THE ANTECEDENTS OF INFORMATION SECURITY POLICY COMPLIANCE

by

Burcu Bulgurcu

B.Sc., Middle East Technical University, 2003
M.Sc., Middle East Technical University, 2006

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF APPLIED SCIENCE

in

The Faculty of Graduate Studies

Business Administration

THE UNIVERSITY OF BRITISH COLUMBIA
(Vancouver)

July 2008

ABSTRACT

Information security is one of the major challenges for organizations that critically depend on information systems to conduct their businesses. Ensuring safety of information and technology resources has become the top priority for many organizations since the consequences of failure can be devastating. Many organizations recognize that their employees, who are often considered as the weakest link in information security, can be a great resource as well to fight against information security-related risks. The key, however, is to ensure that employees comply with information security related rules and regulations of the organization. Therefore, understanding of compliance behavior of an employee is crucial for organizations to effectively leverage their human capital to strengthen their information security.

This research aims at identifying antecedences of an employee's compliance with the information security policy (ISP) of his/her organization. Specifically, we address how employees without any malicious intent choose to comply with requirements of the ISP with regards to protecting the information and technology resources of their organizations. Drawing on the Theory of Planned Behavior, we show an employee's attitude towards compliance results in his/her intention to comply with the ISP. Of those, *Benefit of Compliance* and *Cost of Non-Compliance* are shown to be shaped by positive and negative reinforcing factors; such as, *Intrinsic Benefit*, *Safety of Resources*, *Rewards* and *Intrinsic Cost, Vulnerability of Resources,* and *Sanctions*, respectively. We also investigate the role of information security awareness on an employee's ISP compliance behavior. As expected, we show that information security awareness positively influences attitude towards compliance. We also show that information security awareness positively influences the perception of reinforcing factors and negatively increases perception of the *Cost of Compliance*. As organizations strive to get their employees to follow their information security rules and regulations, our study sheds light on the role of an employee's information security awareness and his/her beliefs about the rationality of compliance and non-compliance with the ISP.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

First of all, I would like to thank UBC Research and Social Sciences and Humanities Research Council of Canada (SSHRC) for providing funding for this study. I would like to thank and express my heartfelt gratitude to my advisor, Assist. Prof. Hasan Cavusoglu. His guidance, support, and positive attitude throughout the study encouraged me keep up with the work all the way through. I am also grateful to my co-supervisor, Prof. Izak Benbasat, for leading this study and sharing his valuable experiences and feedback.

1. INTRODUCTION

The heavy reliance of organizations on Information Systems (IS) requires them to deal with the risks associated with those systems. Today, information security-related risks are the major challenge for many organizations since information security-related risks may have dire consequences including corporate liability, loss of credibility, or monetary damage (Cavusoglu et al. 2004). Hence, ensuring information security has become one of the top managerial priorities in many organizations (Brancheau et al. 1996; Lohmeyer et al. 2002; Ransbotham and Mitra 2008).

To ward off information security-related risks and hence ensure information security, organizations often rely on technology-based solutions (Deloitte 2005; Ernst & Young 2005). Although technology-based solutions help improve information security (Straub 1990), exclusively (or excessively) relying on technology-based solutions is not sufficient to address information security-related risks in today's complex information systems (Cavusoglu et al. 2008; Dhillon and Backhouse 2001; Siponen 2005). Empirical and anecdotal evidence indicate that the numbers of information security-related incidents are increasing while organizations make more investments in technology-based solutions support. This implies that success in information security can be achieved when organizations invest in both technical and socio-organizational resources.

As the focus in information security has shifted towards individual and organizational perspectives of information security, information security awareness (ISA) has emerged as one of the key socio-organizational resources (Hentea 2005; Peltier 2005; Puhakainen 2006; Siponen 2000; Siponen 2001). Creating information security awareness among employees improves the information security of the organization (Cavusoglu et al. 2008) since employees are often the weakest link in information security (Mitnick and Simon 2002). Organizations also create information security policies (hereafter

ISP) to provide guidelines to employees as to what they should do in order to ensure information security while they interact with information system to perform their business responsibilities (Whitman et al. 2001). Effectively dealing with information security-related risks necessitates that employees must comply with the ISP of their organizations. Although creating guidelines and policies are essential to start with, it is not enough to ensure employees' compliance with them. Therefore, an understanding of what factors motivate employees to comply with the ISP of their organizations is essential for IS management. This will help IS managers diagnose deficiencies of their information security management efforts with regards to human aspect of information security and give them an opportunity to solve the behavioral issues of information security management. Except for a recent effort by Pahnila et al. (2007) who investigated the factors affecting the compliance of employees of one Finnish company, by and large, in the literature, there is still a lack of theorizing on, and empirical support for what determine an employee's compliance with information security policies. Our study aims at extending our knowledge about the employee's compliance with the ISP in the literature. We address three specific questions in this research:

(i) What are the broad classes of beliefs held by an employee about the rationality of compliance and non-compliance with the ISP? And how do these beliefs influence his/her attitudes towards compliance and in turn their intention to comply?

(ii) What are the salient reinforcing factors that help form those broad classes of beliefs?

(iii) What is the role of information security awareness in shaping those factors and beliefs and in influencing the employee's attitude towards compliance?

