2010). According to Byrne (2009,) the value for SRMR ranges from zero to 1.0, with well-fitting models obtaining values less than .05. Still, values as high as .08 may be acceptable (Hu and Bentler, 1999). Thus, this study applies a cut-off value of .08.

Another group of statistics to measure the fit of the model are incremental fit indices, such as the incremental fit index (IFI), the Tucker Lewis index (TLI), and the comparative fit index (CFI). Incremental fit indices differ from absolute fit indices in that they assess how well the estimated model fits any alternative baseline model (i.e., the null model) (Hair et al., 2010). Null model is hypothesized to be the simplest model that can be theoretically justify (Hair et al., 2010). The CFI is one of the most often reported fit index due to being one of the measures least affected by sample size (Bentler, 1990). The CFI ranges from zero to 1.00 with a value greater than .90 indicating acceptable model fit (Byrne, 2009). Hair et al. (2010) provided cut-off values ranges from greater than .90 to greater than .97, depending on situations (i.e., sample size and number of variables). Following Kline (2011), this study uses χ^2 statistic to assess model fit along with the SRMR, the RMSEA, and the CFI. The cut-off values are presented in Table 0.2. The analysis of measurement model is reported in section 5.3.

Table 0.2: SEM Fit Indexes and the cut-off values used for this study

	Overall Model Fit : Chi-Square (χ^2) Statistic		
	RMSEA	SRMR	CFI
Recommended value of good and acceptable fit	≤.08	≤.08	≥.9
Modification for model misspecification	>.08	>.08	<.9

Note: RMSEA = Root mean square error of approximation; SRMR = Standardized root mean square residual; CFI = Comparative fit index.
Sources: Adopted from Kline (2011); Byrne (2009); Hu and Bentley (1999).

Stage 5 is a process of *specifying the structural model.* At this stage, the validated measurement model is transformed into a structural model by assigning the relations from one construct to another, which is the proposed research framework or theoretical model. The structural model for this research is represented by the hypothesized paths, H_1 to H_{12}, as shown in Table 0.2. Figure 9.2 presents the structural model produced by AMOS.

The final stage is *validating the structural model*. The goal of this stage is to test the proposed theoretical model. In doing so, two tests are emphasized; model fit and consistency of the structural relations with theoretical expectations (Hair et al., 2010). Similar to the assessment of measurement model validity, the test of model fit uses the fit measures, such as χ^2 statistic, the SRMR, the RMSEA, and the CFI. The second test of structural model validity is to examine individual path estimates. One has to assess whether each path coefficent is consistent with the expectation (e.g., directionality, magnitude, etc). The analysis of structural model has been reported in section 5.4.

Testing for mediating effects

A mediation effect is an indirect effect of a predictor variable on an outcome variable through a mediating or intervening variable (MacKinnon et al., 2002). The indirect effect may be calculated using methods such as the causal steps procedure, or by calculating the difference in coefficients (MacKinnon et al., 2002). To formally test the mediation effect, the significance of each hypothesized indirect relation must be tested. However, according to MacKinnon et al. (2002), of 50 studies reviewed mediation, fewer than one third included any test of significance of the mediating variable. Prior studies provide much information for various methods for conducting significance tests for indirect effects, including Baron and Kenny (1986), Freedman and Schatzkin (1992), Sobel (1982), and Mackinon and Lockwood (2001). Preacher and Hayes (2008) suggested that the product-of-coefficients strategy is appropriate, as well as the bootstrapping method. Hence, this study uses product-of-coefficients test by Sobel (1982), also known as Sobel test (Sobel 1982, 1986) and the bootstrapping method (Shrout and Bolger, 1992), using the SPSS macro from Preacher and Hayes (2008).

Chapter 5. Analysis and Results

5.1 Introduction

In chapter 4, the research methodology and the design were discussed. This chapter provides information about the respondents' profile along with the data screening process, as well as the results of measurement and structural models. Most of the data in this study were analyzed using AMOS version 18. Apart from AMOS 18, SPSS was used for some analysis.

The following sections describe the tests performed, divided into three subsections: Initial data screening, assessment of measurement model, and assessment of structural model. Section 5.2 explains the following: respondents' profile, analysis of missing data, test of multivariate normality and outliers, and analysis of common method variance. In section 5.3, the measurement model will be examined. The assessment of construct validity comprises assessments of reliability, convergent validity, and discriminant validity. In section 5.4, the results of the path or structural model will be presented. The following analyses were performed: model fit, parameter estimates and diagnostics, and mediation.

5.2 Data Screening

Methodological approaches, including tests of multivariate normality, identification of missing data, identification of outliers, and analysis of common method variance (CMV) will be discussed in this section. Initial data screening of 326 complete responses identified that some respondents met the exclusion criteria questions. Those who selected that they have no IS security policy in the organization or were completely unaware of the IS security policy

requirements were excluded from the study. Additionally, respondents who did not provide information regarding years of working in their current company were also excluded. It was assumed that these respondents were not currently being employed. This resulted in a final sample size of 290 responses with potentially useable data.

Demographic Information

As reported in Table 0.1, most of the respondents were male (69%). The data also showed that the majority of the respondents have undergraduate or graduate degrees (combined 81.4%). This was expected given that the sample of respondents was obtained from graduate students. Age differences were also apparent, with most of the respondents (50.7%) were relatively young, between the ages of 26 and 35. Most of the respondents have been working with their current company less than five years (70%). Almost 35% of them were at the managerial level. In terms of the intensity of using computers at work, the respondents reported an average of 7.7 hours per day. This may indicate that the jobs require the respondents to use computers heavily, suggesting that their IS security behaviors may be important.

The results in Table 0.2 show that the industry types of the firms diverse widely. No industry dominates the others. In terms of firm size (number of employees), one-third of the firms has employees less than 500, which can be considered as small and medium sized (U.S Small Business Association [SBA], 2012).

Table 0.1: Respondents' Profile

Demographic Features	Frequency (n=290)	Percentage
Gender		
Male	202	69.7
Female	86	29.7
Missing	2	0.7
Level of Education		
College degree	45	15.5
Undergraduate degree	118	40.7
Graduate degree	118	40.7
Other	6	2.1
Missing	3	1
Age		
20 – 25	72	33.4
26 – 35	147	50.7
36 – 45	49	16.2
46 – 55	18	14.8
56 – 65	1	27.9
Missing	3	1.7
Years of working in current organization		
Less than 5 years	203	70
More than 5 years	87	30
Position in current organization		
Owner of the Firm	8	2.8
Managing Director / Director	24	8.3
Chief Executive Officer	2	7
General Manager/Manager	47	16.2
Executive/Leader/ Officer	28	9.7
Non-management	155	53.4
Missing	26	9
	Mean	**SD**
Hours of computer usage at work per day	7.7	2.5

Table 0.2: Companies' Profile

Demographic Features	Frequency (n=290)	Percentage
Firm size (by number of employees)		
Fewer than 500	97	33.4
500 – 999	17	5.9
1,000 – 4,999	47	16.2
5,000 – 10,000	43	14.8
More than 10,000	81	27.9
Missing	5	1.7
Industry		
Education	49	16.9
Financial Services	49	16.9
Government	24	8.3
Food/Beverage	5	1.7
Health Care	35	12.1
Manufacturing	17	5.9
Non-Profit	4	1.4
Medical, Bio-Technology, Pharmacology	6	2.1
Real Estate	2	0.7
Other Services	18	6.2
Information Technology	23	7.9
Telecommunications	5	1.7
Travel	0	0
Wholesale/Retail	13	4.5
Others	31	10.7
Missing	9	3.1

Examination of Missing Data

Non-ignorable missing data is data that cannot be classified as ignorable. It could be known or unknown. Known missing data is due to procedural factors such as errors in data entry and morbidity of the respondents. Researchers have little control over known non-ignorable missing data (Hair et al., 2010). Unknown missing data are instances related directly to the respondent. For example, a respondent may refuse to respond to certain questions due to the sensitivity of the question or the respondent may not have sufficient knowledge or no opinion about the question. In this situation, researchers should anticipate these problems and minimize

them in the research design and data collection process. However, if this still happens, researchers can apply certain types of remedies to mitigate the effect of missing data.

Hair et al. (2010) suggested four steps of missing data diagnosis: (1) determining the type of missing data, (2) determining the extent of missing data, (3) diagnosing the randomness of missing data, and (4) selecting a method to deal with missing data. In step 1, the type of missing data, ignorable or non-ignorable was determined. The second step was conducted to assess the extent and impact of the missing data. This was performed by tabulating the percentage and the number of missing data for each variable and case.

Table 0.3 contains the descriptive statistics for the variables, including the percentage of missing data on each variable. The lowest amount of missing data in these metric variables was 0 cases for CHOI1 (Item 1 for the construct choice), MEAN1 (Item 1 for the construct meaning), MEAN2 (Item 2 for the construct meaning), PACT3 (Item 3 for the construct participation), SETA2 (Item 2 for the construct SETA), SETA3 (Item 3 for the construct SETA), SETA4 (Item 4 for the construct SETA), ACC1 (Item 1 for the construct access), and ACC2 (Item 2 for the construct access), and the highest was 1.7% (5 cases) for COMP2 (Item 2 for the construct competence). This shows that all the variables have low levels of missing data.

Table 0.3: Missing Data by Variables

Variable	N	Mean	Std. Deviation	Missing		Variable	N	Mean	Std. Deviation	Missing	
				Count	Percent					Count	Percent
ISPC1	289	6.24	1.128	1	0.3	SETA1	289	4.46	2.036	1	0.3
ISPC2	288	5.71	1.287	2	0.7	SETA2	290	3.36	2.081	0	0
ISPC3	288	5.48	1.412	2	0.7	SETA3	290	4.44	2.027	0	0
CHOI1	290	4.45	1.78	0	0	SETA4	290	4.75	1.97	0	0
CHOI2	288	4.24	1.761	2	0.7	SETA5	288	4.61	2.005	2	0.7
CHOI3	289	4.51	1.841	1	0.3	ACC1	290	4.49	1.832	0	0
MEAN1	290	5.09	1.759	0	0	ACC2	290	4.81	1.651	0	0
MEAN2	290	4.94	1.759	0	0	ACC3	289	5.03	1.582	1	0.3
MEAN3	286	4.98	1.694	4	1.4	PART1	289	3.99	1.983	1	0.3
COMP1	286	5.09	1.436	4	1.4	PART2	287	3.57	2.111	3	1
COMP2	285	5.08	1.347	5	1.7						
COMP3	287	4.79	1.461	3	1						
PACT1	289	4.69	1.791	1	0.3						
PACT2	289	4.31	1.933	1	0.3						
PACT3	290	4.44	1.968	0	0						

Note. ISPC = IS security policy compliance intentions; CHOI = Perceived choice; MEAN = Perceived meaning; COMP = Perceived competence; PACT = Perceived impact; SETA = IS security education, training and awareness; ACC = Access to IS security strategy and goals; PART = Participation in IS security decision-making.

Table 0.4 contains information regarding the amount of missing data per case. Based on the complete case approach (listwise deletion), 272 cases were identified as being valid. It was apparent that only one case has an excessive number of missing values (40%), making it likely to be a candidate for deletion. Nevertheless, the extent of missing data for another 17 cases was low (< 20%). Of these 17 cases, 13 cases were missing one data only. According to Little and Rubin (1987), excluding cases with missing data reduces the sample size and valuable information. This decrease can lead to reduced statistical power, overestimated variances, and wider confidence intervals (Allison, 2003). Hence, apart from conventional listwise deletion, an alternative missing data method was performed wherein only one case was deleted and the remaining 17 cases were imputed (replaced).

Table 0.4: Missing Data by Cases

Number of Missing Data per Case	Percentage of Missing Data per Case	Number of Cases	Percentage
0	0%	272	94
1	4%	13	4.5
2	8%	2	0.7
3	12%	1	0.3
4	16%	1	0.3
10	40%	1	0.3
	Total	290	100%

A decision to choose the alternative missing data method depends on the randomness of the missing data. Step 3 involves a procedure to determine whether the missing data are distributed randomly across the cases and variables. If the missing data pattern is missing completely at random (MCAR), all imputation methods for remedies are appropriate (Hair et al., 2010). However, if the missing data is missing at random (MAR), researchers can use a model-based approach to impute the missing data (Hair et al., 2010). The condition of MCAR was examined using Little's multivariate test (Little and Schenker, 1995). A MCAR missing data pattern is indicated by a non-significant statistical level ($p < .05$), showing that the observed pattern does not differ from the random pattern (i.e., null hypothesis). The results showed that the little's MCAR test had a significance level of .034, indicating a significant result. Thus, the null hypothesis was rejected and the missing data was deemed to be MAR. Based on this result, a model-based imputation method was selected as the alternative missing data method.

In step 4, the model-based imputation was performed based on the 289 cases. For this study, the expectation maximization (EM) algorithm method was used. The primary advantages of the EM algorithm are simplicity and ease of computing (Little and Rubin, 1987). According to Little and Rubin (1987), The EM algorithm formalizes a relatively old ad hoc idea for handling missing data: (1) replace missing values by estimated values, (2) estimate parameters, (3) re-

estimate the missing values assuming the new parameter estimates are correct, (4) re-estimate parameters, and so forth, iterating until convergence (p. 129). In other words, EM is an iterative method to find the best possible value for the parameters (means, standard deviations, or correlations), assuming the missing data were replaced. EM is readily available in the Missing Value Analysis (MVA) module in SPSS.

Sensitivity analyses were performed to compare the results of the listwise deletion (272 cases) and EM methods (289 cases). CFAs showed that the model with 289 cases (χ^2=484.45 (*df*=247, p <.05); RMSEA=.058; SRMR=.05; CFI=.94) fits the data slightly better than the model with 272 cases (χ^2=467.62 (*df*=247, p <.05); RMSEA=.065; SRMR=.07; CFI=.93). In no instances did the imputation method change the overall model fit considerably. Consequently, it was decided to leave all 289 observations in the analysis.

Examination of Univariate Normality and Outliers

A next data-screening step was completed, which involved assessing a multivariate normality. Kline (2011) purported that multivariate normality is an assumption of Maximum Likelihood Estimation (MLE). As this study is using AMOS for data analysis, where the structural model estimation was performed with MLE, the analysis is subject to the assumption of multivariate normality. The normality problem exists when the multivariate distribution of the observed variables has tails and/or peaks that differ from the normal distribution (Byrne, 2009). There are statistical tests to detect multivariate normality, such as Mardia's (1985) test, but there are some weaknesses (Klein, 2011). Fortunately, multivariate non-normality can be detected through inspection of univariate distributions (Klein, 2011).

Two tests are appropriate to determine the univariate normality, skewness and kurtosis. Data distributions with either highly skewed or with high kurtosis is indicative of non-normality,

which will have an effect on the estimation parameters and/or model specification (Hall and Wang, 2004). Variables with values of skew index (*SI*) > ±3 are seen as extremely skewed wherein the sign of the *SI* indicates the direction of the skew (Klein, 2011). Klein (2011) also suggested that variables with values of the kurtosis index (*KI*) > ±10 suggest a problem. Table 0.5 provides the results of skewness and kurtosis. By the rules of thumb mentioned above, no item exhibited significant skew or kurtosis.

Table 0.5: Assessment of Normality – Skew and Kurtosis

Variable	min	max	skew	kurtosis	Variable	min	max	skew	kurtosis
ISPC1	1	7	-1.893	4.142	PACT1	1	7	-0.48	-0.804
ISPC2	1	7	-1.114	1.046	PACT3	1	7	-0.34	-1.019
ISPC3	1	7	-1.127	1.105	PART1	1	7	-0.06	-1.23
CHOI1	1	7	-0.328	-0.775	PART2	1	7	0.22	-1.333
CHOI2	1	7	-0.283	-0.899	ACC1	1	7	-0.52	-0.779
CHOI3	1	7	-0.356	-0.912	ACC2	1	7	-0.66	-0.238
MEAN1	1	7	-0.767	-0.394	ACC3	1	7	-0.66	-0.359
MEAN2	1	7	-0.708	-0.374	SETA1	1	7	-0.36	-1.13
MEAN3	1	7	-0.703	-0.387	SETA2	1	7	0.37	-1.183
COMP1	1	7	-0.728	0.23	SETA3	1	7	-0.35	-1.135
COMP2	1	7	-0.708	0.462	SETA4	1	7	-0.52	-0.92
COMP3	1	7	-0.608	-0.073	SETA5	1	7	-0.43	-1.084

Note. ISPC = IS security policy compliance intentions; CHOI = Perceived choice; MEAN = Perceived meaning; COMP = Perceived competence; PACT = Perceived impact; SETA = IS security education, training and awareness; ACC = Access to IS security strategy and goals; PART = Participation in IS security decision-making.