Drawing on the theory of planned behavior (TPB) (Fishbein and Ajzen 1975; Ajzen 1991); we postulate that an employee's intention to comply with the ISP of his/her organization is influenced by employee's attitude towards compliance and employee's perceived behavior control. Based on rational

choice theory (von Neumann and Morgenstern 1944) and its applications in criminology—namely, theory of crime and punishment (Becker 1968) and theory of participation in illegitimate activities (Ehrlich 1973), we identified three broad classes of beliefs about the rationality of compliance and non-compliance with the ISP – namely, *Benefit of Compliance*, *Cost of Non-Compliance* and *Cost of Compliance* – and postulate that these three broad classes of beliefs influence the employee's attitude towards compliance with the ISP. Although rewards (Boss and Kirsch 2007; Pahnilaet al. 2007) and sanctions (Kankanhalli et al. 2003; Pahnila et al. 2007; Straub 1990), which are notions related to the first two broad classes of beliefs respectively, have been studied before, *Cost of Compliance* is new to the information security literature and has not yet been studied. Further, although rewards and sanctions are motivational factors that help employees form the first two broad classes of beliefs, we believe that they are not the only ones. Hence, within the context of information security, we identify three salient motivational factors—*Intrinsic Benefit*, *Safety of Resources*, and *Rewards*—that drive *Benefit of Compliance*, and three salient motivational factors—*Intrinsic Cost*, *Vulnerability of Resources*, and *Sanctions*—which drive *Cost of Non-Compliance*. Further, we investigate the role of information security awareness. Specifically, we postulate that information security awareness influences employee's perception of salient reinforcing factors for forming beliefs about *Benefit of Compliance*, *Cost of Non-Compliance*, and *Cost of Compliance* as well as employee's attitude towards compliance.

The research questions about antecedences of an employee's compliance behavior were addressed by using the data collected through survey of 464 employees from various organizations. Analyses of data suggest that three broad classes of beliefs that an employee possesses about the rationality of compliance and non-compliance significantly affect his/her attitude towards compliance with the ISP of his/her organization. Further, we found that three positive reinforcing factors significantly influence

an employee's perception of *Benefit of Compliance* and three negative reinforcing factors significantly influence and employee's perception of *Cost of Non-Compliance*.

Lastly, we identified the key role that an employee's information security awareness plays in his/her compliance behavior. We found that information security awareness positively influences an employee's attitude towards compliance. Other than this direct effect, we found that information security awareness indirectly affects the employee's attitude towards compliance through the employee's perception of reinforcing factors and cost beliefs about compliance. Particularly, information security awareness positively influences an employee's perception of reinforcing factors leading to the formation of beliefs about *Benefit of Compliance* and *Cost of Non-Compliance*, and negatively influences an employee's belief about *Cost of Compliance*.

2. LITERATURE REVIEW

Previous studies on IS security highlighted a number of important topics such as IS security effectiveness (Kankanhalli et al. 2003; Straub 1990; Woon and Kankanhalli 2003), security planning and risk management (Straub 1998; Straub and Welke 1998; Soo Hoo 2000), economics of IS security and evaluation of IS security investments (Cavusoglu et al. 2004a, 2004b, 2004c), and design, development and alignment of information security policies (Doherty and Fulford 2006; Siponen and Iivari 2006). While these studies expand our understanding of IS security from various perspectives, there is no doubt that the number of existing studies is not commensurate with the importance of IS security. Other than a few exceptions, there is a gap in the literature particularly in the socio-organizational and human aspects of information security.

An emerging research stream on the human perspective of information security focuses on end-user (insider) behaviors and particularly attempts to identify the factors leading to good, appropriate, and ethical behaviors regarding information security. Insiders refer to employees who are explicitly or implicitly granted privileges authorizing use of a particular system or facility (Neumann 1999). The current literature recognizes that insiders may pose a great challenge to an organization since ignorance, mistakes, and deliberate acts of employees can jeopardize the ultimate goal of establishing information security in the organization (E-Crime Watch Survey 2006; Lee and Lee 2002; Lee et al. 2003; SANS Institute 2007). Recent survey reports and anecdotal evidence vastly support the given argument. According to the CSI/FBI survey, 64 percent of the respondents reported that some of the information security-related loses that they have incurred is due to the insiders (CSI/FBI 2006).

In the extant literature, employees' computer abuse and misuse of IS resources are the major information security-related issues with regards to insiders. Hence, most of the earlier empirical studies conducted to investigate end-user behaviors assume that employees would have malicious

intents and intentionally involve in disruptive, unethical, or illegal behaviors. Therefore, often based on the general deterrence theory, these studies focus on the deterrent and preventive strategies (i.e. sanctions) for reducing IS misuse and computer abuse. For example, Straub and Nance (1990) investigate how to discover computer abuse and how to discipline perpetrators. To understand problems posed by an employee, Willison (2006) investigates the relationship between the offender and the context that he or she is in based on the rational choice and situational crime prevention theories. Lee and Lee (2002) empirically test the influence of organizational factors, information security policy and information awareness programs on prevention of computer abuse. Lee et al. (2003) analyze computer abuse considering the abuse of insiders and outsiders through assessing the role of deterrence and organizational factors.

An insider act can be malicious, neutral, or beneficial (Bottom 2000; Stanton et al. 2005). Among all security threats caused by the employees, malicious acts constitute the smallest fraction (CSI Survey 2007). We believe that the belief structures of insiders with or without malicious intentions are different. Hence, they should be distinctly identified and explicated. Furthermore, while the problems caused by naïve end-users can be deterred by persuasive communication and appropriate security training and awareness programs, intentional abuse and misuse cannot. Therefore, we limited our focus in this study to *insiders without any malicious intents* and their protection of information and technology resources.

Unlike studies arguing deterrence effects of negative reinforcement and sanctions, a few studies focus recently on beneficial acts of end-users with regards to information security and their actual compliance with the security requirements. Boss and Kirsch (2007) introduce the concept of *mandatoriness* which is shown to motivate individuals to take security precautions. The acts of specifying policies, evaluating behaviors, and computer self-efficacy were found to be effective in

convincing individuals that security policies are mandatory, however, reward was not found to be a significant factor to mandatoriness. Pahnila et al. (2007) propose a theoretical model to explain employees' IS security policy compliance. Information quality were found to have significant effect on actual IS policy compliance, threat appraisal and facilitating conditions were found to have significant effect on attitude towards compliance, whereas sanctions and rewards were not found to have significant effect on intention to comply and actual compliance with IS security policy respectively. Dinev et al. (2008) attempt to understand end user behavior towards protective information technologies, which is defined as computer technologies that protect data and systems from security related threats, and posit that cultural differences moderate the strength of the relationships in the behavioral model in the context of protective information technologies. Although West (2008) conceptually highlighted cost of compliance in employee's behavior, the causal relationships between cost of compliance and an employee's attitude towards compliance has not been empirically studied yet. Using insights gained from the literature, this study seeks to extend our understanding of employee's information security-related behaviors by proposing an integrative model to explicate the role of rationality-based beliefs on employee's compliance behavior with the information security-related rules and regulations of his/her organization.