The next step of data screening involved the identification of potential outliers. Multivariate outliers refer to data that do not fit the standard sets of correlations exhibited by the other data in the dataset. Although univariate outliers have an extreme score on single variable, multivariate outliers have extreme scores on more than one variable (Kline, 2011). Specifically, they are cases with extreme scores on two or more variables (Tabachnick and Fidell, 2001). Outliers can influence the analysis results by pulling the mean away from the median. To detect multivariate outliers in AMOS, a Mahalanobis d-squared (D^2) test can be performed. D^2

indicates the distance in standard deviation units between a set of scores (vectors) for an individual case and the means for all variables (centroid) (Kline, 2011). According to Kline (2011), a case with a very high D^2 and a low p-value (p <.05) may lead to a rejection of the null hypothesis that the case comes from the same population as the rest. This case is the most likely candidate to be considered outlier.

Table 0.6: Observations farthest from the centroid (Mahalanobis distance)

Observation number	Mahalanobis d-squared	p1
189	72.07	0
224	63.832	0
118	59.699	0
125	57.693	0
102	57.622	0
143	56.217	0
151	55.612	0
276	52.021	0.001
109	50.589	0.002
.	.	.
.	.	.
.	.	.
213	38.703	0.039
219	38.604	0.04
24	38.433	0.042
8	37.871	0.048
.	.	.
.	.	.
.	.	.
261	28.475	0.286
71	28.44	0.288
273	28.133	0.302
289	28.034	0.306

Table 0.6 provides the excerpt of D^2 for this study. The results showed that 43 cases have D^2 values with a p-value of less than .05, indicating that these cases could potentially be outliers. Casewise diagnostics during each regression procedure were completed using the SPSS software to identify whether the potential outliers are influential cases. Field (2009) suggested that standardized residuals with an absolute value greater than 3 are cause for concern for influential

case. Regression analyses were performed with and without these outliers to see the impact of the outliers on regression coefficients. In no instances did the removal of potential outliers exert undue influence over the parameters of the model. Consequently, it was decided to leave all potential outliers in the analysis leaving 289 cases.

Examination of Common Method Variance (CMV)

The final step of data screening involved an examination of CMV. Since only self-report data was collected, the possibility of CMV was present. Harman's one-factor test was conducted to assess whether CMV is present (Podsakoff and Organ, 1986). In conducting the Harman's single-factor test, all variables of IS security policy compliance intentions, competence, meaning, impact, choice, SETA, access, and participation related to IS security were entered into factor analysis using principal axis factoring with varimax rotation. Results showed the presence of six distinct factors with eigenvalues greater than 1.0 (see Table 0.7). These six factors together accounted for 70.3% of the total variance and the largest factor did not account for the majority of the variance (i.e., 32.0%), indicating that CMV should not pose a pervasive issue (Podsakoff et al., 2003).

Summary

This section described the respondents' and companies' profile, examined the possibilities of missing data, multivariate normality, outliers, and common method variance. As stated, an initial 290 usable cases were used to report the demographics. The data screening process identified one case with extreme missing data (40%), which was removed from the sample. The remaining missing data (<20% per case) were imputed using the EM model-based imputation method. The remaining 289 cases were tested for univariate normality and outliers. The results showed that the data was normally distributed. However, several cases were

identified as potential outliers, but none was excluded leaving 289 usable cases for hypothesis testing. 289 valid cases with seven IVs and 25 items indicate a very good case-to-variable ratio (i.e., 12:1). This ratio satisfies the suggested ratio of 10:1 for CFA (Fornell and Larcker, 1981).

Table 0.7: Harman's Factor Score

Factor	Initial Eigenvalues			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	8.02	32.08	32.08	3.648	14.592	14.592
2	3.477	13.907	45.987	2.87	11.48	26.072
3	1.912	7.647	53.634	2.762	11.047	37.119
4	1.694	6.775	60.409	2.165	8.66	45.779
5	1.314	5.255	65.664	2.045	8.181	53.961
6	1.158	4.63	70.294	1.916	7.664	61.624
7	0.939	3.756	74.05			
8	0.766	3.064	77.114			
9	0.658	2.632	79.747			
10	0.546	2.185	81.931			
11	0.515	2.06	83.991			
12	0.485	1.94	85.931			
13	0.463	1.853	87.784			
14	0.406	1.626	89.41			
15	0.365	1.46	90.869			
16	0.316	1.264	92.134			
17	0.301	1.204	93.338			
18	0.262	1.049	94.386			
19	0.262	1.048	95.434			
20	0.232	0.928	96.362			
21	0.207	0.828	97.19			
22	0.189	0.757	97.948			
23	0.183	0.734	98.681			
24	0.171	0.683	99.365			
25	0.159	0.635	100			

5.3 Measurement Model and Confirmatory Factor Analysis (CFA)

Anderson and Gerbing's (1988) two-step approach, in which the measurement model was assessed and improved prior to testing of the structural model, was used. This section describes the assessments of measurement model. The assessment seeks to provide empirical support for the hypothesized relationships. Hair et al. (2010) suggested two types of assessments, construct validity or CFA, and overall model fit. The following section reports the results of these assessments.

Construct validity

The aim of the construct validity analysis was to assess whether the measured variables (indicator items) related to a specific latent construct are really measuring the latent construct as theoretically predicted. To assess construct validity, Hair et al. (2010) suggested assessing the model's convergent validity and discriminant validity. Convergent validity was assessed by factor loadings and average variance extracted (AVE). At a minimum, all the factor loadings must be statistically significant ($p < .05$). A good rule of thumb is that the standardized loading estimates and the AVE should be .5 or higher (Hair et al., 2010). Table 0.8 reports the standardized loading estimates for the data. The lowest loading estimate obtained was .53, linking the latent variable Choice to the variable CHOI2. More importantly, none of loadings falls below the acceptable cut-off of .5, indicating that all items loaded significantly well to their respective latent construct.

Table 0.8: Factor loadings

	SETA	ACCESS	PART	IMPACT	COMPETENCE	MEANING	CHOICE	ISP COMPLIANCE INTENTION
SETA1	0.84							
SETA2	0.62							
SETA3	0.74							
SETA4	0.91							
SETA5	0.78							
ACC1		0.74						
ACC2		0.66						
ACC3		0.74						
PART1			0.81					
PART2			0.79					
PACT1				0.83				
PACT2				0.9				
PACT3				0.86				
COMP1					0.89			
COMP2					0.81			
COMP3					0.87			
MEAN1						0.88		
MEAN2						0.87		
MEAN3						0.89		
CHOI1							0.87	
CHOI2							0.53	
CHOI3							0.84	
ISPC1								0.61
ISPC2								0.85
ISPC3								0.69

Note. ISPC = IS security policy compliance intentions; CHOI = Perceived choice; MEAN = Perceived meaningful; COMP = Perceived competence; PACT = Perceived impact; SETA = IS security education, training and awareness; ACC = Access to IS security strategy and goals; PART = Participation in IS security decision-making.

Table 0.9 reports the means, standard deviations, Cronbach's alphas, AVEs, correlations, and the square root of AVEs of the latent constructs. AVEs were estimated to provide additional information for the convergent validity. An AVE of .5 or greater is considered acceptable (Hair et al., 2010). The AVE for the latent constructs competence, meaning, impact,

and choice, the dimensions of the psychological empowerment construct, were .73, .77, .74, and .58, respectively.

Similarly, the latent constructs IS security policy compliance intentions, SETA, Access, and Participation had AVE estimates of .52, .63, .51, and .64. The results confirm that the items of a specific construct measure the same construct. Further, the Cronbach's alpha values for all of the constructs were greater than .75. A Cronbach's alpha values of .7 or greater is considered acceptable (Gefen et al. 2000; Nunnally and Bernstein 1994). The results indicate that the responses are consistent across the items within a construct.

In addition, to confirm the discriminant validity of the constructs, the square root of the AVEs for each construct were compared to the correlations of the constructs with their latent variables (Fornell and Larcker, 1981). As reported in Table 0.9, the square root of the AVEs for all constructs, reported in the diagonal of the correlation matrix, were larger than the corresponding off-diagonal correlations. The off-diagonal scores are the correlations associated with that constructs. These results indicate that the latent constructs of this study have appropriate discriminant validity (Fornell and Larcker, 1981).

Table 0.9: Descriptive Statistics, Inter-correlations, and Internal Consistency

	Mean	SD	α	CR	AVE	1	2	3	4	5	6	7	8
1. ISPC	3.378	0.623	0.752	0.762	0.521	**0.722**							
2. SETA	4.416	1.502	0.881	0.870	0.631	0.502**	**0.794**						
3. Acess	3.842	1.005	0.756	0.758	0.512	0.595**	0.573**	**0.716**					
4. Participation	4.276	1.501	0.778	0.779	0.639	0.220**	0.286**	0.482**	**0.799**				
5. Impact	3.693	1.412	0.895	0.895	0.740	0.069	0.028	0.239**	0.638**	**0.860**			
6. Competence	4.930	1.224	0.889	0.891	0.732	0.541**	0.571**	0.514**	0.466**	0.182**	**0.855**		
7. Meaning	5.093	1.480	0.910	0.910	0.772	0.557**	0.381**	0.621**	0.523**	0.281**	0.622**	**0.878**	
8. Choice	4.207	1.432	0.781	0.798	0.579	0.211**	0.096*	0.154**	0.524**	0.366**	0.279**	0.271**	**0.761**

Note: N = 289. ISPC = IS security policy compliance intentions; Choice = Perceived choice; Meaning = Perceived meaningfulness; Competence = Perceived competence; Impact = Perceived impact; SETA = IS security education, training and awareness; Access = Access to IS security strategy and goals; Participation = Participation in IS security decision-making; Mean = Average; SD = Standard deviation; α = Cronbach's Alpha, CR = Composite reliability, and AVE = Average Variance Extracted. Values below the diagonal are correlation estimates among constructs and diagonal elements are square root AVE.
*p <.05, **p <.01 (2-tailed).

Table 0.9 also reports the correlations among the latent constructs. Most of the correlations are significant (p <.05), except the correlations between impact and IS security policy compliance intentions, and between choice and SETA. Interestingly, there was a significant positive correlation between SETA and participation in IS security decision-making (r =.29, p <.01). There were also strong positive correlations between SETA and access to IS security strategy and goals (r =.57, p <.01) as well as IS security strategy and goals, and participation in IS security decision-making (r =.48, p <.01). These large magnitude correlations are consistent with previous research that suggested that there should be strong relations between empowerment work practices (Spreitzer, 1996). In addition, there were large magnitude correlations between perceived meaning and competence (r =.62, p <.01) as well as perceived choice and competence (r =.37, p <.01). There were moderate relations between meaning and impact (r =.28, p <.01), competence and impact (r =.18, p <.05), choice and competence (r =.28, p <.01), as well as choice and meaning (r =.27, p <.01). These large to moderate magnitude correlations are consistent with previous research that suggested that there should be "strong relations" between dimensions of psychological empowerment, such as perceived meaning, competence, impact, and choice (Spreitzer, 1996).

Also of note, none of the significant correlations were too large (r > .80), indicating no issues of multicollinearity (Field, 2009). Still, variance inflation factors (VIF) were computed to assess the threat of multicollinearity. A VIF of more than 10.0 is an indication of a severe issue, and less than 4.0 is an indication of no issue of multicollinearity (Bowerman and O'Connell, 1990). As none of the VIF in this study exceeded 4.0, it can be concluded that multicollinearity was not a problematic issue. Together with the results of the assessment of reliability, as well as

convergent and discriminant validity, these results suggest the latent constructs and the overall model have validity. Thus, all items were retained for further analysis.

Assessment of the measurement model fit

Table 0.10 presents the values of the fit indices for the measurement model of this study. The overall measurement model fit was χ^2=484.45 (*df*=247, p <.001), SRMR=.063, RMSEA .058 with CI_{90}: (.05, 0.065), and CFI=.94. The results reported that the values of SRMR and RMSEA are less than the selected cut-off values of .08 (Hu and Bentley, 1999; Byrne, 2009; Kline, 2011) corresponds to an "acceptable" fit (McDonald and Ho, 2002). Further, the value of CFI is marginally lower than the cut-off of .95 (Hu and Bentley, 1999; Klein, 2011). However, many researchers use a cut-off value of .90 as acceptable fit (McDonald and Ho, 2002). Thus, overall, the results signify a reasonably good fit for the proposed measurement model.

Table 0.10: Fit Indices of the Proposed Measurement Model

	Chi-Square (χ^2) Statistic = 484.45 (*df* = 247, p < .001)		
	RMSEA	SRMR	CFI
Proposed Measurement Model	.058 CI_{90}(.05, 0.065)	0.063	.943

Note: RMSEA = Root mean square error of approximation; SRMR = Standardized root mean square residual; CFI = Comparative fit index; CI_{90} =90% Confidence interval. All results were computed by AMOS.

Model diagnostics, such as modification indices (MIs) were conducted to ensure that the measurement model was well specified. MIs refers to any possible relation that is not estimated in a model (Byrne, 2009). The purpose of MIs is to check for model fit. While the χ^2 statistic, SRMR, RMSEA, and CFI provide global fit assessments, MIs focus on fit in various part of the model separately, and, thus, local fit. A model could have a reasonable fit, but it may contain severe misspecifications on one specific parameter. Overall fit assessments are based on specific free parameters and constrained parameters. The free parameter means that the parameter is

estimated, whereas constrained parameters are fixed at a certain value. For example, referring to the factor loadings in Table 0.8, the variable ACC1 has a loading on the construct Access, but not on the construct SETA. This indicates that the loading of the variable ACC1 on the construct SETA is fixed to 0 whereas the loading between the variable ACC1 and the construct Access is estimated. AMOS calculates a MIs for the possible loading of the variable ACC1 to other constructs (e.g., SETA). MIs indicate how much the χ^2 value of a model would drop if the parameter is freed instead of constrained. In other words, MIs indicate by how much the model fit could improve if a variable (i.e., ACC1) is allowed to load to another construct (i.e., SETA). If an MI shows a value higher than 20, it indicates that the respective fixed parameter is 'wrong' and should be considered a serious misfit (Byrne, 2009). MIs for the factor loadings (see Table 0.11) were all below 20, indicating no serious impact on model fit (Byrne, 2009). Thus, no modification was made.

Table 0.11: Modification Indices

Loading			M.I	Loading			M.I
PACT1	<---	MEANING	11.99	**COMP2**	<---	CHOICE	4.907
PACT1	<---	COMPETENCE	6.411	**PACT3**	<---	MEANING	4.115
PACT1	<---	ACCESS	7.203	**PACT3**	<---	ISP COMPLIANCE	6.385
PACT1	<---	SETA	4.074	**ACC1**	<---	SETA	7.987
PACT1	<---	ISP COMPLIANCE	15.95	**ACC1**	<---	SETA2	5.16
ISPC3	<---	COMPETENCE	4.288	**ACC2**	<---	SETA	4.343
CHOI1	<---	ACCESS	5.956	**ACC3**	<---	CHOICE	4.384
CHOI1	<---	ISP COMPLIANCE	8.158	**SETA2**	<---	CHOICE	17.25
CHOI2	<---	COMPETENCE	5.988	**SETA2**	<---	PART	18.04
CHOI3	<---	MEANING	4.151	**SETA2**	<---	ISP COMPLIANCE	5.15
CHOI3	<---	COMPETENCE	9.962	**SETA2**	<---	PART2	4.208
PACT1	<---	MEANING	6.303	**SETA3**	<---	MEANING	5.209
PACT1	<---	COMPETENCE	6.079	**SETA4**	<---	PART	6.231
CHOI3	<---	ISP COMPLIANCE	8.228	**SETA5**	<---	CHOICE	4.606

Note. ISPC = ISP compliance intentions; CHOI = Perceived choice; MEAN = Perceived meaningful; COMP = Perceived competence; PACT = Perceived impact; SETA = IS security education, training and awareness; ACC = Access to IS security strategy and goals; PART = Participation in IS security decision-making.

Overall results of the measurement model

In summary, the fit assessments generally supported the proposed measurement model. In the measurement validation process, the model showed convergent validity and discriminant validity. The measured items had significant loadings with their respective latent constructs. The AVEs for all the constructs were higher than the minimum threshold of .5 (Hair et al., 2010). The square root of the AVEs for each construct were higher than the correlations of the constructs with their latent variables. Further, the fit indices indicated that the measurement model achieved a fairly satisfactory level of fit (χ^2=484.45 (*df*=247, p <.001), SRMR=.063, RMSEA .058, and CFI=.94). Both the RMSEA and SRMR were below the recommended cut-off values of .08, and the CFI was slightly below the cut-off value of .95. Furthermore, the MIs showed no issue of misfit. Thus, it can be concluded that the proposed measurement model was well specified.

5.4 Assessment of Structural Model

After assessing the measurement model, the second step of Anderson and Gerbing's two-step approach is to evaluate the appropriateness of the proposed structural model (Anderson and Gerbing, 1988). A structural model is a composite of a measurement model and a path model (Mcdonald and Ho, 1992).