Finally, despite the importance of information security awareness, we believe that there is still a lack of empirical studies analyzing its impacts on information security. Siponen (2000; 2001) conceptually analyze information security awareness and suggest methods to increase it based on various theoretical perspectives. A few conceptual studies (Furnell et al. 2002; Hentea 2005; Thomson and Solms 1998) highlight the importance of ISA education and training Additionally, Puhakainen (2006) proposes a design theory for improving IS end-user security behavior and ISA campaigns and training. Yet, to the best of our knowledge, direct and indirect roles of information security awareness

on an employee's compliance behavior have not been studied in the literature. Beyond showing the direct influence of the ISA on the employee's attitude towards compliance, we aim to extend our understanding of the antecedences of compliance by untangling the relationships between the ISA and an employee's perception of reinforcing factors and their rationality-based beliefs about compliance and non-compliance.

3. THEORETICAL FRAMEWORK

Based on the theory of planned behavior (TPB) (Fishbein and Ajzen 1975; Ajzen 1991), rational choice theory (von Neumann and Morgenstern 1944), and its specific applications in criminology -- theory of crime and punishment (Becker 1968) and theory of participation in illegitimate activities (Ehrlich 1973), we propose a research model that explains employee's intention to comply with the ISP. TPB constitutes the foundation of our research framework. Developed to explain and predict human behavior, TPB suggests that intentions to perform behaviors of different kinds can be predicted with high accuracy from attitudes toward the behavior, subjective norms, and perceived behavioral control; and these intentions together with perceptions of behavioral control, account for considerable variance in actual behavior (Ajzen 1991). Building on TPB, we expand our scope to understand how employee's attitude towards compliance with the ISP is influenced and formed. Based on rational choice theory (von Neumann and Morgenstern 1944), we posit that employee's beliefs about the rationality of compliance and non-compliance with the ISP are the antecedents of employee's attitude towards compliance behavior. Rational choice theory is a dominant paradigm in economics to explain individual, social and economic behaviors in various contexts. According to the theory, an individual determines how he/she should act by considering costs and benefits of different actions. In criminology, widely-accepted theory of crime and punishment suggests that a criminal maximizes his/her expected benefits from an illicit activity in excess of the expected cost of punishment (Becker 1973). Becker (1973, p.170) argues that the cost/benefit analysis of crime is "intended to be sufficiently general to cover all violations". Hence, cost/benefit analysis is not specific to crimes committed with malicious intent but is also applicable to violations without malicious intent. Theory of participation in illegitimate activities (Ehrlich 1973) extends theory of crime and punishment by not only considering costs and benefits of an illegitimate activity but also considering costs and benefits of

the corresponding legitimate pursuits. Drawing on the rational choice theory, theory of crime and punishment, and theory of participation in illegitimate activities, we argue that beliefs about the rationality of compliance and non-compliance significantly determine employee's attitude towards compliance behavior. Since we did not consider employees with malicious intent, based on the aforementioned theories, we identified three broad classes of beliefs about the rationality of compliance and non-compliance: *Benefit of Compliance*, *Cost of Non-Compliance* and *Cost of Compliance*. We posit that these three broad classes of employee's beliefs individually influence employee's attitude towards compliance.

Rational choice theory does not advocate that individuals would make the same decision when they face the same costs and benefits of an action. This is the major misperception about this theory stemming mainly from the misunderstanding of the concept of rationality. The "rationality" in the theory means that an individual choices the action by comparing costs and benefits of alternatives in accordance with his/her *stable* preference functions and constraints facing him/her. Accordingly, individuals might have different preference functions which might take different factors into consideration. For example, an individual might consider emotions or feelings as a part of his/her preference function while another individual might not. The key to the theory is the idea that an individual does not make decisions in an arbitrary manner. That is, under the same circumstances, an individual would not reach different decisions. Please note that our use of rational choice theory is limited to identification of broad classes of beliefs associated with the costs and benefits of compliance and non-compliance. We do not hypothesize to determine which of those beliefs based on rationality

perspective is more dominant than the others.[1] Our objective is to determine what the significant beliefs about the rationality of compliance and non-compliance are.

Among those three classes of beliefs about the rationality of compliance and non-compliance beliefs, concepts which are related to *Benefit of Compliance* and *Cost of Non-Compliance* have been discussed in information security literature. Particularly, studies based on general deterrence theory (Kankanhalli et al. 2003; Pahnila et al. 2007; Straub 1990) highlights sanctions as an inhibiting factor which reduces information security violations and hence improves information security while recent studies discuss rewards (Boss and Kirsch 2007; Pahnila et al. 2007) as a motivating factor which increases compliance with the rules and regulations and hence improve information security in the organizations. Although rewards and sanctions are relevant factors for individuals in their decision making with regards to compliance, in the information security context, based on the review of academic and professional information security literature, we identified six motivational factors that help employees form their beliefs about *Benefit of Compliance* and *Cost of Non-Compliance*: *Intrinsic Benefit*, *Safety of Resources, Rewards*, *Intrinsic Cost, Vulnerability of Resources,* and *Sanctions*. Based on Skinner's classification (Skinner and Holland 1961), the first three of these motivational factors are positive reinforcing factors and the last three of these motivational factors are negative reinforcing factors. Hence, we posit that *Intrinsic Benefit*, *Safety of Resources* and *Rewards* are positively associated with the *Benefit of Compliance*; and *Intrinsic Cost, Vulnerability of Resources*, and *Sanctions* are positively associated with the *Cost of Non-Compliance*. We believe that understanding motivational factors that help employees form their beliefs about *Benefit of Compliance*

[1] Although it is not our focus in this paper, prospect theory (Kahneman and Tversky 1979) could be used if we were to identify which dimension of employee's belief is more dominant in his/her decision making.

and *Cost of Non-Compliance* is important for organizations since they can manipulate those factors to reinforce desirable actions of employees, in our specific context, compliance.

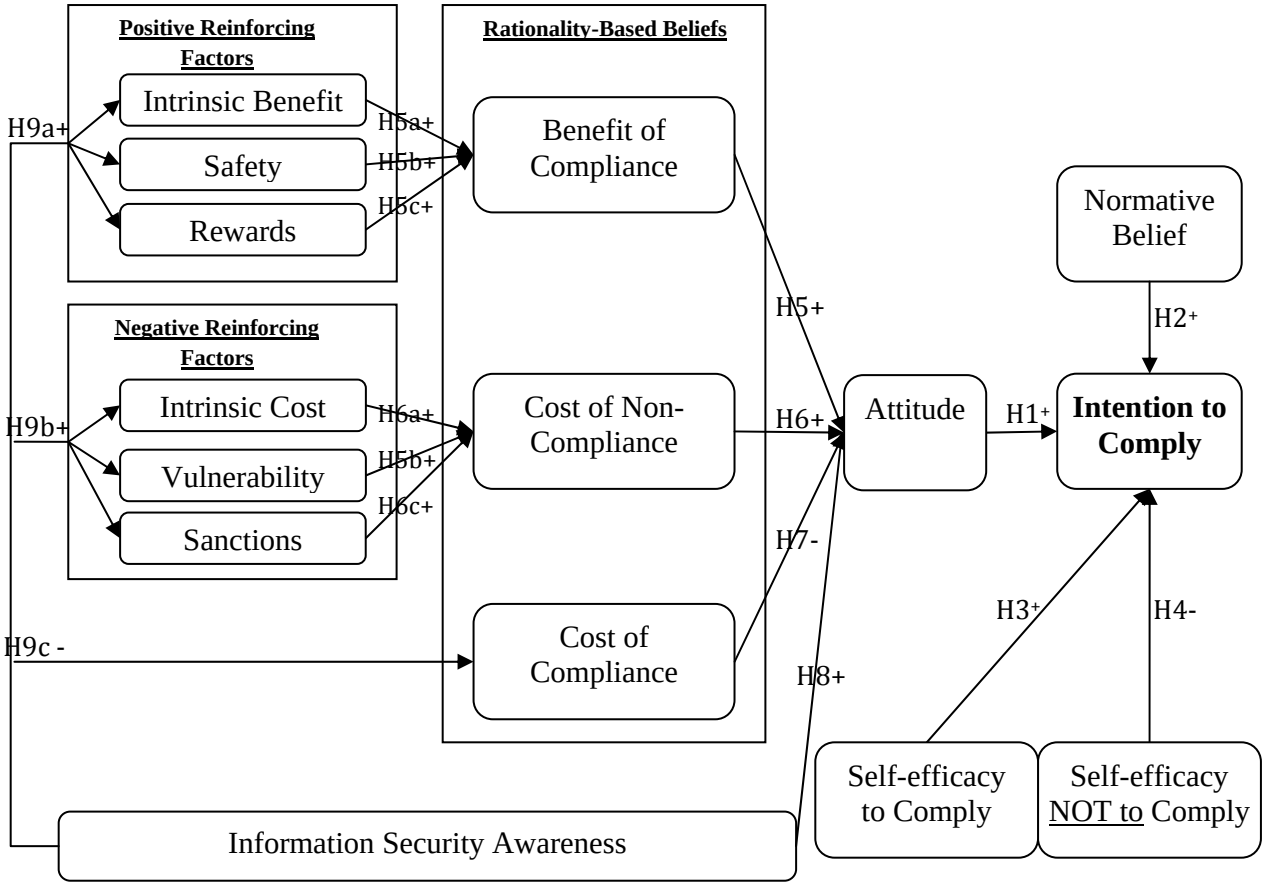
We are also interested in the role of information security awareness in employee's compliance with the ISP. The objective of creating information security awareness is to make employees aware of the information security-related risks and to educate them about their roles and responsibilities to ensure information security. Hence, we posit that information security awareness is positively associated with employee's attitude towards compliance with the ISP. However, we also believe that information security awareness influences how an employee perceives reinforcing factors and the *Cost of Compliance*. This is partly based on the Elaboration Likelihood Model (ELM) (Petty and Cacioppo 1986) which posits that a person's knowledge level, as well as motivation, will influence her engaging in more information processing about an issue (via the central route to persuasion) in attitude formation, rather than relying on peripheral cues.

4. RESEARCH MODEL AND HYPOTHESES

The proposed research model on an employee's ISP compliance behavior is based on the theory of planned behavior (Ajzen 1991). According to the theory, being an indication of an individual's readiness to perform a given behavior, behavioral intention is created by individual's attitude toward behavior, subjective norm, and perceived behavioral control. The behavior that we try to explain in this study is *an employee's compliance with the requirements of the ISP of his/her organization*. Therefore, in line with the TPB, we posit that an employee's intention to comply with the requirements of the ISP of his/her organization is associated with the employee's attitude towards compliance, Normative beliefs, and perceived behavior control which is operationalized in this study with two distinct constructs; namely, employee's *Self-Efficacy to Comply* with the ISP and employee's *Self-Efficacy Not to Comply* with the ISP. An employee's intention to comply with the requirements of the ISP is used as the dependent variable in this study since the TPB proposes that behavioral intention is the immediate antecedent of performing the behavior, and with perceived behavior control, accounts for considerable variance in the actual behavior. Hence, we believe that studying an employee's intention to comply with the ISP will provide insight about the actual compliance behavior. In the proposed research model, attitude towards complying with the ISP which represents the degree to which the performance of the behavior is positively or negatively valued is determined by three broad classes of beliefs about the rationality of compliance and non-compliance with the ISP: *Benefit of Compliance, Cost of Non-Compliance,* and *Cost of Compliance*. We postulate that these three broad classes of beliefs along with information security awareness influence employee's attitude towards compliance with the ISP. *Cost of Compliance* represents *direct (immediate)* consequences of complying with the ISP on the employee, whereas *Benefit of Compliance* and *Cost of Non-Compliance* represent *further* ramifications of complying or not complying with the ISP. Since *Benefit of*