Structural Model Fit

Structural model validity is assessed by comparing the estimated covariance matrix with the observed covariance matrix. A structural model cannot fit any better (e.g., lower χ^2) than the measurement model because the structural model cannot have more relations between constructs than the measurement model (Hair et al., 2010). The measurement model assumes that a relation exists between each pair of constructs whereas the structural model relations are simpler. That means, the measurement model is a "larger" model with more freely estimated parameters, and

the structural model is a "smaller" model with fewer parameters freely estimated, and that the structural model is nested in the measurement model (Anderson and Gerbing, 1988). Therefore, measurement model fit provides a baseline to assess structural model fit. The fit indices of the proposed structural model are presented in Table 0.12.

Table 0.12: Proposed Structural Model Fit Indices

	Overall Model Fit		
Fit Measures	RMSEA	SRMR	CFI
Proposed Structural Model Fit	.068 CI_{90}(.61, .075)	.09	.92
χ^2 (df) of the Proposed Structural Model	608.55 (263) ($p < .001$)		
χ^2 (df) of the Measurement Model	484 (247) ($p < .001$)		

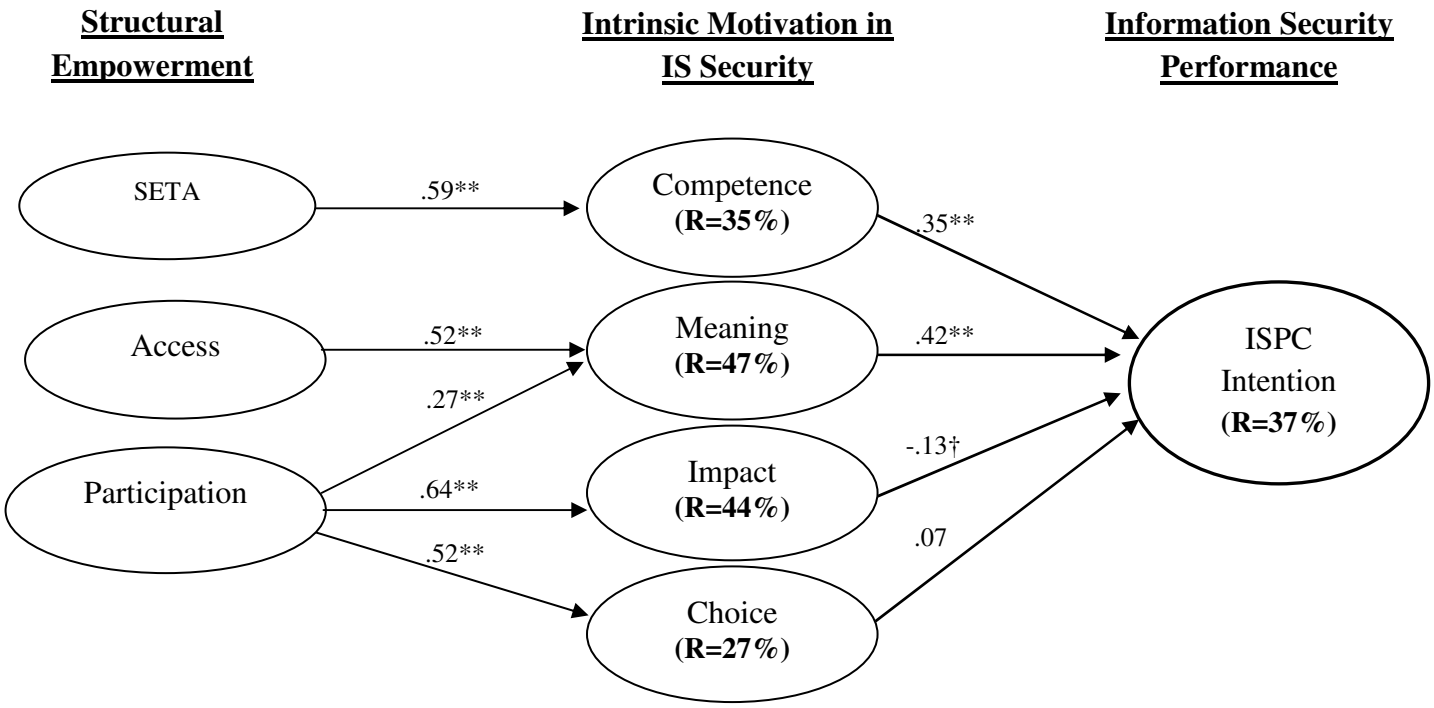
Note: df = degree of freedom; RMSEA = Root mean square error of approximation; SRMR = Standardized root mean square residual; CFI = Comparative fit index; CI_{90} =90% Confidence interval. All results were computed with AMOS.

The structural model fit was χ^2=608.55 (*df* =263, p <.001), SRMR=.09, RMSEA=.068 with CI_{90}: (.061, .075), and CFI = .92. The RMSEA was lower than the cut-off value of .08, the SRMR was slightly above the cut-off value of .08, and the CFI was lower than the cut-off value of .95, but still acceptable at the cut-off value of .90. The fit indices indicated that the structural model achieved a fairly satisfactory level of fit. The proposed structural model is shown in Figure 5.1 with the estimated regression coefficients of the paths (β) and their *p*-value.

Also of important note, the structural model was a composite of a measurement model and path model (Mcdonald and Ho, 1992). Therefore, it might be useful to decompose the measure of fit into measurement and path models (Mcdonald and Ho, 1992; Williams and O'Boyle, 2010; O'Boyle and Williams, 2011). Mcdonald and Ho (1992) purported that if a composite model has an unacceptable fit, it is important to know if the misfit is contributed by the measurement model, path model or both. Thus, global fit indices produced by a composite

model may yield misleading conclusions about the adequacy of a path model (Williams and O'Boyle, 2010). Mcdonald and Ho (1992) revised the formula for the RMSEA that focuses on path model. O'Boyle and Williams (2010) have referred to this RMSEA as RMSEA-P. The RMSEA-P for the proposed structural was .15, slightly higher than the cut-off of .10 (Brown and Cudeck, 1993). The results indicate that the path model had a poor fit.

Figure 0.1: Results of the Proposed Structural Model



Note: † p <0.1; * p <.05; ** p <0.01 (two-tailed tests); ISPC = ISP compliance intentions; SETA = IS security education, training and awareness; ACC = Access to IS security strategy and goals; PART = Participation in IS security decision-making. **The full SEM model is shown in Appendix-Figure 9.3.**

Hypothesis Testing

Good fit alone is not sufficient to support the validity of the structural model (Hair et al., 2010). Assessment of the validity of the structural model must include an examination of the individual structural parameter estimates against the corresponding hypotheses. A researcher

needs to investigate the extent to which the parameter estimates are statistically significant and in the predicted direction (Hair et al., 2010). In addition, variance-explained estimate, or R^2 for the relations between the predictor variables and the outcome variable should also be reported.

The validity of the structural model were assessed based on the standardized estimated path coefficient (β) along with the critical ratio (CR) and the p-value, as shown in Table 5.13. The standard decision rules ($CR \geq 1.96$ and $p \leq .05$) were applied to determine the significance of all path coefficients (Byrne, 2009). In addition, Figure 5.1 displays the path model with the standardized estimated path coefficients (β), the significance levels, and the explanatory power or variance explained (R^2).

The effect of the dimensions of psychological empowerment on IS security policy compliance intentions (Hypothesis 1 – 4)

Hypothesis 1 stated that perceived competence of IS security tasks positively relate to IS security policy compliance intentions. Table 0.13 shows that perceived competence was positively related to IS security policy compliance intentions (β=.35, p <.01). The finding supports Hypothesis 1. This result suggests that a high degree of competence of IS security tasks tends to increase one's intentions to comply with organizational IS security policy.

Hypothesis 2 stated that perceived meaningfulness of IS security positively relates to IS security policy compliance intentions Table 0.13 shows that the path coefficient was significant (β=.42, p <.01), providing a support for this hypothesis. This indicates that the higher the degree of perceived meaningfulness of the IS security tasks, the greater the intention to comply with the required tasks. In other words, if one perceives that IS security tasks are meaningful and important, it motivates him/her to comply with organizational IS security policy. Thus, Hypothesis 2 was supported.

Table 0.13: Hypothesized Path Relations for Proposed Structural Model

	Hypothesis	Proposed Structural Model				Results*
		Standardized Parameter Estimate	S.E	C.R. (t)	p	
H_1	Perceived competence of IS security task positively affects one's intention to comply with the IS security policies.	0.35	0.04	8.97	.000	Supported
H_2	Perceived meaningfulness of IS security task positively affects one's intention to comply with the IS security policies.	0.42	0.04	12.00	.000	Supported
H_3	Perceived impact of IS security task positively affects one's intention to comply with the IS security policies.	-0.13	0.03	-4.19	.051	Not supported
H_4	Perceived choice of IS security task positively affects one's intention to comply with the IS security policies.	0.07	0.03	2.41	.332	Not supported
H_5	SETA programs are positively associated with one's perceived competence of IS security task.	0.59	0.06	9.37	.000	Supported
H_6	Access to the organizational IS security strategy and goals is positively associated with one's perceived meaningfulness of IS security task.	0.52	0.1	5.25	.000	Supported
H_7	Participation in IS security decision making is positively associated with one's perceived meaningfulness of IS security task.	0.27	0.12	2.31	.000	Supported
H_8	Participation in IS security decision making is positively associated with one's perceived impact of IS security task.	0.64	0.07	9.85	.003	Supported
H_9	Participation in IS security decision making is positively associated with one's perceived freedom of IS security task.	0.52	0.06	8.13	.000	Supported

Note: † p <0.1; * p <.05; ** p <0.01 (two-tailed tests); S.E = Standard Error; CR = Critical Ratio

Hypothesis 3 suggested that perceived impact of IS security positively relates to IS security policy compliance intentions. Table 0.13 shows that perceived impact was negatively related to IS security policy compliance intentions at a marginal level of significance (β=-.13, p <.1). Thus, Hypothesis 3 was not supported.

Hypothesis 4 stated that perceived choice in IS security positively relate to IS security policy compliance intentions. Unlike competence and meaning, the result in Table 0.13 showed that perceived choice did not predict IS security policy compliance intentions (β=.07, p >.1). As a result, there was no evidence that choice or self-determination predicted IS security policy compliance intentions. Therefore, Hypothesis 4 was not supported.

The R^2 for intentions to comply with IS security policy is .37, indicating that 37% of the variance of the intentions to comply can be explained by these four dimensions of psychological empowerment. This suggests that feelings of empowerment do have a significant influence on IS security policy compliance intentions.

The effect of elements of structural empowerment (Hypothesis 5 – 9)

Hypothesis 5 stated that SETA positively relates to psychological empowerment, specifically perceived competence. Table 0.13 shows that SETA was positively related to perceived competence (β=.59, p <.01). Therefore, Hypothesis 5 was supported. The R^2 for perceptions of competence was .35, indicating that the variance of competence explained by SETA is 35%.

Hypothesis 6 stated that access to IS security strategy and goals positively relates to perceived meaning. The result (see Table 0.13) shows that access to IS security strategy and goals predicted meaning (β=.52, p <.01). Further, Hypothesis 7 stated that participation IS security decision-making is associated with perceptions of meaning. The results indicate that

participation in IS security decision-making is related to perceptions of meaning (β=.27, p <.01). Therefore, Hypotheses 6 and 7 were supported. Both access to IS security strategy and goals, and participation in IS security decision-making explained 47% the variance of meaning.

Hypothesis 8 and 9 stated that participation in IS security decision-making predicts impact and choice, respectively. The results (see Table 0.13) show that participation in IS security decision-making predicts perceptions of impact (β=.64, p <.01) and perceptions of choice (β=.52, p <.01). Both Hypotheses 8 and 9 were supported. The R^2 for perceptions of impact and choice are .44 and .27 respectively.

In sum, two of four dimensions of psychological empowerment (i.e., perceived competence and meaning) did predict IS security policy compliance intentions. However, contrary to the predictions, perceived impact negatively related to IS security policy compliance intentions and perceived choice did not predict employee's intentions to comply with IS security policy. Additionally, all structural empowerment facets related to the dimensions of psychological empowerment, as hypothesized. SETA positively related to perceived competence, access to IS security strategy and goals was related to perceived meaning and impact, and participation in IS security decision-making predicted perceived meaning, impact, and choice.

Results for the mediating effects (Hypothesis 10 – 12)

Table 0.14 displays the five hypotheses for mediating effects. Hypothesis 10 predicted that SETA was related to IS security policy compliance intentions via competence. The indirect effect (β_{IND}) was .1285 (*SE*=.0222). Using the Sobel test, the indirect effect of SETA was statistically significant (z=5.788, *SE*=.0222, p <.01). Also, the bootstrap analysis supported the conclusion of mediation (the 95% bias-corrected confidence interval for the total indirect effect excluded zero ([.0901, .1764]) (Preacher and Hayes, 2008). Thus, perceptions of competence did

mediate the relations between SETA and IS security policy compliance intentions, providing support for Hypothesis 10.

Hypothesis 11 stated the effect from access to IS security strategy and goals to IS security policy compliance intentions will be mediated by perceptions of meaning. Notably, the indirect effect (β_{IND}) was .1865 (*SE*=.0344). The results of the Sobel test (z=5.422, *SE*=.0344, p <.01), and the bootstrap analysis (the 95% bias-corrected confidence interval for the total indirect effect excluded zero ([.1217, .2567])) support a conclusion of mediation. As a result, the findings indicated that the perceptions of meaning mediated the relations between access to IS security strategy and goals, and IS security policy compliance intentions. Hypothesis 11 was thus supported.

Hypothesis 12a through 12c proposed that three dimensions of psychological empowerment (i.e., perceptions of meaning, impact, and choice) act as mediators of the relations between participation in IS security decision-making and IS security policy compliance intentions. As shown in Table 0.14, the indirect effect (β_{IND}) through meaning was .1684 (*SE*=.0204). The Sobel test suggested that the indirect effect is statistically significant (z=8.255, *SE*=.0204, p <.01). The bootstrap analysis supported the conclusion of mediation as well. The results show that the 95% bias-corrected confidence interval for the total indirect effect excluded zero ([.1324, .2122]). Thus, the results suggest that perceptions of meaning mediated the relations between participation in IS security decision-making and IS security policy compliance intentions. Thus, Hypothesis 12a was supported.

The indirect effect (β_{IND}) from participation in IS security decision-making process to the perceived impact to IS security policy compliance intentions was -.0879 (*SE*=.078). The results of the Sobel test (z=-1.127, *SE*=.078, p >.1) and the bootstrap analysis (the 95% bias-corrected

confidence interval for the total indirect effect included zero ([-.142, .043])) fail to support hypothesis 12b. Thus, perceived impact did not mediate the relation between participation in IS security decision-making and IS security policy compliance intentions.

Hypothesis 12c was not supported too. Notably, the indirect effect (β_{IND}) was .0128 (*SE* = .0189). The Sobel test indicated that the indirect effect of participation in IS security decision-making via choice was not statistically significant (z=.0677, *SE*=.0189, p >.05). The bootstrap analysis did not supported a conclusion of mediation as well (the 95% bias-corrected confidence interval for the total indirect effect included zero ([-.023, .0621]). This results suggest that perceptions of choice do not mediated the relations between participation in IS security decision-making and IS security policy compliance intention.

In sum, perceived competence served as mediating variable between SETA and IS security policy compliance intentions. As hypothesized, perceptions of meaning was an important mediator of the relations between access to IS security strategy and goals and IS security policy compliance intentions (i.e., Hypothesis 11), and participation in IS security decision-making and IS security policy compliance intentions (i.e., Hypothesis 12a). However, perceived impact and choice do not mediate the relations between participation in IS security decision-making and IS security policy compliance intentions. Overall, there was empirical support for Hypotheses 10, 11, and 12a, but not for 12b and 12c.

Table 0.14: Mediation of the SETA, Access and Participation of Employees on Intentions to Comply with IS security policy through Employees' Perception of Competence, Meaning, Impact, and Choice

.

	Hypothesis	Specific Indirect Effect	Point Estimate (β_{IND})	Product of Coefficent			Bootstrapping BC 95% CI	
				SE	Z	p	Lower	Upper
H_{10}	The effect of SETA on one's intention to comply with IS security policies is mediated by perceived competence of IS security task.	SETA --> Competence --> ISPC	0.1285	0.0222	5.788	.000	0.09	0.1764
H_{11}	The effect of access to IS security strategy and goals on one's intention to comply with IS security policies is mediated by perceived meaningfulness of IS security task.	ACCESS --> Meaning --> ISPC	0.1865	0.0344	5.422	.000	0.122	0.2567
H_{12a}	The effect of participation in IS security decision making on one's intention to comply with IS security policies is mediated by perceived meaningfulness of IS security task.	PART --> Meaning --> ISPC	0.1684	0.0204	8.255	.000	0.132	0.2122
H_{12b}	The effect of participation in IS security decision making on one's intention to comply with IS security policies is mediated by perceived impact of IS security task.	PART --> Impact --> ISPC	-0.0879	0.078	-1.127	.130	-0.1421	0.0431
H_{12c}	The effect of participation in IS security decision making on one's intention to comply with IS security policies is mediated by perceived choice of IS security task.	PART --> Choice --> ISPC	0.0128	0.0189	0.677	.499	-0.0229	0.0521

Note: = ISPC = IS security policy compliance intentions; SETA = IS security education, training and awareness; ACC = Access to IS security strategy and goals; PART = Participation in IS security decision-making; BC = bias corrected; 5,000 bootstrap samples.

5.5 Supplementary Analyses

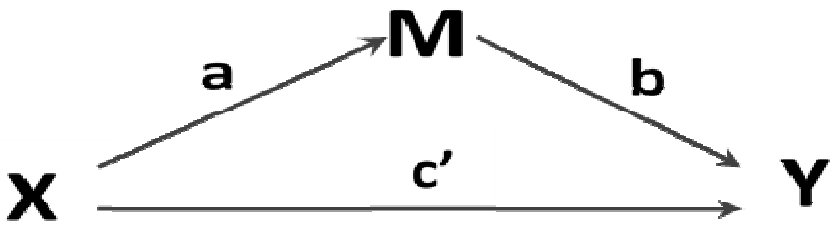
Testing for types of mediating effect

The reported results showed that feelings of meaning and competence can act as mediators in the relations between structural empowerment facets and IS security policy compliance intentions. Although no prediction was made as to whether the mediation role of perceptions of meaning and competence in the model are partial or full mediation, further analysis we made using the method suggested by Kenny and Baron (1986). Following Baron and Kenny, 'path c' is the coefficient for each independent variable (i.e., SETA, Access, and Participation) to the dependent variable (i.e., IS security policy compliance) without the mediator (see Figure 5.2 [a]). 'Path c'' is the coefficient of the link between independent variable and dependent variable when the mediator is in the model (see Figure 5.2[b]). If 'path c'' is significant and smaller than 'path c', this suggests partial mediation. If 'path c'' becomes statistically insignificant and close to zero, it suggests a full mediation.

Figure 0.2: Mediating Effect

(a)

(b)



The results of mediation are presented in Table 0.15. The results indicate that competence partially mediated the effects of SETA on intentions to comply with IS security policy. Perceptions of meaning fully mediated the effects of participation in IS security decision-making on intentions to comply with IS security policy, and it partially mediated the effects of access to IS security goals on intentions to comply with IS security policy.

Table 0.15: Results of mediating analysis

	Mediator: Meaning		Mediator: Competence
	IV: Access	IV: Participation	IV: SETA
Path c	.3777**	.1424**	.2198**
Path c'	.1900**	-.0259	.0913**
	Partial Mediation	**Full Mediation**	**Partial Mediation**

Note: † p <0.1; * p <.05; ** p <0.01 (two-tailed tests); IV = Independent variable

Testing for potential moderating effect

In addition, although not directly hypothesized, an assessment of the moderating effects of access to IS security strategy and goals, and participation in IS security decision-making on perceived meaning, was considered important. Moderation is the effect of a third variable that changes the magnitude or direction of the relations between two other variables (MacKinnon et al., 2012). An interaction term was calculated using mean-centered variables of access to IS security strategy and goals, and participation in IS security decision-making. As shown in Table 0.16 perceived meaning was not predicted by the access-participation interaction (β =-0.032, p >.05). Hence, the possibility of interaction effects was not supported.

Table 0.16: Interacting participation and access on perceptions of meaning

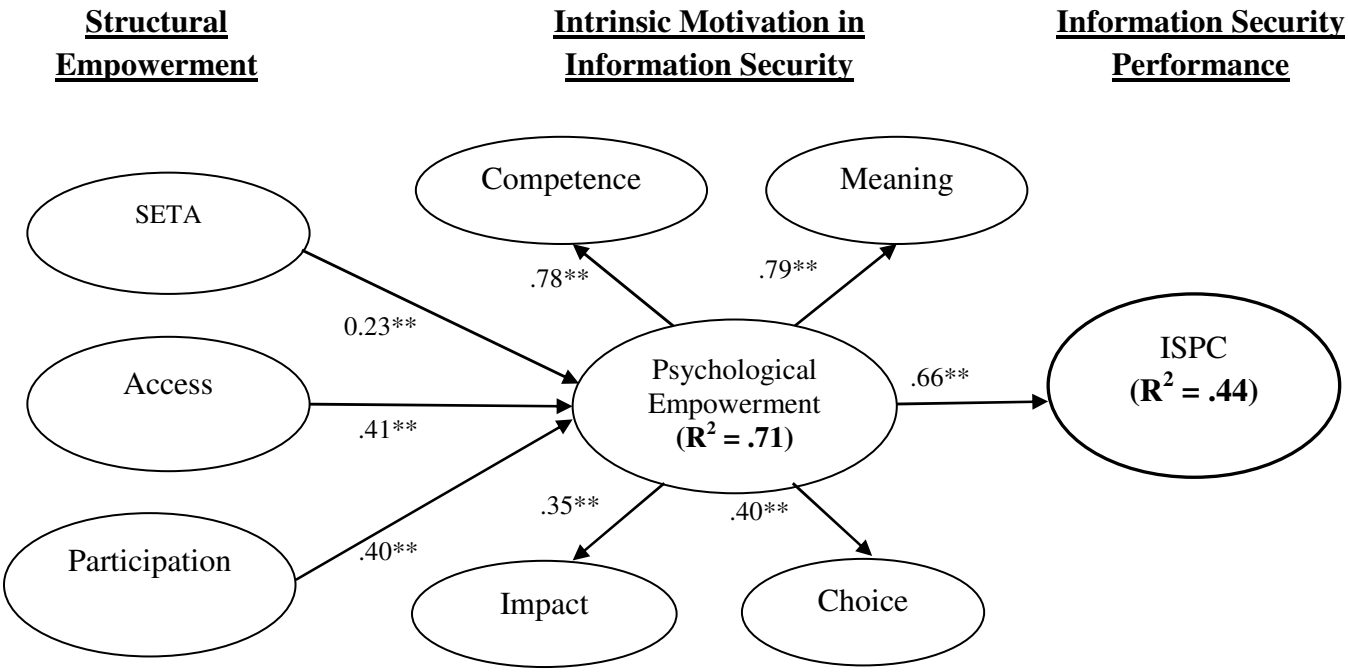
Regression			Standardized Parameter Estimate	S.E.	C.R.	P
Meaning	<---	PART	0.258	0.047	5.498	**
Meaning	<---	ACCESS	0.577	0.048	12.103	**
Meaning	<---	Access_X_Part	-0.032	0.039	-0.825	0.409
ISPC	<---	Meaning	0.64	0.045	14.142	**

Note: = ISPC = IS security policy compliance intentions; ACCESS = Access to IS security strategy and goals; PART = Participation in IS security decision-making.
† p <0.1; * p <.05; ** p <0.01 (two-tailed tests); S.E = Standard Error; CR = Critical Ratio

Testing for second-order construct of psychological empowerment

Finally, to further investigate the notion that empowerment has an overall positive effect on IS security performance, a post hoc test was conducted by introducing psychological empowerment as a second-order construct. The second-order construct of empowerment was treated as a reflective construct with the measures of the latent variable scores of its four dimensions (i.e., competence, meaning, impact, and choice). Figure 5.3 summarizes the empirical model as analyzed with AMOS 18. The R^2 for IS security policy compliance was .44 and the R^2 for psychological empowerment was .77. In addition, all the paths were significant at the level of p <.001. This indicates that psychological empowerment as a single, global construct has a positive effect on IS security behavior, and is strongly predicted by structural empowerment facets.

Figure 0.3: Structural model with empowerment as a second-order construct



Note: ISPC = IS security policy compliance intentions; SETA = IS security education, training and awareness; ACC = Access to IS security strategy and goals; PART = Participation in IS security decision-making. R^2 = variance explained.
† p <0.1; * p <.05; ** p <0.01 (two-tailed tests);

5.6 Summary

This chapter reported the analysis and the results of the proposed research model. The chapter started with a description of the data screening processes where 289 cases were identified valid. The 289 valid cases with seven IVs and 25 items indicate a very good case-to-variable ratio (i.e., 12:1). This ratio satisfies the suggested ratio of 10:1 for CFA (Fornell and Larcker, 1981). The CFA indicated that the proposed measurement model was well specified. Following the CFA, the assessment of the validity of the structural model was performed. It was discovered that the proposed structural model was marginally fit. Four of the 14 hypotheses were not supported. Hypotheses 1, 2, 5, 6, 7, 8, 9, 10, 11, and 12a were supported, and Hypotheses 3, 4, 12b, and 12c were not supported. The next chapter provides a discussion of the results.

Chapter 6. Discussion

6.1 Introduction

The aim of this chapter is to provide an overall synthesis of the research findings and a discussion of implications. A discussion of the implication focuses on the contribution of the research to the IS security field; that is, whether the results confirm previous work or not. This demonstrates the entire research agenda reflected in the dissertation.

This chapter is organized into three sections. After the introduction, the three research questions discussed in Chapter 1 are re-examined. The third section examines the main findings of the research and discusses whether they confirm previous studies or break new ground, and discusses the strengths and weaknesses of the study.

6.2 Reexamination of the research questions

Studies of the relations between extrinsic or controlled motivation of individuals and their IS security behaviors have a long and rich tradition. Earlier work in this vein has shown that sanctions, rewards, and social pressures, predict IS security policy compliance (Straub, 1990; Chan et al., 2005; Bulgurcu et al., 2010; Boss et al., 2009; Herath and Rao, 2009a). However, other studies reported that intrinsic factors could also motivate IS security behavior (Herath and Rao, 2009a, 2009b; Son, 2011). In his study, Son (2011) found that intrinsic motivation—perceptions of legitimacy and value congruence—are more likely than any set of extrinsic motivational factors to encourage compliance with IS security policy. However, the IS security literature has paid far less attention to intrinsic motivational factors when compared to extrinsic

motivational factors. Consequently, calls were made to study the effect of intrinsic motivational factors on IS security policy compliance (Padayachee, 2012; Herath and Rao, 2009a).

Responding to the call, and drawing upon Thomas and Velthouse's (1990) intrinsic motivation model, this dissertation used psychological empowerment as the intrinsic motivational factor. The model purported that psychological empowerment is a manifestation of four cognitions derived from a specific task—competence, meaning, impact, and choice. That is, employees are likely to feel empowered if they perceive that they have the capability to perform the task activities skillfully and successfully, perceive that the value of the task is consistent with their personal beliefs, perceive that they can make a significant difference or contribute to the organization if they execute the task, and finally, perceive that they feel in control to select tasks and perform in ways that seem appropriate.

Theory and prior studies have both argued that feelings of empowerment exert influence on individuals to put more effort towards the execution and performance of a task (Oldham and Hackman, 1980; Deci and Ryan, 1985; Thomas and Velthouse, 1990; Spreitzer et al., 1997; Kraimer et al., 1999; Liden et al., 2000). Although empirical studies found that these four dimensions are capturing the essence of psychological empowerment construct (Spreitzer, 1995a; Kraimer et al., 1999), researchers argued that it is also crucial to disentangle which psychological empowerment dimension actually associates with outcomes (Spreitzer et al., 1997; Kraimer et al., 1999; Maynard et al., 2012). In fact, studies have found that each dimension contributes to different outcomes (Spreitzer et al., 1997; Kraimer et al., 1999). Hence, this study responded to the gaps in the IS security literature by investigating the influences of each dimension of psychological empowerment on IS security compliance intentions.

The argument presented in the first chapter states that employees' intrinsic motivation may be driven by factors external to the employees (Thomas and Velthouse, 1990; Ryan and Deci, 2000). Prior studies in IS security compliance have suggested various external factors and strategies, such as providing training, improving the task design, enhancing the IS security climate, and so on, to drive employees' intrinsic motivation (Herath and Rao, 2009b; Bulgurcu et al., 2010; Son, 2011). However, rather than exploring the range of external factors empirically, most studies have simply acknowledged their importance. Thus, this current study was motivated to fill the gap. One way an organization can stimulate the feelings of empowerment among its employees is providing empowering work structures. This include the enhancement of their knowledge and skills through training and education related to the task, providing them access to information about the strategy and goal of the task, and involve them in decision-making processes related to their tasks (Spreitzer, 1995a; Wallach and Meuller, 2006; Hon and Rensvold, 2006; Lanschinger et al., 2004). Although most studies have 'bundled' these practices, Maynard et al. (2012) argued that it is difficult to determine which structural empowerment facets are actually related to the four dimensions of psychological empowerment. Therefore, this study has attempted to uncover the relations among the structural empowerment facets and the dimensions of psychological empowerment in the context of IS security.

The idea of psychological empowerment serving as mediator between structural empowerment and individual performance-related outcomes has been supported in numerous studies (Spreitzer, 2007; Maynard et al., 2012). Nielsen (1986) claimed that changing the organizational structural context is not enough to change individual behavior; ultimately, an individual feeling of empowerment is necessary to influence such behaviors (cf. Spreitzer, 1995b). Consistent with this line of argument, this study has replicated previous studies to

investigate the mediating role of psychological empowerment on the relations between elements of structural empowerment, and IS security policy compliance intentions.

In sum, the review presented above led to three specific research questions: What is the impact of the four dimensions of employees' psychological empowerment, on IS security policy compliance intentions? How do elements of structural empowerment, including SETA, access to information regarding IS security strategy and goals, and participation in IS security decision-making, enhance the dimensions of psychological empowerment with respect to IS security? Do the four dimensions of psychological empowerment mediate the relations between elements of structural empowerment and IS security policy compliance intentions? The following subsections discuss the findings and the implications.

Research Question 1

This study argued that employees' intrinsic motivation affects their IS security policy compliance intentions. Specifically, this study examined how employees' perceptions of empowerment (i.e., their perceptions of competence, meaning, impact, and choice) affect their intentions to display IS security compliance behavior. As Thomas and Velthouse's (1990) intrinsic motivation theory indicates, individuals who feel that their work or task is empowering, they are more motivated to expend more energy and work hard on the task (Thomas and Velthouse, 1990).

The findings of this study are mixed. In general, the results suggest that the feeling of empowerment, dominated by the perceptions of competence and meaning dimensions, has positive effects on IS security policy compliance intentions, as predicted in Hypothesis 1 and 2. However, Hypothesis 3 and 4, which predict that feelings of impact and choice relate to IS security compliance, were not supported. These results are agreed with findings by Liden et al.

(2000), who found that meaning and competence are strong predictors of work satisfaction, behavioral intentions, and job performance.

The results indicate that feelings of competence influence individuals' intentions to comply with the IS security policy. The significant effect of competence implies that employees who saw themselves as having the skills and capability to manage the IS security tasks have the intention to perform those tasks. Previous studies have found evidence that employees' belief in their competence in IS security influences their decision to perform (or not perform) IS security related activities, particularly those prescribed by the organizational IS security policies (Chan et al., 2005; Workman et al., 2008; Herath & Rao, 2009; Rhee et al., 2009). In fact, a meta-analysis by Stajkovic and Luthans (1996) concluded that the perceived competence influences task performance in various contexts.

Furthermore, the results suggest that feelings of meaning are related to IS security policy compliance intentions. The significant effect of meaning indicates that employees who felt that the IS security tasks are meaningful are motivated to put more effort to accomplish the goals of the IS security tasks. As Thomas and Velthouse's (1990) theory indicates, individuals are more likely to engage, do well, and put more energy into a task if the task activities are meaningful, serve an important purpose, and are in accordance with their own values and goals. This result is also consistent with previous studies showing that meaning is associated with numerous work-related benefits, such as courtesy behavior, work performance, higher commitment to work, and engagement at work (e.g., Liden et al., 2000; Wat and Shaffer, 2004; Wang and Lee, 2009; May et al., 2004). The result supports extant literature but not in IS security literature because perceptions of meaning derived from IS security tasks have never been studied in IS security research. Thus, this study contributes to the IS literature by concluding that employees tend to

intrinsically motivated to perform the IS security tasks and achieve IS security goals if they perceive that the IS security tasks are meaningful.

Contrary to expectations, perceptions of impact had a marginal significant negative relations with IS security policy compliance intentions. This indicates that the stronger individuals' feelings of impact of the IS security tasks, the lower their intentions to comply with IS security policy. This result is contrary to prior findings that found that impact is positively related to IS security behavior and other individual performance-related outcomes (Herath and Rao, 2009b; Seibert et al., 2011; Maynard et al., 2012). For instance, Herath and Rao (2009b) found that employees are found to adopt a favorable IS security compliance behaviors when they perceived that their IS security actions can benefit the organization. However, in the current study, the effect was only marginally significant.

In addition, the results of this study do not support the hypothesized relations between perceived choice or self-determination and IS security policy compliance intentions. This indicates that whether or not the employees feel that they can operate the IS security tasks autonomously, may not matter. Spreitzer et al. (1997) also reported this somewhat surprising result. Spreitzer et al. (1997) found that self-determination was only marginally related to the affective outcomes of work satisfaction but not to performance-related outcomes. Further, Liden et al. (2000) found that self-determination did not relate to either affective or performance outcomes.