Compliance and *Cost of Non-Compliance* cannot be directly observed by the individual we posit that *Benefit of Compliance* and *Cost of Non-Compliance* are formed by salient motivational beliefs that provide positive and negative reinforcing factors, respectively. Furthermore, we propose that information security awareness not only directly impacts employees' attitude, but also influences the salient reinforcing factors that form employee's beliefs about the *Benefit of Compliance* and *Cost of Non-Compliance* as well as employee's beliefs about *Cost of Compliance*. Hence, the model posits that information security awareness is not only directly influencing an employee's attitude towards compliance but mediated through the beliefs and reinforcing factors as well. Figure 1 presents our conceptual model. The following sections discuss operationalization of constructs and formation of our hypotheses.

Figure 4.1: Proposed Model of the Antecedents of ISP Compliance



4.1. Constructs from the Theory of Planned Behavior

Since our research model is based on TPB, we adopted constructs from TPB into our context of ISP compliance. Table 1 provides definitions of these constructs and their sources. Note that perceived self-efficacy is defined as individual's beliefs about his/her capability to produce a designated level of performance of a given behavior (Bandura 1977; 1994). Since compliance and non-compliance with the requirements of the ISP require different capabilities of the employee, we conceptualize perceived behavioral control with two distinct self-efficacy constructs that influence employee's intention to comply positively and negatively.

Table 4.1: Definitions and Sources of Constructs taken from the Theory of Planned Behavior

Construct	Definition	Sources
Attitude towards compliance with the ISP	An employee's positive feelings about complying with the requirements of the ISP of his/her organization.	Theory of Planned Behavior (Fishbein and Ajzen 1975; Ajzen 1991)
Normative Beliefs	An employee's perceived social pressure about his/her compliance with the requirements of the ISP caused by behavioral expectations of such important referents as executives, colleagues, managers.	Social Bond Theory (Hirschi 1969), Theory of Planned Behavior (Fishbein and Ajzen 1975; Ajzen 1991)
Self-Efficacy to Comply	An employee's judgment of his/her own skills, knowledge or competency about fulfilling the requirements of the ISP.	Social Cognitive Theory (Bandura 1977; 1994; 1997)
Self-Efficacy Not to Comply	An employee's judgment of his/her skills, knowledge, or competency about not complying with the requirements of the ISP without being detected.	Social Cognitive Theory (Bandura 1977; 1994; 1997)
Intention to Comply	An employee's intention to protect information and technology resources of his/her organization from potential security breaches.	Theory of Planned Behavior (Fishbein and Ajzen 1975; Ajzen 1991)

Based on the extant literature investigated relationships between TPB constructs, we form the following hypotheses in out context of ISP compliance:

Hypothesis 1. *An employee's attitude towards compliance with the organization's ISP positively influences his/her intention to comply with the requirements of the ISP.*

Hypothesis 2. *An employee's normative beliefs positively influence his/her intention to comply with the requirements of the ISP.*

Hypothesis 3. *An employee's self efficacy in complying with the requirements of the ISP positively influences his/her intention to comply with the requirements of the ISP.*

Hypothesis 4. *An employee's self efficacy in not complying with the requirements of the ISP negatively influences his/her intention to comply with the requirements of the ISP*.

4.2. Beliefs about Rationality of Compliance and Non-Compliance

The TPB argues that behavioral beliefs which represent subjective probability that the behavior will produce a given outcome influence individual's attitude towards behavior (Ajzen 1991). This study focuses on beliefs that an employee use to rationalize their compliance or non-compliance behavior. Drawing on rational choice theory (von Neumann and Morgenstern 1944), we define three broad classes of beliefs about the rationality of compliance and non-compliance: *Benefit of Compliance*, *Cost of Non-Compliance*, and *Cost of Compliance*. Although an employee directly form his/her belief about *Cost of Compliance*, we argue that positive and negative reinforcing factors are antecedents to beliefs about *Benefit of Compliance* and beliefs about *Cost of Non-Compliance*, respectively. The following subsections discuss these three constructs and their antecedents in case of *Benefit of Compliance* and *Cost of Non-Compliance*.

4.2.1. Perceived Benefit of Compliance

Perceived Benefit of Compliance is defined as the overall anticipated favorable return to an employee due to his/her compliance with the requirements of the ISP. In the context of ISP compliance, we identify that *Intrinsic Benefit*, *Safety of Resources*, and *Rewards*, referred as positive reinforcing factors, are antecedents of an employee's perception on the benefits of compliance. Since behavioral beliefs contribute to an individual's attitude in direct proportion to his/her subjective assessment of probability that the behavior produces the outcome in question (Ajzen 1991), we propose that an employee's perceived *Benefit of Compliance* will lead to positive attitude towards complying with the requirements of the ISP. Furthermore, since positive outcome reinforces the

perceived likelihood of the specific behavior (Skinner and Holland 1961), we believe that positive reinforcing factors help an employee form his/her belief about the benefits of compliance.