Finally, as the post-hoc analysis results have indicated, psychological empowerment has an overall positive impact on employees' IS security policy compliance intentions. This provides support for the intrinsic motivation model (Thomas and Velthouse, 1990) and the contentions of intrinsic motivation studies in various domains (e.g., Spreitzer, 1995a; Laschinger et al., 2004;

Aryee and Chen, 2006). However, when the dimensions of psychological empowerment were detangled and tested individually, only two of the dimensions (i.e., perceptions of competence and meaning) predicted IS security policy compliance intentions. Although another two dimensions (i.e., perceptions of impact and choice) are not positively related to IS security policy compliance intentions, the results were not surprising because different dimensions of psychological empowerment may influence different outcomes (Spreitzer et al., 1997). The results of this study are also aligned with Kraimer et al.'s (1999) claim that perceived impact and choice may relate to affective outcomes, rather than behavioral intentions.

Research Question 2

This study argued that structural empowerment practices are associated with employees' psychological empowerment. More specifically, structural empowerment allows employees to obtain power in terms of opportunity for training, participation in decision-making, and access to information, which hence may influence the feelings that they are empowered (Spreitzer, 1996; Spreitzer, 2008; Seibert et al., 2011). The position of intrinsic motivation theorists is that although intrinsic motivation is an innate part of individuals and derived from a specific task, it must be prompted and enhanced by external factors (Oldham and Hackman, 1980; Deci and Ryan, 1985; Thomas and Velthouse, 1990). Therefore, external factors such as structural empowerment work practices is vital in enhancing employees' intrinsic motivation.

The results of this study also support for the relations between structural empowerment work practices and psychological empowerment, which is aligned with prior studies in various contexts (Spreitzer, 1996; Siu et al., 2005; Wallach and Mueller, 2006; Bordin et al., 2006). In other words, the obtained results suggest that different structural empowerment facets relate to different dimensions of psychological empowerment, consistent with prior studies (Spreitzer et

al., 1997; Liden et al., 2000). Specifically, this study found that IS security training, education, and awareness (SETA) are significantly related to the competence dimension of psychological empowerment (Hypothesis 5). This indicates that employees develop their competence or self-efficacy through the ongoing acquisition of knowledge regarding the IS security controls. As self-efficacy arguments indicate, self-efficacy beliefs are developed through an effective mastery experiences (Bandura, 1977). This is consistent with previous studies showing that perceived opportunity for training predicts perceptions of competence (Gist et al., 1989; Agarwal et al., 2000; Liao et al., 2009).

Next, access to information security strategy and goals are significantly related to meaning (Hypothesis 6). A meta-analytic by Seibert et al. (2011) concluded that information about strategy or operational goals allows employees to see the work as personally meaningful because they understand how their work fits into the goals and strategies. This indicates that access to information regarding IS security strategy and goals would allow employees to feel informed about where an organization is headed. Hence, they should know how their own IS security tasks contribute to achieving the IS security goals. That is, they acquire a greater sense that the IS security task is meaningful to be executed because they know that their IS security task is supporting the IS security objectives and benefit the organization at the end. This finding is apparently consistent with past findings reported by Spreitzer (1996) and Bordin et al. (2006).

Interestingly, the study found that participation in IS security decision-making led to enhanced feelings of three dimensions of psychological empowerment. This is consistent with results reported by Wallach and Muller (2006), who found that actual participation in decision-making pertinent to one's own work had a strong positive influence on the meaning and autonomy, and was marginally related to the impact and competence dimensions of

psychological empowerment. This indicates that participation in decision-making should enable employees to contribute their opinions in the decision related to the IS security task alongside their superiors. Thus, participation allows employees to feel that they have opportunity for freedom and independence for IS security task-related decisions. Further, when employees participate in the decision-making process, they may enjoy the opportunity to set the IS security decisions jointly with their superiors. This could make them feel that they are an important asset to the organization and that they can impact their work environment. While participating, employees have the opportunity to provide input that is consistent with their own values or needs, increasing the feeling that the IS security tasks are meaningful and important. Finally, their involvement with the decision-making process allows them to enhance the mastery experience of IS security, which should increases their feelings of competence.

In sum, all the hypothesized relations between the structural empowerment facets and the dimensions of psychological empowerment were supported. As expected, this study found that when employees were engaged in their work environment through empowerment work practices, such as opportunity for training, access to information, and participation in decision-making related to IS security, it is likely that employees felt more empowered in terms of their feelings competence, meaningfulness, impact, and choice. This supports the contention made in prior studies that different dimensions of empowerment are influenced by different antecedents (i.e., Spretizer et al., 1997; Kraimer et al., 1999).

Research Question 3

Finally, this dissertation explored how the dimensions of psychological empowerment mediate the relations between structural empowerment facets and IS security policy compliance intentions. This study provides evidence that structural empowerment facets are associated with

two of the dimensions of psychological empowerment—and that both in turn are related to IS security policy compliance intentions. The mediating effects that were uncovered involved the competence dimension of psychological empowerment in the relations between SETA and IS security policy compliance (hypothesis 10) and the meaning dimension of psychological empowerment in the relations between access to IS security strategy and goals and IS security policy compliance (hypothesis 11), as well as participation in IS security decision-making processes and IS security policy compliance (hypothesis 12a). However, the impact and choice dimensions of psychological empowerment did not mediate the relations between participation and IS security policy compliance (hypothesis 12b and 12c). These findings suggest that the structural empowerment practices characterized by SETA, access to IS security strategy and goals, and participation in IS security decision-making processes are important in influencing two psychological empowerment dimensions (i.e., competence and meaning), which should ultimately motivate employees to engage and expend more time and energy in IS security policy compliance. This finding provides support for Liden et al.'s (1990), who reported that meaning and competence mediated the relations between job characteristics and work satisfaction as well as commitment.

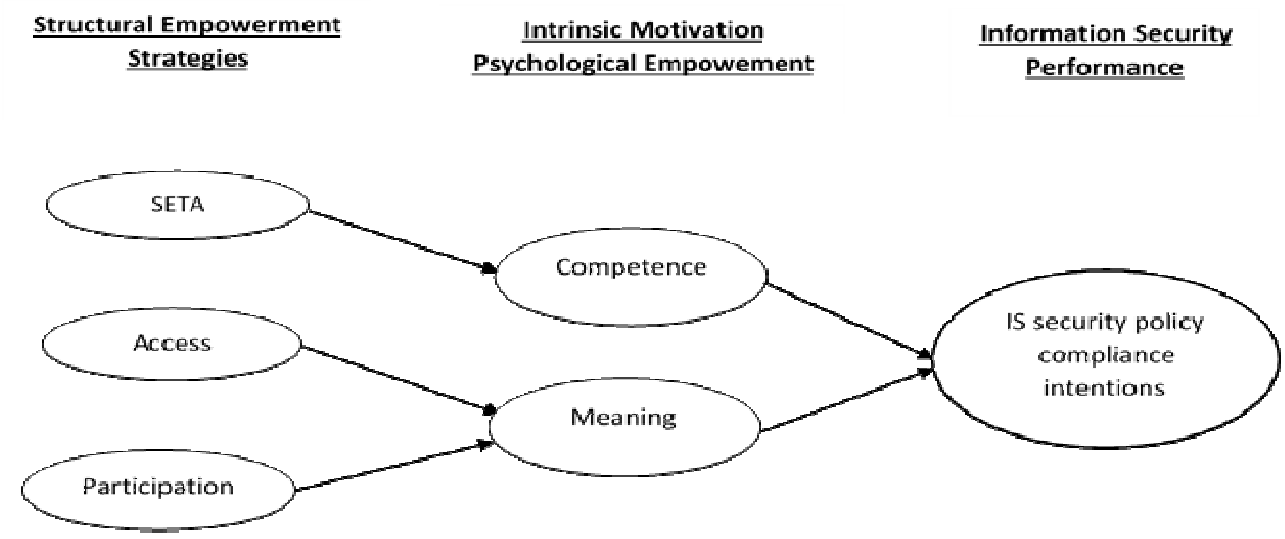
Finally, an ad hoc analysis was performed to determine whether the mediating role of perceptions of meaning and competence are partial or full mediation. The study found that meaning fully mediated the effects of participation in IS security decision-making on intention to comply with IS security policy. Competence was found to partially mediated the relations between SETA and intention to comply with IS security policy and meaning partially mediated the relations between access to IS security goals and IS security policy compliance intentions.

6.3 Summary

This study identifies four components of psychological empowerment - feelings of competence, meaning, impact, and choice - to provide theoretical explanations for the antecedents of the employees' intention to comply with IS security policy. Furthermore, the study postulates that structural empowerment facets, including SETA, access to IS security strategy and goals, and participation in IS security decision-making, may influence employees' compliance intentions indirectly through the dimensions of psychological empowerment. Overall, the study found support for the theoretical model. Based on the data collected from 289 respondents who were familiar with the IS security policy requirements, all but four of the hypotheses were supported. Figure 6.1 represents the IS security policy compliance model derived from this study.

A number of implications may be derived from the results. One of the more important implications follows from the indirect (full mediation via meaning) relations between participation in IS security decision-making and IS security policy compliance intentions. A complete understanding of employees' IS security behaviors in organizations requires the recognition of both intrinsic and external factors. Focusing only on providing structural empowerment (i.e. extrinsic factor) to the exclusion of psychological empowerment (i.e. intrinsic factor) provides an incomplete picture of IS security behaviors.

Figure 0.1: Current study IS security policy compliance model



Pyschological empowerment, dominated by the meaning and competence dimensions, had an overall positive impact on employee IS security policy compliance intentions. These results indicate that individual intention to execute IS security tasks (i.e., compliance with IS security policy) in the workplace are influenced by their perceptions of how the goals of IS security are meaningful and important to them, and by the degree of confidence in the skills and abilities they have about the IS security tasks. That is, individual perceptions about empowerment, specifically with regard to their perceived competence and meaning dimensions related to IS security tasks, plays vital role in affecting their IS security behaviors. These findings provide evidence of the importance of intrinsic motivational factors in influencing employee compliance behavior. This is clearly in line with IS security research findings that acknowledge the importance of intrinsic factors in the conduct of IS security behaviors (Herath and Rao, 2009b; Bulgurcu et al., 2010; Son, 2011).

The question that arises as a result of these observations is: what are the strategies to maximize employees intrinsic motivation, especially their feelings of empowerment related to IS security tasks? This study provides evidence that the psychological empowerment of employees

related to IS security tasks can be influenced by the structure in organizations that share power with their employees. The sharing of power is materialized in term of engaging employees in the IS security decision-making process, giving them more opportunities to access the IS security strategy and goals, and providing them with training and education programs related to IS security (SETA). Participation in IS security decision-making was found to positively relate to the three dimensions of psychological empowerment (i.e. meaning, impact, and choice), SETA and access to IS security strategy and goals were related to the competence and meaning dimensions of empowerment, respectively. Participation in IS security decision-making allows employees to contribute their inputs, ideas, and thoughts in the risk assessment, design, and implementation of IS security controls, hence increasing their feelings of empowerment. This result is particularly interesting in light of Dhillon et al.'s (2004) view that employees who were left out from all major decision-making and had no say on the latest developments related to IS security in the organization has been attributed to feelings of oppression. Providing SETA to all levels of employees in organizations gives them the opportunity to impart general knowledge of IS security environment, along with the skills necessary to perform the required IS security tasks. Finally, communicating the well specified IS security policy that consists of goals of IS security allows individuals to feel informed about where an organization is headed in the context of IS security. Thus, organizations attempting to foster empowerment should pay particular attention to give employees opportunities to participate in IS security decision-making, access to SETA and IS security strategy and goals.

An interesting feature of this study concerns the mediating effects of the competence and meaning, on the relations between the structural empowerment facets and the IS security policy compliance intentions. According to Nielsen (1986), changing the organization's structural

context is not enough to influence individual behavior; ultimately, an individual feelings of empowerment are necessary to influence such behavior (cf. Spreitzer, 1996). Consistent with this line of argument, this study suggests that the meaning and competence dimensions may play a mediating role with respect to IS security compliance behavior.

The mediating effects have an implication for the interpretation of many IS security studies that have tested the direct effects between work environment, such as participation, communication of the goals, and training, and IS security outcome while excluding the psychological state. The results of this dissertation indicate that SETA not only has a direct effect on IS security behavior shown in previous studies (e.g., D'Arcy et al., 2009) but also the indirect effect through feelings of competence. Similarly, studies that have examined the relations between participation and effective IS security (e.g., Spears and Barki, 2010) has not tested the mediating effects. The current study has found that the meaning dimension of psychological empowerment completely mediate the relations between participation in IS security decision-making and IS security compliance. Furthermore, Boss et al. (2009) identified that a well-specified IS policy that gives clear directions to achieve IS security goals, was related to precautionary behavior via perceptions of mandatoriness of IS security policy compliance. The present study provides similar results, but tested the mediating role of feelings of meaning in the relations between access to IS security strategy and goals and IS security policy compliance. Therefore, these findings indicate that focusing on extrinsic factors is not enough to truly understand the underlying reason of employee IS security policy compliance intentions.

However, the results did not support earlier prediction that employees feelings of impact and choice may influence their IS security policy compliance intentions. While the results did not support Thomas and Velthouse's (1990) intrinsic motivation model, this is not surprising.

Earlier studies found that different dimensions of psychological empowerment may have different strengths to influence different outcomes (Spreitzer et al., 1997; Kramier et al., 1999; Wat and Shaffer, 2005). For instance, Wat and Shaffer (2005) found that the meaning dimension relates to courtesy behavior, the competence dimension relates to consceintiousness and sportmanship behaviors, the impact dimension predicts consceintiousness, and the self-determination dimension relates to altruism. In fact, Kraimer et al. (1999) purported that the impact and self-determination dimensions are personal control that are expected to be related to affective outcomes, rather than behavioral outcomes.

In the context of this study, impact refers to an individual sense of control over the outcomes of the IS security tasks. One possible explanation for the negative relations between feelings of impact and IS security policy compliance intentions would be that, while employees perceived that they can impact their organizations if they perform the IS security tasks, the IS security tasks might be too complicated or too technical. Due to the complexity of the IS security tasks, they might think that the IT team or IT department will take care of it, and thus, feel that there is no need to put too much effort on the IS security tasks. As a result, their IS security policy compliance intentions is not as high as others are. Another, more likely, explanation is that the negative coefficient is statistical artifact. When the correlated independent variables are regressed simultaneously, the regression coefficients become unstable, manifested in the form of either reduced magnitude of effect size or change in direction (Pedhazur and Schmelkin cf. Wat and Shaffer, 2005). In this study, the bivariate correlation between feelings of impact and IS security compliance was not even significant (see Table 0.9. Note the positive, but not significant correlation between impact and IS security policy compliance). Thus, the relations between feelings of impact and IS security policy compliance merits further investigation.

Choice or self-determination refers to individuals sense of control of IS security tasks. The insignificant effect of self-determination on IS security policy compliance may indicate that having autonomy in IS security tasks is less important than having feelings of meaning and competence. One possible explanation might be the fact the IS security policy compliance is perceived as mandatory (Boss et al., 2009). Therefore, whether or not the employees may have a high degree of control over what IS security tasks to take and how to perform these IS security tasks, they may expend effort to comply with IS security policy. Also, while individuals may appreciate IS security task autonomy, the act of securing the information is considered as ‘part of

the job' hence individuals apply much effort in doing the IS security tasks regardless of their autonomy. Another possible explanation is that, as suggested by Kraimer et al. (1999) having a sense of control of IS security tasks may be more related to affective outcomes, such as emotional distress, job satisfaction, and role stress, rather than task effort and performance. From a methodological perspective, as explained in the previous paragraph, the insignificant findings may be due to a statistical artifact (see Table 5.9. Note the positive and the significant correlation between choice and IS security policy compliance [r = .211, p <.01]). Thus, the relations between perceived choice and IS security behavior requires further investigation.

Chapter 7. Conclusion

7.1 Introduction

This thesis has involved an empirical investigation of intrinsic motivation and IS security policy compliance intentions. This encapsulates theoretical reasoning from two theories. The central research question underpinning this thesis was: how does intrinsic motivational factor influence one's intention to comply with IS security policy? All relevant literature towards identifying and answering the research questions were consolidated in Chapter 2. Based on the review in Chapter 2, a conceptual model and the hypotheses were developed in Chapter 3. The quantitative research approach was suggested to investigate the expectations, was discussed in Chapter 4. The quantitative model was tested in Chapter 5, followed by the discussion of the results in Chapter 6. This chapter addresses the practical and theoretical implications of the dissertation. Finally, a discussion of the limitations of this dissertation and possible future research directions are discussed.

7.2 Contributions of the Study

The most important part of any study is the contribution it makes to a body of knowledge. This research makes several contributions cross the practical and theoretical realms. The following sections highlight the contributions of research as these relate to the IS security literature and beyond.

Theoretical Contributions

This research makes five major theoretical contributions. First, as far our review of the literature, this is perhaps the first study investigating effects of psychological empowerment derived from the assessment of IS security tasks. Such an investigation extends the use of Thomas and Velthouse's (1990) intrinsic motivation model. Differing from previous studies that examine the effects of extrinsic and/or intrinsic motivations (e.g., Straub, 1990; Bulgurcu et al., 2010; Boss et al., 2009; Herath and Rao, 2009a; Herath and Rao, 2009b; Son, 2011), the present study focuses on how the assessments of IS security tasks stimulate the feelings of competence, meaning, impact, and choice and thereby motivates individuals to expend effort to perform the IS security tasks. Such a focus allows us to increase our knowledge of IS security behavior motivations. The results support prior studies that employees may be intrinsically motivated to comply with IS security policy. Further, the dissertation used the variables from Kanter's (1977) structural empowerment theory, including training, access to information, and participation, as antecedents of the intrinsic motivation. Although the variables are not new in IS security literature, they are used in this study to predict psychological empowerment, and ultimately to influence IS security behavior, unlike other studies that used these variables to predict the direct association with IS security behavior (D'Arcy et al., 2009; Spears and Barki, 2010). **Hence, the results of this study are able to explain how structural empowerment can contribute to improve IS security behaviors, via psychological empowerment.**

Second, this study provides fresh empirical affirmation in the literature from a new context of investigation. The study investigated the relations between psychological empowerment and individual performance-related outcome on a very specific task (i.e., IS security tasks). The results imply that psychological empowerment, dominated by feelings of meaning and competence, shows relation with IS security policy compliance intentions. This

validates the extensive findings from different research settings for a very specific task and a new context, and helps with generalization.

Third, this study contributes to the empowerment literature by investigating the individual dimensions of psychological empowerment and structural empowerment facets, separately. This study provides in-depth considerations of the various facets of structural empowerment and the dimensions of psychological empowerment, which have not received due attention in the literature (Maynard et al., 2012). Prior studies often 'bundle' these dimensions. Hence, this study is able to explain which dimensions are actually driving the associations. Among those structural empowerment facets, participation in IS security decision-making is related to three dimensions of psychological empowerment (i.e, meaning, impact, and choice). SETA can only predict perceptions of competence, and access to IS security strategy and goals is related to the meaning dimension only. In terms of predicting IS security policy compliance intentions, only competence and meaning dimensions are the significant variables. These results further confirm prior studies that postulate different dimensions of psychological empowerment predict different outcomes and driven by different factors (Spreitzer et al., 1997).

Fourth, the study investigated the mediating role of psychological empowerment. The mediating effects that were uncovered involve the meaning and competence dimensions in the relations between structural empowerment facets and IS security compliance behavior. The results further enhance the current body of literature across a wide variety of studies that have confirmed the mediating role of psychological empowerment. More interestingly, this study contributes to the literature by explicitly testing the individual dimensions as a mediator. Only two dimensions of psychological empowerment were found to be the mediators.

Finally, the current study further validated the single 12-item measure of psychological empowerment developed by Spreitzer (1995a). What is more interesting is that the measures were slightly modified to fit into a very specific work task, but still both the convergent and discriminant validity were achieved. Not only that, this study has integrated two models of empowerment, structural (i.e., organizationally-centric) and psychological (i.e., individually-centric) to form a complete perspective of empowerment. Spreitzer (2007) posited that a thorough understanding of empowerment in the workplace requires the integration of both perspectives.

Practical Implications

The primary practical implication of this research is the connection between intrinsic motivation, measured by four dimensions of psychological empowerment, and IS security behavior. IS security behavior of employees is critical to the success of organizations, particularly when the incidents of IS security breaches originated from the insiders are more costly to handle than the outsider IS security breaches (Richardson, 2011). Employees are able to affect the IS security of the organization by engaging in, or complying with IS security policy (Bulgurcu et al., 2010). Thus, it is useful to consider the factors that motivate employees to comply with the IS security policy (Straub, 1990; Herath and Rao, 2009a; Bulgurcu et al., 2010). Specifically, this dissertation focused on intrinsic motivation because it has received far less attention in IS security literature as compared to extrinsic motivation (Son, 2011; Padayachee, 2011).

In essence, this dissertation demonstrates how psychological empowerment, dominated by meaning and competence dimensions, can influence employees IS security policy compliance intentions. This is encouraging, as it suggests that employees who feel empowered about their IS

security tasks are more willing to expend more efforts towards accomplishing the IS security tasks. As such, organizations that are concerned about managing human functions related to IS security should note that in order to increase employees' IS security policy compliance, imposing more external and controlled forces (e.g., sanctions, social pressures, and rewards) is not enough. Rather, management should find ways to maximize employees' intrinsic motivation, in terms of feelings of competence and meaning, in order to increase the likelihood of compliance.

In relation to the above, the present study investigated factors to enhance the intrinsic motivation. The current study offers important strategies for organizations to increase employees' intrinsic motivation. Rather than spending more money on providing rewards or implementing penalties to encourage (or discourage) IS security policy compliance (or non-compliance), organizations may actually focus on empowerment practices. As the results have indicated, it is strongly recommended for management to share more 'power tools' to the subordinates at all levels. Specifically, it is suggested that organizations attempt to foster feelings of empowerment related to IS security, should pay specific consideration to allow employees to participate in IS security decision-making processes. A participation strategy should give an opportunity for employees to contribute their input, ideas and thoughts about the IS security that are consistent with their own values or goals, and opportunities to set decisions regarding IS security jointly with the superiors. When employees are able to participate, they will feel empowered, and ultimately motivate them to comply with the IS security policy.

In addition, providing training related to IS security is important to increase employees' feeling of competence. It is strongly recommended for management to create IS security training and education programs that strives to increase employees personal mastery of IS security via hands-on exercises and activities or regular demonstration of IS security issues and

countermeasures. This will provide opportunities to observe successes and failures of other IS security behaviors and hence encourage and support their own IS security skills and responsible development. Thus, when designing an IS security training program, particular attention should be given to increasing employee IS security skills. Furthermore, allowing access to IS security strategy and goals is an important strategy to enhance employees' feelings of meaning of IS security tasks. It is recommended that management improves or diversifies the communication channels so that the well-specified IS security policy that consists of goals of IS security is conveyed to all employees. When employees understand the direction where the organization is heading related to IS security, they might know how their own IS security tasks would contribute to achieving the IS security goals. That is because employees find connections between the goals of IS security policy and their values.

Finally, it is suggested that when there are limited resources in organizations to empower the employees, management can combine those strategies. For example, management can communicate IS security strategy and goals in IS security training programs in order to affect both feelings of competence and meaning. Further, participation strategy could include participation in goal-setting decisions instead of only in IS security task-related decisions.

7.3 Limitations

This study has several limitations. First, this study employed cross-sectional approach to understand individuals IS security policy compliance. There are few weaknesses of this approach. For instance, it does not permit conclusions concerning causal direction. Further work should employ a longitudinal or an experimental design to lend further support to the causal relations hypothesized. Second, it is possible that the respondents' feelings and thoughts in answering the survey questions were influenced by environments, known as a 'halo effect'

(Herath and Rao, 2009a). Future studies can consider capturing the information regarding employees IS security compliance behavior by observing the behavior of employees at their workplace, or by obtaining the information from other sources (i.e., supervisors, peers). Case studies from one or a few organizations would also be useful future research since such case studies could provide an opportunity to measure employees' actual behavior related to IS security policy compliance and actual information regarding the structural empowerment practices at the workplace. In addition, respondents to this study self-reported their intention to comply with IS security policy. There is a possibility that they masked their true intention because noncompliance is socially undesirable (Trevino, 1992). To overcome the issue, Siponen and Vance (2010) suggested a use of hypothetical scenarios that provide a richer description.

Second, limitations are identified related to selection of participation. The non-random selection of MBA, MBA Executive, and MS Executive students in the USA to represent employees in organizations has limitation on several fronts. The first is that not all of them were necessarily currently working. While careful consideration was made to ensure that only people currently employed were selected as respondents, there was still a possibility that they were not. The next limitation with using students is generalizing results to all employees. As the non-random selection has represented different companies in various industries, the results are only generalizable to a similar population. Further, the limitations include data homogeneity, because the research only involved US data. Hence, one of the most important steps should be to conduct this study with a random selection of employees in various organizations across countries, and not just students.

Finally, since all measures were self-reported, thus the identified relations may have been inflated by common method variance (CMV). However, the fact that the Harman's factor score test found discriminant validity of the measures, it could weaken the issue of CMV.

7.4 Future Research

To extend the findings of this study, three recommendations are suggested for future investigations. First, the results of the present study indicate that, different from what was hypothesized, feelings of impact have a negative effect, and feelings of autonomy have no effect, on IS security policy compliance intentions. Future researchers are urged to further investigate these two psychological empowerments components' effects, and find possible contingent factors that may affect their influences on IS security policy compliance. It is speculated that the dimensions of psychological empowerment may interact.

Second, this study has investigated and determined the importance of employees' beliefs regarding competence of IS security tasks on their decision to perform or not to perform the IS security tasks. However, this study has used the term 'IS security tasks' to represent the overall or general IS security tasks. If more specific focus, such as complexity of IS security tasks were considered (e.g., security patching task and updating password task requiring different level of skills), we would be able to obtain more specific and meaningful results on how to design the SETA. Assuming the results show that respondents do not comply with IS security because they are not confident with their ability to do the patching task which is more difficult than the password changing task, SETA programs can be modified to focus on patching task. Thus, one possible direction for future research would be to focus on a very specific IS security tasks to truly understand the relation between employees' perceptions of competence and behavioral outcome. Future study may also test for the moderating effect of IS security task complexity.

Third, the focus of the current study is on structural empowerment practices, as antecedent of psychological empowerment. Therefore, examining the effects of other factors is beyond the scope of this study. Future research should use a more integrated model to compare and contrast different drivers to enhance feelings of empowerment. It would be desirable for

future studies to include other external variables such as task characteristics, leader-member exchange (LMX), formal and informal power, and personality traits.

7.5 Summary

In sum, this dissertation has provided three primary contributions to the IS security literature. First, this study has considered the influence of psychological empowerment on employees IS security policy compliance intentions answering previous calls for research that examines the intrinsic motivation for IS security behavior (Herath and Rao, 2009b; Padayachee, 2011, Son, 2011). Most notably, the findings of this research have shown the importance of two dimensions of psychological empowerment, competence and meaning when investigating the intrinsic motivation for IS security compliance. In addition, different dimensions of psychological empowerment may predict different outcomes (Spreitzer et al., 1997; Kraimer et al., 1999). Consistent with this line of argument, this study has confirmed that the competence and meaning dimensions are more important than the impact and choice dimensions in predicting individuals performance-related outcome, in the context of IS security. Second, this dissertation has considered how structural empowerment influences the psychological empowerment (Spreitzer, 1995a; Spreitzer, 1996). The findings have indicated that different structural empowerment facets predict different dimensions of psychological empowerment. Finally, this dissertation has shown the potential for structural empowerment to affect IS security compliance intentions via two dimensions of psychological empowerment—competence and meaning. In other words, psychological empowerment is a key mechanism that explains how structural empowerment contributes to IS security compliance intentions.

LIST OF REFERENCES

Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). Research Report: The Evolving Relation Between General and Specific Computer Self-Efficacy-An Empirical Assessment. *Information Systems Research*, 11(4), 418.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179-211.

Albrecht, W.S., Albrecht, C.C., and Albrecht, C.O. (2004). Fraud and corporate executives: Agency, Stewardship and Broken Trust. *Journal of Forensic Accounting,* 5 (2004), pp. 109–130.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445.

Alge, B. J., Ballinger, G. A., Tangirala, S., and Oakley, J. L. (2006). Information Privacy in Organizations: Empowering Creative and Extrarole Performance. *Journal of Applied Psychology, 91*(1), 221-232.

Allison, P. D. (2003). Missing Data Techniques for Structural Equation Modeling. *Journal of Abnormal Psychology*, 112(4), 545-557.

Anderson, C. L., and Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly, 34*(3), 613-A615.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, 103 (3), 411-423.

Ariss, S. S. (2002). Computer Monitoring: Benefits and Pitfalls Facing Management. *Information and Management, 39*(7), 553-558.

Avolio, B. J., Zhu, W., Koh, W., & Bhatia, P. (2004). Transformational leadership and organizational commitment: Mediating role of psychological empowerment and moderating role of structural distance. *Journal of Organizational Behavior*, 25, 951–968.

Bandura, A. (1977). Self-Efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review, 84*(2), 191-215.

Bandura, A. (1995). *Self-efficacy in changing societies*. New York: Cambridge University Press

Baron, R.M. and Kenny, D. A. (1986). The moderator–mediator distinction in social psychology research: Conceptual, strategic, and statistical considerations. *Journal of Personality Social Psychology.* vol. 51, pp. 1173–1183.

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin*, 107(2), 238-246.

Bonias, D., Bartram, T., Leggat, S.G., and Stanton, P. (2010), 'Does Psychological Empowerment Mediate the Relation Between High Performance Work Systems and Patient Care Quality in Hospitals?' *Asia Pacific Journal of Human Resources*, 48, 319–337.

Bordin, C., Bartram, T., and Casimir, G. (2006). The Antecedents and Consequences of Psychological Empowerment among Singaporean IT Employees. *Management Research News*.

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*(2), 151-164.

Bowen, D. E. and Lawler, E. E. 1992. The Empowerment of Service Workers: What, Why, How, and When. *Sloan Management Review*, 33: 31-39.

Bowerman, B. L. and O'Connell, R. T. (1990). *Linear Statistical Models: An Applied Approach (2nd ed.)*. Duxbury Press, Belmont, California.

Broedling, L. A. (1977). The Uses of the Intrinsic-Extrinsic Distinction in Explaining Motivation and Organizational Behavior. *Academy of Management Review, 2*(2), 267-276.

Browne, M. W., & Cudeck, R. (1989). Single sample cross-validation indexes for covariance structures. *Multivariate Behavioral Research*, 24, 445-455.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-A527.

Byrne, B.M. (2009). *Structural Equation Modeling with AMOS (2nd ed.).* Routiledge. Taylor and Francis Group.

Campbell, J. P., McCloy, R. A., Oppler, S. H., & Sager, C. E. (1993). A theory of performance. In N. Schmitt & W. C. Borman (Eds.), Personnel selection in organizations (pp. 35-70). San Francisco: Jossey-Bass.

Carless, S.A. (2004). Does psychological empowerment mediate the relation between psychological climate and job satisfaction? *Journal of Business and Psychology, 18 (4),* 405.

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), 18-41.

Chen, G., and Klimoski, R. J. (2003). The Impact of Expectations on Newcomer Performance in Teams as Mediated by Work Characteristics, Social Exchanges, and Empowerment. *Academy of Management Journal, 46*(5), 591-607.

Chen, Y., Ramamurthy, K., and Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems, 29*(3), 157-188.

Comrey, A. L., and Lee, H. B. (1992). *A First Course in Factor Analysis* (Second ed.). Hillsdale, New Jersey: Lawrence Erlbaum Associates.

Conger, J. A., and Kanungo, R. N. (1988). The Empowerment Process: Integrating Theory and Practice. *Academy of Management Review, 13*(3), 471-482.

Cotton, J. L., Vollrath, D. A., Froggatt, K. L., Lengnick-Hall, M. L., & Jennings, K. R. (1988). Employee Participation: Diverse Forms and Different Outcomes. *Academy of Management Review*, 13(1), 8-22.

CSO. (2010). *2010 CyberSecurity Watch*. Retrieved online on August 20, 2012 from http://www.csoonline.com/documents/pdfs/2010CyberSecurityResults.pdf

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), 79-98.

Davis, D. (2000). *Business Research for Decision Making*. Pacific Grove, CA: Duxbury Press.

Davis, J. H., David, S. F., and Donaldson, L.L. (1997). *The Academy of Management Review*. Vol. 22, No. 1 (Jan., 1997), pp. 20-47.

Deci, E. L., and Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behavior*. New York: Plenum.

Deci, E. L., and Ryan, R. M. (2009). The "What" and "Why" of Goal Pursuits: Human Needs and the Self-Determination of Behavior. *Psychological Inquiry*, Vol. 11, No. 4, October 2000, pp. 227–268.

Deci, E. L., Koestner, R., and Ryan, R. M. (1999). A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological Bulletin, 125*(6), 627.

Dhillon, G. (1996). *Interpreting the Management of Information Systems Security.* (Unpublished Dissertation). London School of Economics and Political Sciences, London, United Kingdom.

Dhillon, G. (2001). *Information Security Management: Global Challenges in the New Millennium*: Idea Group Pub.

Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases*. Hoboken, NJ: John Wiley and Sons.

Dhillon, G., Silva, L., and Backhouse, J. (2004). Computer crime at CEFORMA: A case study. *International Journal of Information Management, 24*(6), 551-561.

Diamantopoulos, A. and Siguaw, J.A. (2000), *Introducing LISREL*. London: Sage Publications.

Dominique, D. (1999). More Managers Monitor e-mail. *Computerworld, 33 (42)*.

Donaldson, L., & Davis, J. H. (1991). Stewardship Theory or Agency Theory: CEO Governance and Shareholder Returns. *Australian Journal of Management* (University of New South Wales), 16(1), 49.