In our context, we define *Intrinsic Benefit* as an employee's positive feelings, such as satisfaction, accomplishment, and fulfillment about his/her compliance with the requirements of the ISP of his/her organization. (Deci and Ryan 1985) suggests that intrinsic motives help people feel free to make their own choices concerning their behavior (self determination) and justify their actions in terms of internal reasons such as their own inspirations. Similarly, we propose that *Intrinsic Benefit*s would help employees justify their actions about complying with the ISP by partially driving their perceptions on the *Benefit of Compliance*.

S*afety of Resources* is defined as an employee's perception that the safety of his/her information and technology resources at work are enhanced as a result of his/her compliance with the requirements of the ISP. We believe that employees are concerned with the safety of their information and technology resources at work. West (2008) argues that seeing that the security mechanisms are working and that the actions taken are actually making employees' resources safer is a reinforcing motivation for employees to comply with the requirements. Therefore, we posit that perceived safety of an employee's resources positively influences his/her perceptions on the benefits of compliance.

Rewards is defined as tangible or intangible compensations given to an employee by his/her organization in return for his/her compliance with the requirements of the ISP. The examples could be pay raises, monetary or non-monetary awards, personal mention and appreciation in oral or written assessment reports, promotions, and reputation. Although rewarding pro-security behaviors is not common in practice yet, Boss and Kirsch (2007) and Pahnila (2007) recently highlighted the importance of incentives in information security (Boss and Kirsch 2007; Pahnila 2007). Moreover, rewards as an incentive have been found as a significant mechanism to change behaviors in various

contexts in education, organizational behavior, and psychology. Hence, we believe that rewarding pro-security behavior would also contribute to an employee's perception on the benefits of compliance. Formally, we propose the following hypotheses in relations to benefits of compliance and its antecedences:

Hypothesis 5: An employee's perceived Benefit of Compliance will positively influence his/her attitude towards complying with the requirements of the ISP.

Hypothesis 5a: Intrinsic benefit that an employee obtains due to his/her compliance with the ISP is positively associated with his perception on the benefit of compliance.

Hypothesis 5b: Safety of resources at work which is obtained due to the employee's compliance with the ISP is positively associated with his/her perception on the benefits of compliance.

Hypothesis 5c: Rewards that an employee is given due his/her compliance with the ISP is positively associated with his perception on the benefit of compliance.

4.2.2. Perceived Cost of Non-Compliance

Perceived Cost of Non-Compliance is defined as the overall anticipated unfavorable consequences to an employee due to his/her non-compliance with the requirements of the ISP. Based on the TPB (Ajzen 1991), we propose that an employee's perceived *Cost of Non-Compliance* will lead to positive attitude towards complying with the requirements of the ISP. Furthermore, studies based on general deterrence theory (Kankanhalli et al. 2003; Pahnila et al. 2007; Straub 1990) highlight the importance of sanctions as a countermeasure to deter computer security-related crimes since sanctions can provide enough motivations to lead employees to believe that there is a cost associated with not adhering the security-related rules and regulation. However, a sanction, although it is important, is *not* the only

negatively reinforcing factor that helps employees form their beliefs about the cost of not adhering to the rules and regulations (Siponen 2000). In the context of ISP compliance, we identify that *Intrinsic Cost*, *Vulnerability of Resources*, and *Sanctions*, referred as negative reinforcing factors, are the antecedents of an employee's perceived *Cost of Non-Compliance*. Since negative outcome reinforces the likelihood of the specific behavior (Skinner and Holland 1961), we believe that negative reinforcing factors help an employee form his/her belief about the benefits of compliance.

In our context, *Intrinsic Cost* is defined as an employee's negative feelings such as stress, guilt, shame, and embarrassment due to his/her non-compliance with the ISP. Hence, we expect that an employee's *Intrinsic Cost* would influence his/her beliefs on the *Cost of Non-Compliance*.

Sanctions is defined as tangible or intangible penalties given to an employee, such as demotions, loss of reputation, reprimands, monetary or non-monetary penalties, personal mention in oral or written assessment reports, due to his/her non-compliance with the requirements of the ISP. A number of studies have focused specifically on the deterrent effects of sanctions (Straub 1990; Straub and Nance 1990; Straub and Welke 1998) to reduce the criminal behavior. Accordingly, we propose that sanctions reinforce an employee's belief about *Cost of Non-Compliance*.

Vulnerability of Resources is defined as an employee's perception that his/her information and technology resources at work are exposed to security-related risks and threats as a consequence of his/her non-compliance with the ISP. If an employee perceives that non-compliance creates vulnerabilities to his/her information and technology resources at work, he/she tends to believe that non-compliance is costly. Therefore, we posit that *Vulnerability of Resources* reinforces an employee's belief about *Cost of Non-Compliance*. Overall, we propose the following hypotheses:

<u>Hypothesis 6:</u> *An employee's perceived Cost of Non-Compliance will positively influence his/her attitude towards complying with the requirements of the ISP.*

Hypothesis 6a: *Intrinsic cost that an employee incurs due to his/her non-compliance with the ISP is positively associated with his/her perception on the Cost of Non-Compliance.*

Hypothesis 6b: *Perceived vulnerability of resources at work which is caused due to employee's non-compliance with the ISP is positively associated with his/her perception on the Cost of Non-Compliance.*

Hypothesis 6c: *Sanctions that an employee faces due his/her non-compliance with the ISP is positively associated with his/her perception on the Cost of Non-Compliance.*