Ergeneli, A., Sag, G., Ari, I., & Metin, S. (2007). Psychological empowerment and its relation to trust in immediate managers. *Journal of Business Research*, 60, 41–56.

Ford, M. T., and Tetrick, L. E. (2011). Relations among Occupational Hazards, Attitudes, and Safety Performance. *Journal of Occupational Health Psychology, 16*(1), 48-66.

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

Furnell, S. M., Gennatou, M., and Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management, 15*(5/6), 352-357.

Gefen D., Straub D.W., and Boudreau, M. (2000). Structural Equation Modeling Techniques and Regression: *Guidelines for Research Practice Communications of AIS*. Volume 4, Article 7.

Gist, M. E., & Mitchell, T. B. (1992). Self-Efficacy: A Theoretical Analysis of Its Determinants and Malleability. *Academy Of Management Review*, 17(2), 183-211.

Gist, M. E., Schwoerer, C., & Rosen, B. (1989). Effects of Alternative Training Methods on Self-Efficacy and Performance in Computer Software. Journal of Applied *Psychology*, 74(6), 884.

Hackman, J., and Oldham, G. R. (1980). *Work Redesign*. Reading, Mass.: Addison-Wesley.

Hair, J. F., Black, W. C., Babin, B. J., and Anderson, R. E. (2010). *Multivariate Data Analysis* (Seventh Edition ed.): Prentice Hall Higher Education.

Hall, P. and Wang, Q. (2004). Exact Convergence Rate and Leading Term in Central Limit Theorem for Student's t Statistic. *Annals of Probability*, 32(2), 1419-1437.

Harris, M. A. (2010). *The Shaping of Managers' Security Objectives through Information Security Training*. (Unpublished Dissertation). Virginia Commonwealth University. Richmond, VA.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems, 18*(2), 106-125.

Herath, T., and Rao, R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Hoffman, G. M. (1994). *The Technology Payoff: How to Profit with Empowered Workers in The Information Age*: Irwin Professional Pub.

Hon, A. H. Y., and Rensvold, R. B. (2006). An interactional perspective on perceived empowerment: the role of personal needs and task context. *International Journal of Human Resource Management, 17*(5), 959-982.

Hsu, M.-H., and Chiu, C.-M. (2004). Internet self-efficacy and electronic service acceptance. *Decision Support Systems*, 38, 369-381.

Hu, L., and Bentler P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives, *Structural Equation Modeling: A Multidisciplinary Journal*, 6:1, 1-55.

Kanter, R. M. (1977). *Men and women of the corporation*: Basic Books.

Kark, R., Shamir, B., & Chen, G. (2003). The two faces of transformational leadership: Empowerment and dependency. *Journal of Applied Psychology*, 88, 246–255.

Karsten, R. and Roth, R. M. (1998). Computer Self-Efficacy: A Practical Indicator of Student Computer Competency in Introductory IS Courses. *Informing Science The International Journal of an Emerging Transdiscipline*,Vol.1(3), p.61

Ke, W. and Zhang, P. (2011). Effects of Empowerment on Performance in Open-Source Software Projects. *IEEE Transactions on Engineering Management*, Vol.58(2), pp.334-346

Kirby, S. L., and Davis, M. A. (1998). A Study of Escalating Commitment in Principal-Agent Relations: Effects of Monitoring and Personal Responsibility. *Journal of Applied Psychology, 83*(2), 206-217.

Kirsch, L. J. (2004). Deploying Common Systems Globally: The Dynamics of Control. *Information Systems Research, 15*(4), 374-395.

Kline, R. B. (2011). *Principles and Practice of Structural Equation Modeling (3rd ed.).* The Guilford Press.

Knoop, R. (1995), "Influence of participative decision-making on job satisfaction and organizational commitment of school principals", *Psychological Report*, Vol. 76, pp.379-382.

Kraimer, M. L., Seibert, S. E., & Liden, R. C. (1999). Psychological empowerment as a multidimensional construct: A test of construct validity. *Educational and Psychological Measurement, 59*, 127–142.

Laschinger, H. K. (1996). A theoretical approach to studying work empowerment in nursing: a review of studies testing Kanter's theory of structural power in organizations. *Nursing Administration Quarterly, 20*(2), 25-41.

Laschinger, H. K. S., Finegan, J. E., Shamian, J., and Wilk, P. (2004). A longitudinal analysis of the impact of workplace empowerment on work satisfaction. *Journal of Organizational Behavior, 25*(4), 527-545.

Laschinger, H. K. S., Finegan, J., Shamian, J., & Wilk, P. (2001). Impact of structural and psychological empowerment on job strain in nursing work settings: expanding Kanter's Model. *Journal of Nursing Administration*, 31, 260–272.

Lawler, E. E. (1986). *High-involvement management*. San Francisco, CA: Jossey-Bass.

Lawler, E. E. (1992). The ultimate advantage. San Francisco: Jossey-Bass.

Leach, J. (2003). Improving user security behavior. *Computers and Security, 22*(8), 685-692.

Liao, H., Toya, K., Lepak, D. P., and Hong, Y. (2009). Do they see eye to eye? Management and employee perspectives of high-performance work systems and influence processes on service quality. *Journal of Applied Psychology*, 94, 371–391.

Liden, R. C., Wayne, S. J., and Sparrowe, R. T. (2000). An examination of the mediating role of psychological empowerment on the relations between the job, interpersonal relations, and work outcomes. *Journal of Applied Psychology, 85*(3), 407-416.

Little, R.J.A. and Rubin, D.B. (1987) Statistical Analysis with Missing Data. J. Wiley & Sons, New York.

Little, R.J.A. and Rubin, D.B. (1987) *Statistical Analysis with Missing Data*. J. Wiley & Sons, New York.

Little, R.J.A. and Schenker, N. (1995). Missing data, in Arminger, G., Clogg, C. and Sobel, M. (Eds.): *Handbook of Statistical Modeling for the Social and Behavioral Sciences*, Plenum, New York.

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

Logan, M. S., and Ganster, D. C. (2007). The Effects of Empowerment on Attitudes and Performance: The Role of Social Support and Empowerment Beliefs. *Journal of Management Studies, 44*(8), 1523-1550.

MacKinnon, D. P., Lockwood, C. M., Hoffman, J. M., West, S. G., & Sheets, V. (2002). A comparison of methods to test Mediation and other intervening variable effects. *Psychological Methods*, 7, 83-104.

Manz, C. C., and Sims Jr, H. P. (1987). Leading Workers to Lead Themselves: The External Leadership of Self-Managing Work Teams. *Administrative Science Quarterly, 32*(1), 106-129.

May, D. R., Gilson, R. L., & Harter, L. M. (2004). The psychological conditions of meaningfulness, safety, and availability, and the engagement of the human spirit at work. *Journal of Occupational & Organizational Psychology*, 77(1), 11-37.

Maynard, M. T., Gilson, L. L., and Mathieu, J. E. (2012). Empowerment-fad or fab? A multilevel review of the past two decades of research (vol 38, pg 1231, 2012). *Journal of Management, 39*(2), 567-567.

McDonald, R. P., & Ho, M.-H. R. (2002). Principles and practice in reporting structural equation analyses. *Psychological Methods*, 7(1), 64-82.

Mirchandani, D., and Motwani, J. (2003). Reducing Internet Abuse in the Workplace. *SAM Advanced Management Journal 68*(1), 22.

Mitnick, K. D. (2002). *The Art of Deception: Controlling the Human Element of Security* New York: Wiley Publishing.

Murray, B. (1991). *Running Corporate and National Security Awareness Programs* Paper presented at the Proceedings of the IFIP TC11 Seventh International Conference on IS Security Amsterdam.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18*(2), 126-139.

Nagin, D. (1975). *General Deterrence: A Review of the Empirical Evidence*. S.l.: s.n.].

Nunnally J. C. and Bernstein I. H. (1994). *Psychometric Theory (3rd ed.)*. New York:McGraw-Hill.

Nunnally, J. C. (1978). *Psychometric theory (2nd ed.)*. New York: McGraw-Hill.

O'Boyle, E. H., Jr., and Williams, L. J. (2011). Decomposing model fit: Measurement vs. theory in organizational research using latent variables. *Journal of Applied Psychology*, 96(1), 1-12.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers and Security, 31*(5), 673-680.

Pahnila, S., Siponen, M., and Mahmood, A. (2007). Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. PACIS 2007 Proceedings.

Podsakoff, P. M., and Organ, D. W. (1986). Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management*, 12(4), 531.

Podsakoff, P. M., MacKenzie, S. B., Jeong-Yeon, L., 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), 879.

Ponemon, L. (2009). *Trends in Insider Compliance with Data Security Policies: Employees Evade and Ignore Security Policies* :Ponemon Institute. Retreived on February 2, 2012 from http://www.ponemon.org/blog/more-employees-ignoring-data-security-policies.

Porter, L. W., Steers, R. M., Mowday, R. T., and Boulian, P. V. (1974). Organizational commitment, job satisfaction, and turnover among psychiatric technicians. *Journal of Applied Psychology,* 59, 603-609.

Preacher, K., and Hayes, A. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, 40(3), 879-891.

Puhakainen, P., and Siponen, M. (2010). Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34*(4), 767-A764.

Quinn, R.E., and Spreitzer, G.M. (1997). The road to empowerment: Seven questions every leader should consider. *Organizational Dynamics*, Autumn, 26(2): 37-51.

Rhee, H.-S., Kim, C., and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security, 28*(8), 816-826.

Richardson, R. (2011). *2010/2011 CSI Computer Crime and Security Survey*. USA: Computer Security Institute. Retrieved on February 4, 2012 from http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html.

Ryan, R. M., and Deci, E. L. (2000). Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology, 25*(1), 54-67.

Scandura, T. A., Graen, G. B., and Novak, M. A. (1986). When managers decide not to decide autocratically: An investigation of leader–member exchange and decision influence. *Journal of Applied Psychology, 71*(4), 579-584.

Seibert, S. E., Wang, G., and Courtright, S. H. (2011). Antecedents and Consequences of Psychological and Team Empowerment in Organizations: A Meta-Analytic Review. *Journal of Applied Psychology, 96*(5), 981-1003.

Shrout, P. E., & Bolger, N. (2002). Mediation in experimental and nonexperimental studies: New procedures and recommendations. Psychological Methods, 7, 422-445.

Siau, K., Nah, F. F.-H., and Teng, L. (2002). Acceptable Internet Usage Policy. *Communications of the ACM, 45*(1), 75-79.

Sipior, J. C., and Ward, B. T. (2009). A Framework for Employee E-mail Privacy within the United States. *Journal of Internet Commerce, 8*(3/4), 161-179.

Siponen, M., and Vance, A. (2010). Neutralization: New Insights into The Problem Of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487-A412.

Siponen, M., Pahnila, S., and Mahmood, A. (2007). Employees' Adherence to Information Security Policies: An Empirical Study New Approaches for Security, Privacy and Trust in Complex Environments. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff and R. von Solms (Eds.), (Vol. 232, pp. 133-144): Springer Boston.

Siu, H. M., Laschinger, H. K. S., and Vingilis, E. (2005). The effect of problem-based learning on nursing students' perceptions of empowerment. *Journal of Nursing Education, 44*(10), 459-469.

Skyes, G., and Matza, D. (1957). Techniques of Neutralisation: A Theory of Delinquency. *American Sociological Review*, 22, 664-670.

Smith, W. P., and Tabak, F. (2009). Monitoring Employee E-mails: Is There Any Room for Privacy? *Academy of Management Perspectives, 23*(4), 33-48.

Sobel, M. E. (1982). Asymptotic intervals for indirect effects in structural equations models. In S. Leinhart (Ed.), *Sociological methodology*, pp.290-312. San Francisco: Jossey-Bass.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information and Management, 48*(7), 296-302.

Spears, J. L., and Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly, 34*(3), 20.

Spreitzer, G. (2007). Taking Stock: A review of more than twenty years of research on empowerment at work. In The Handbook of Organizational Behavior, C. Cooper and J. Barling eds. Sage Publications.

Spreitzer, G. M. (1995a). An empirical test of a comprehensive model of intrapersonal empowerment in the workplace. *American Journal of Community Psychology, 23*(5), 601-629.

Spreitzer, G. M. (1995b). Psychological Empowerment in the Workplace: Dimensions, Measurement and Validation. *Academy of Management Journal, 38*(5), 1442-1465.

Spreitzer, G. M. (1996). Social Structural Characteristics of Psychological Empowerment. *Academy of Management Journal, 39*(2), 483-504.

Spreitzer, G. M., Kizilos, M. A., and Nason, S. W. (1997). A Dimensional Analysis of the Relation between Psychological Empowerment and Effectiveness, Satisfaction, and Strain. *Journal of Management, 23*(5), 679.

Stajkovic, A. D., & Luthans, F. (1998). Self-efficacy and work-related performance: A meta-analysis. *Psychological Bulletin*, 124(2), 240-261

Stanton, J. M., Stam K. R., Guzman, and Caldera. (2003). *Examining the linkages between organizational commitment and information security.* Paper presented at the *IEEE Systems, Management, and Cybernetics Conference*, Washington DC, USA.

Stanton, J. M., and Weiss, E. M. (2000). Electronic monitoring in their own words: an exploratory study of employees' experiences with new types of surveillance. *Computers in Human Behavior, 16*(4), 423-440.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security, 24*(2), 124-133.

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

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

Straub, D. W., and Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441-469.

Tabachnick, B. G., and Fidell, L. S. (2001). *Using Multivariate Statistics* (Fourth edition). Needham Height, MA: Pearson Education.

Thomas, K. W. (2009). *Intrinsic motivation at work: what really drives employee engagement*. 2nd ed. San Francisco: Berrett-Koehler Publishers.

Thomas, K. W., and Velthouse, B. A. (1990). Cognitive Elements of Empowerment: An "Interpretive" Model of Intrinsic Task Motivation. *Academy of Management Review, 15*(4), 666-681.

Tyler, T. R., and Blader, S. L. (2005). Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following In Work Settings. *Academy of Management Journal, 48*(6), 1143-1158.

Urbaczewski, A., and Jessup, L. M. (2002). Does Electronic Monitoring of Employee Internet Usage Work? *Communications of the ACM, 45*(1), 80-83.

U.S Small Business Association. (2012). *Small Business Size Standards.* Retrieved from https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf.

Venkatesh, V., and Brown, S. A. (2001). A Longitudina Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges. *MIS Quarterly, 25*(1), 71-102.

Wallach, V. A., and Mueller, C. W. (2006). Job Characteristics and Organizational Predictors of Psychological Empowerment among Paraprofessionals within Human Service Organizations: An Exploratory Study. *Administration in Social Work, 30*(1), 94-115.

Wang G., and Lee, P. D. (2009). Psychological Empowerment and Job Satisfaction: An Analysis of Interactive Effects. *Group & Organization Management*, 34(3), 271-296.

Wat, D., and Shaffer, M. A. (2005). Equity and relation quality influences on organizational citizenship behaviors: The mediating role of trust in the supervisor and empowerment. *Personnel Review, 34*(4), 406-422.

Wathne, K. H., and Heide, J. B. (2000). Opportunism in Interfirm Relations: Forms, Outcomes, and Solutions. *Journal of Marketing, 64*(4), 36-51.

Westland, C. J. (2010). Lower bounds on sample size in structural equation modeling. *Electronic Commerce Research and Applications*, 9(6), 476-487.

Williams, L., and O'Boyle, E. (2011). The myth of global fit indices and alternatives for assessing latent variable relations. *Organizational Research Methods*, 14 (2), 350-369.

Workman, M., Bommer, W. H., and Straub, D. W. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Zacharatos, A., Barling, J., and Iverson, R. D. (2005). High-Performance Work Systems and Occupational Safety. *Journal of Applied Psychology, 90*(1), 77-93.

Zhang, X., and Bartol, K. M. (2010). Linking Empowering Leadership and Employee Creativity: The Influence of Psychological Empowerment, Intrinsic Motivation, and Creative Process Engagement. *Academy of Management Journal, 53*(1), 107-128.

Zikmund, W. G. (2003). *Business Research Methods (7th ed.)*. Mason, OH: Thomson/South-Western.