4.2.3. Perceived Cost of Compliance

Perceived Cost of Compliance is defined as an employee's perception that compliance with the requirements of ISP is time consuming and hinders his/her work progress and/or personal productivity. The security precautions that the ISP requires an employee to take in order to ensure information security may lead to directly perceptible and often immediate negative consequences to the employee such as, inconveniences associated with complying and efforts required for complying. Employees desire to accomplish their tasks effectively and efficiently. Since pro-security behaviors which are expected from an employee require time and effort that could have been directed to business activities that the employee is supposed to conduct, an employee often sees compliance with the ISP as a barrier to progress of his/her work and his/her productivity. In some cases, security requirements may even conflict with the employee's primary tasks and result in sacrificing information security in return for accomplishing the primary tasks (Pahnila 2007). Moreover, the *Cost of Compliance* is usually real and immediate unlike the positive returns of compliance such as safety and rewards which are ambiguous and pending. Hence, time and effort required for compliance make it easy to ignore security requirements (Boss & Kirsch 2007). West (2008) also argues that employees tend to favor quick

decisions based on learned rules or heuristics since they have limited capacity for information processing and multitasking. Since security requirements often complicate the task, employees may not consider them while performing their tasks. Hence, employees "do what expedites their activity rather than what they know they ought" (PWC 2008). In line with theory of participation in illegitimate activities which emphasizes the importance of the allocation of limited resources (Ehrlich 1973), we believe that *Cost of Compliance* plays crucial role in influencing an employee's attitude towards compliance. Therefore, we hypothesize:

Hypothesis 7: An employee's perceived Cost of Compliance will negatively influence his/her attitude *towards complying with the requirements of the ISP.*

4.3. Information Security Awareness

Information security awareness refers to a state where employees in an organization are aware of and ideally committed to the security objectives of his/her organization (Siponen 2000). Security awareness of employees constitutes an important part of an effective information security management program (Cavusoglu et al. 2008). In this study, *Information Security Awareness* is defined as an employee's consciousness of information security and cognizance of the information security policy of his/her organization. *General Security Awareness* and *ISP Awareness* constitute the key dimensions of information security awareness. *General Information Security Awareness* is defined as an employee's overall knowledge and understanding of potential information security-related issues and their ramifications. An employee with general security awareness is likely to know how to deal with security related issues since he/she is aware of their significance. Beyond general information security awareness, organizations have specific expectations, which are reflected in the ISP, from their employees. *ISP Awareness* is defined as an employee's knowledge and understanding of the

requirements prescribed in the ISP of his/her organization and the objectives of these requirements. Fishbein and Ajzen (1975) suggest that one of the most effectual and recommended ways of producing a change in human beliefs is persuasive communication. Additionally, Siponen (2000) argues that provision of the organizational security awareness is the most important factor for persuading employees to change their compliance actions. Therefore, we posit that an employee's information security awareness results in positive attitude towards complying with the ISP. Further, we believe that information security awareness influences an employee's perception of positive and negative reinforcing factors, which are antecedents of employee's beliefs about *Benefit of Compliance* and beliefs about *Cost of Non-Compliance*, and beliefs about *Cost of Compliance*. Consequently, we propose following hypotheses:

Hypothesis 8: An employee's information security awareness will positively influence his/her attitude towards complying with the requirements of the ISP.

Hypothesis 9a: An employee's information security awareness is positively associated with his/her perception of factors positively reinforcing his/her beliefs.

Hypothesis 9b: An employee's information security awareness is positively associated with his/her perception of factors negatively reinforcing his/her beliefs.

Hypothesis 9c: An employee's information security awareness is negatively associated with his/her belief about Cost of Compliance.

5. RESEARCH METHODOLOGY

We used the survey method to test our model. We developed a survey instrument by identifying and creating appropriate measurements based on a comprehensive literature review. The initial survey instrument was refined based on card sorting exercises and exploratory data analysis of two small-scale pre-tests. Data was collected by administering the finalized survey instrument online. Details of processes that we followed are summarized below.

5.1. Item Development

The process of item development began with an investigation of previous theoretical and empirical literature. The measurement items of the constructs were developed based on the existing scales of the previous research. Whenever existing measures which successfully capture our conceptualization of information security-related constructs exist, they are adopted. If not, we adapted existing measures which are proven reliable and valid into our context of ISP compliance. Otherwise, new measures were developed by closely following our definitions of constructs in this study. Table 2 presents all the constructs, along with their types, their sources, and how many items that we used to measure them. Except for the intention to comply, all constructs were measured reflectively with multiple items on seven-point Likert scales. The anchors of the measurement items can be found at Appendix B. Both reflective and formative measurement items were developed for intention to comply construct, and the model was tested with two different types of measurement items.

Table 5.1: Sources of Measurement Constructs

Construct	Sub-Constructs	Type	Source	Items
Information Security Awareness		Reflective		
	General Security Awareness	Reflective	Developed for this study	4
	ISP Awareness	Reflective	Developed for this study	4
Perceived Benefit of Compliance		Reflective	Developed for this study	4
	Intrinsic Benefit	Reflective	Developed for this study	4
	Safety of Resources	Reflective	Developed for this study	6
	Rewards	Reflective	Boss and Kirsch, 2007	4
Cost of Compliance		Reflective	Developed for this study	4
Cost of Non-Compliance		Reflective	Developed for this study	4
	Intrinsic Cost	Reflective	Developed for this study	4
	Vulnerability of Resources	Reflective	Developed for this study	5
	Sanctions	Reflective	Boss and Kirsch, 2007	4
Attitude		Reflective	Ajzen, 1991	4
Normative Beliefs		Reflective	Ajzen, 1991	3
Self Efficacy to Comply		Reflective	Developed for this study	3
Self Efficacy Not to Comply		Reflective	Developed for this study	3
Intention to Comply		Reflective	Ajzen, 1991	3
		Formative	Developed for this study	16

5.2. Instrument Pretesting and Refinement

Discussions were held with several faculty members and graduate students who have experience in survey research methods in our organization and their feedback on initial measurement items was received. We also obtained feedback from the participants of an academic workshop held in our Faculty, where we presented our work. Based on the feedback, several items were reviewed and modified. Next, the initial set of items and the predefined categories were submitted for a card-sorting test (Moore and Benbasat 1991). Different set of graduate students who had work experience participated in the card sorting exercise. In general, the sorting resulted in satisfactory classification of items into predefined categories. Thus, the initial items were deemed appropriate and, hence, used in our pilot testing.