APPENDIX

Figure 9.1: Visual Representation of the Measurement Model

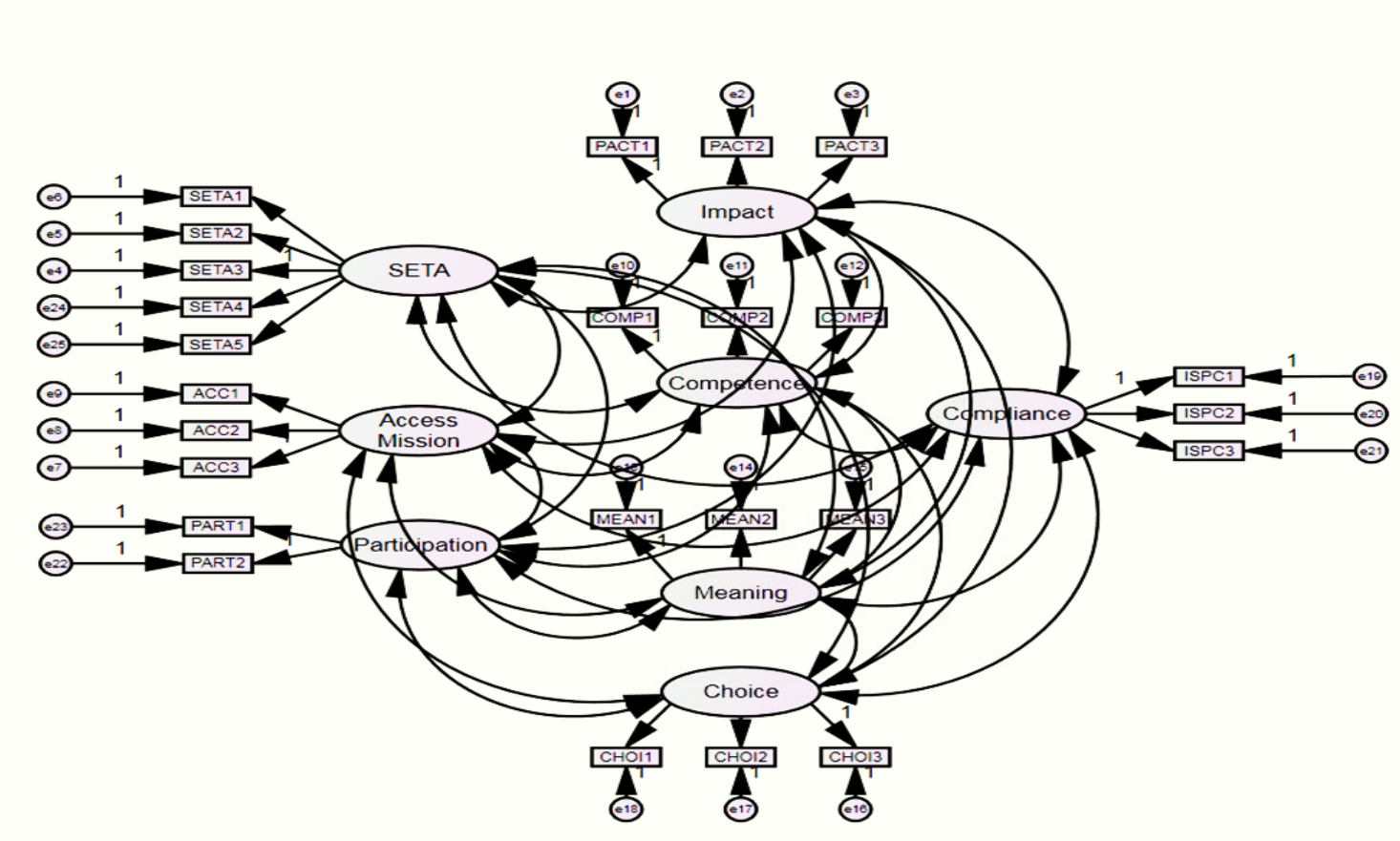


Figure 9.2: Visual Representation of the Structural Model

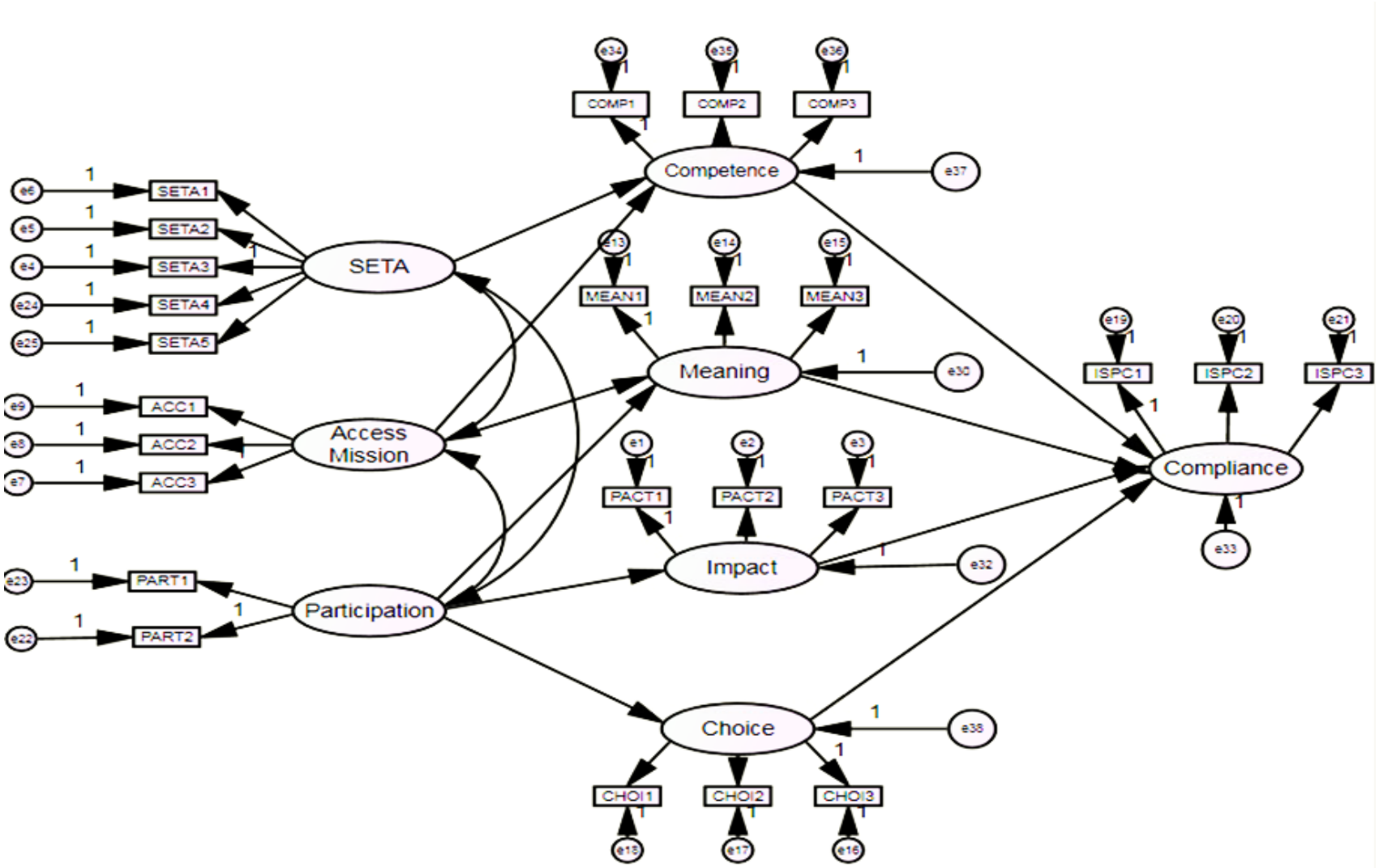


Figure 9.3: Full SEM

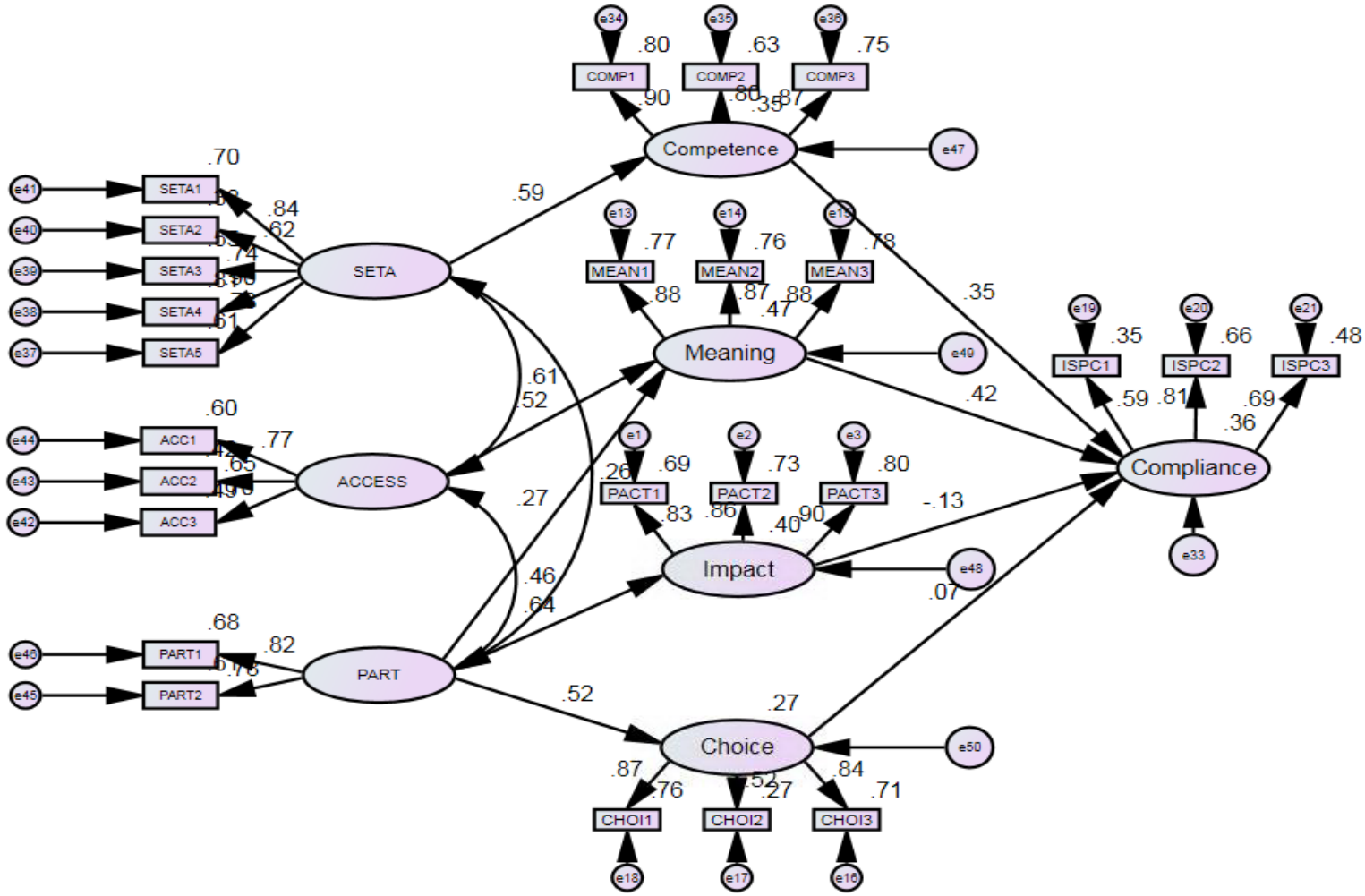


Figure 9.4: Questionnaire

Virginia Commonwealth University

School of Business

Your completion of this survey is greatly appreciated.

All information will be treated strictly confidential.

Study conducted by:

Yurita Yakimin Abdul Talib

PhD Candidate

A STUDY OF INFORMATION SYSTEM SECURITY

If you have any question regarding the questionnaire or the study, feel free to contact the author at:

804 665 5867 (mobile) ; abdultalibyy@vcu.edu (email)

Coverage

The study relates employees in the USA and compliance with organizational IS security policies.

Respondents

Current and previous employees in various work setting should answer this questionnaire. Respondents must be at least 18 years of age.

The Questions

The questions only require your perception with respect to information systems and information security in your organization. **Please keep information systems and information security of your organization in your mind while you fill up this questionnaire.** Read the questionnaire statements and select the most appropriate answer for each. There is no right or wrong answer. It is your opinion that is most justifiable. Some of the questions look similar, but this is important to ensure that we can assess your response scientifically and draw valid conclusions.

Confidentiality, risks and the use of data

Your participation with this study is voluntary. By participating, you will help Information System (IS) research at VCU. As with any research study there are risks. The risks in this study are minimal. Participants could become uncomfortable while answering some of the questions, although there are no risks expected by participating in this study. Your response will be confidential, only group data will be analyzed.

Thank you for your participation!

Part I: Survey questions

1. Has your organization established IS security policies?

   □ Yes □ No

2. To what extent are you aware of the regulations prescribed by the IS security policies of your organization?

Completely unaware						Completely aware
1	2	3	4	5	6	7

Please answer the following questions using a 1 to 7 scale with 1-Strongly Disagree, and 7-Strong Agree. Please circle your answer to each question.

3.	I intend to comply with the requirements of the IS security policies of my organization in the future.	1 2 3 4 5 6 7
4.	I actively participate in defining, reviewing or approving any IS security controls related to protecting the organization's information (e.g. access control, separation of duties, employee training on IS security awareness and etc.)	1 2 3 4 5 6 7
5.	My organization provides employees with education on computer software copyright laws.	1 2 3 4 5 6 7
6.	I have significant autonomy in determining how I do my job of securing information and information systems.	1 2 3 4 5 6 7
7.	I have considerable opportunity for independence and freedom in how I do my job of securing information and information systems.	1 2 3 4 5 6 7
8.	In managing risk to information and information systems in my company, I actively perform, or contribute to decision-making in any risk management activities (e.g. documenting business processes or transactions for risk evaluation, ensuring key controls exist to mitigate specific types of risks, implementing control and etc.)	1 2 3 4 5 6 7
9.	I have significant influence over what happens in my department	1 2 3 4 5 6 7
10.	I understand top management's IS security vision of the organization.	1 2 3 4 5 6 7

11. My organization provides training to help employees improve their awareness of computer and IS security issues.	1 2 3 4 5 6 7
12. I have access to the strategic information I need to do my job of securing information and information systems well.	1 2 3 4 5 6 7
13. In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	1 2 3 4 5 6 7
14. My work of securing information and information systems is personally meaningful to me.	1 2 3 4 5 6 7
15. My work of securing information and information systems is very important to me.	1 2 3 4 5 6 7
16. My organization educates employees on their computer security responsibilities.	1 2 3 4 5 6 7
17. I have a great deal of control over what happen in my department.	1 2 3 4 5 6 7
18. My work of securing information and information systems is meaningful to me.	1 2 3 4 5 6 7
19. I have mastered the skills necessary for my job of securing information and information systems.	1 2 3 4 5 6 7
20. I am confident about my ability to do my job of securing information and information systems.	1 2 3 4 5 6 7
21. My impact on what happens in my department related to IS security is large.	1 2 3 4 5 6 7
22. I am self-assured about my capabilities to perform my job of securing information and information systems activities.	1 2 3 4 5 6 7
23. I can decide on my own how to go about doing my job of securing information and information systems.	1 2 3 4 5 6 7
24. I intend to carry out my responsibilities prescribed in the IS security policies of my organization when I use information and technology in the future.	1 2 3 4 5 6 7
25. In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.	1 2 3 4 5 6 7
26. I intend to protect information and technology resources according to the requirements of the IS security policies of my organization in the future.	1 2 3 4 5 6 7
27. I understand the IS security strategies and goals of the organization.	1 2 3 4 5 6 7

Part II: About yourself and your organization

28. Your gender

□ Male □ Female

29. Your highest level of education

□ Less than high school □ Undergraduate degree

□ High school degree □ Graduate degree

□ College degree □ Other

30. Your age

□ 20–25 □ 56–65

□ 26–35 □ 66–75

□ 36–45 □ 76–85

31. How many years have you used a computer and the Internet? _____

32. On average, how many hours do you use a computer for work every day? _____

33. How many years have you worked for your current organization?

□ less than 1 year □ 10 - 15 years

□ 1 – 5 years □ more than 15 years

□ 5 – 10 years

34. How many years have you worked in your current position in the organization?

□ less than 1 year □ 10 - 15 years

□ 1 – 5 years □ more than 15 years

□ 5 – 10 years

35. Your job title is _____

36. Number of employees in your organization

□ Fewer than 500 □ 5,000–10,000

□ 500–999 □ More than 10,000

□ 1,000–4,999

37. Annual sales revenue of your organization (in your local currency)

□ Less than 1 million □ 200 million – 500 million

□ 1 million – 5 million □ 500 million – 1 billion

□ 6 million – 10 million □ 1 billion – 5 billion

□ 10 million – 50 million □ More than 5 billion

□ 50 million – 200 million

38. In which industry is your organization operating?

□ Education □ Real Estate

□ Financial Services □ Services

□ Government □ Information Technology

□ Food/Beverage/CPG □ Telecommunications

□ Health Care □ Travel

□ Manufacturing□ □ Wholesale/Retail

□ Nonprofit □ Other, please specify _____

□ Medical, Bio-Technology, Pharmacology

Thank you for participating

Vita

Yurita Yakimin Abdul Talib was born in Ipoh Perak, Malaysia. She received his Bachelor of Arts (Honors) in Accounting and Finance from the University of the West of England, Bristol, United Kingdom in 1998. She received a Master's of Science in Information Technology from the University Science of Malaysia in 2002. Her research interests include accounting information systems, behavioral information systems security, and empowerment. She has taught courses at Northern University of Malaysia and the Virginia Commonwealth University in accounting information systems, IT in accounting, system analysis and design, database, audit and control in information systems, formulation of information security policies, and web development.