We first created an online questionnaire. 15 MBA students of our organization reviewed the online questionnaire. Based on their feedback on appearance of the online survey, we improved appearance of the online survey. The items and scales were then subjected to two rounds of pilot testing. The first pilot test was conducted with a small number of respondents (n = 110) drawn from panel members of professional research company we used in the main survey. 55 respondents completed the questionnaire for the first pilot-test, and commented on the wording, length, instructions, and reported concerns if they have any. The validity and reliability of the measurement items were investigated by using 27 participants without any missing answer. Based on our analysis of the data and the comments provided by the participants, the measurement items were further modified. After the revisions, we conducted another card sorting exercise with 6 participants. Based on the results, wording of some measurement items was modified in order to improve the clarity of items and to ensure that constructs are distinguishable. Subsequently, the second pilot test was conducted with another group of respondents (n = 147) once again drawn from panel members of professional research company. 71 respondents completed the questionnaire. 27 responses were discarded due to missing answers. Based on the analysis of data and feedback of participants, all the measurement items were deemed adequate, and ready to be used in the main survey.

5.3. Data Collection: Sample and Procedure

The proposed model presented in Figure 1 was tested using the items presented in Appendix B. We collected data by administering a web-based questionnaire survey. Since our target respondents are employees using IT resources of their organizations and have access to the Internet, a web-based survey is deemed appropriate. A professional market research company located in United States provided a nationwide sample of their panel members.

Several steps have been followed in order to ensure that participants using IT resources of their organizations are familiar with the ISP of their organizations. First, we asked the research company to choose the companies which have a clearly specified and written ISP, and employees who are aware of their company's ISP. Accordingly, the research company sent an invitation e-mail to 3,150 panel members by soliciting participation from panel members who are employed in organizations with a clearly specified and written ISP and who are aware of the ISP of their organizations. The identities of participants were kept confidential by the research company. In return for their participation, participants were provided a point-based incentive redeemable for various prizes. According to the statistics of the server hosting the online survey was 1,098 panel members accepted the invitation. Of all panel members who accepted the invitation, a total of 928 individuals opted to go on and participate to the survey by agreeing consent agreement. Those panel members then were first asked questions regarding demographics. Next, they were asked exclusion questions which can be found in Table 3 in Appendix A so that the data will not include those who work in organizations without an explicitly written ISP and who are unaware of the requirements of the ISP (among a 7 point likert scale, participants who selected completely unaware – 1, or unaware – 2). Those who met the exclusion criteria were not able to proceed with the survey. Thus, 258 of the participants were screened out from the survey at that point. Of all the remaining 670 responses, 175 were eliminated due to incompleteness, and 31 were eliminated due to data runs. Hence, sample of 464 usable questionnaires were included in the analysis, giving an effective response rate of 42%. A possible non-response bias was addressed by using the procedure recommended by Armstrong and Overton (1977). No significant differences has been found between the first third and the last third of the respondents' data, hence we concluded that non response bias is not a threat in this study.

In the final sample, 52% of the respondents were female, 36% were in the 36-45 age range. The average computer usage was 17.6 years, and the average usage of the Internet was 12.2 years. 28% of the respondents reported that they were working for information intensive companies. In terms of the responsibilities of the respondents as well as the annual sales revenue and size of their companies that they are working for, the sample was quite evenly distributed. Sample demographics are presented in Table 4 in Appendix A. We believe that data collected is representative of diverse employee population since it includes a variety of employees with different backgrounds and of organizations with various characteristics.

6. DATA ANALYSES AND RESULTS

6.1. Assessment of Measurement Validation

The measurement and the structural models were tested using structural equation modeling. The component based partial least squares (PLS) approach were used to evaluate the psychometric properties of measurement scales and to test research hypotheses proposed in this study. The PLS, as a component based approach, is preferred over the covariance based approach because it is considered to be more appropriate when formative indicators as well as reflective indicators are used to measure latent constructs within a research model (Chin 1998). For this study, the measurement model was tested using both the reflective and the formative measurement items of the dependent variable to compare the possible differences in results. Moreover, because the PLS focuses on prediction of data and is better suited for exploratory models and theory development, it is considered to be more adequate for this study. The Smart-PLS software package (version 2.0.M3) was used for the estimations. The measurement quality of reflective constructs was assessed by examining the convergent validity, individual item reliability, composite reliability, and discriminant validity of the measurement model (Barclay et al. 1995). Since the measures of all constructs had adequate reliability and validity assessments, all the measurement items of these constructs were kept for testing the structural model. Subsequently, we estimated the structural model and tested the research hypothesis.

First, to ensure the individual item reliability and convergent validity of constructs factor loadings of individual measures on their respective underlying constructs as well as the average variance extracted (AVE) were examined. All the measurement items loadings on respective constructs were above recommended minimum value of 0.707, indicating that at least 50 percent of the variance was shared with the construct (Chin 1998) (see Appendix B). Furthermore, the AVE values for all

reflective constructs were greater than the minimum recommended value of 0.50 (see Table 6 in Appendix C), validating that the items satisfies the convergent validity.

Second, to ensure the discriminant validity of constructs in the research model, the square root of average variance extracted (AVE) for each construct was compared with the other simple correlation scores in the correlation matrix. The square root of AVE for each construct in the model, as reported in the diagonal of the correlation of constructs matrix in Table 6 in Appendix C, is larger than the corresponding off-diagonal correlations of the construct to their latent variables. Additionally, confirmatory factor analysis was performed, and the cross loadings of the items on other constructs were examined. As recommended, all the measurement item loadings on the intended constructs were above 0.78, and at least 0.1 less on its loadings on other constructs (Gefen and Straub 2005) (See Table 7 in Appendix C).

Furthermore, to confirm the scale reliability and internal consistency of the constructs in the research model, the composite reliability (Fornell and Larcker 1981) and Chronbach's alpha scores were calculated. A composite reliability of 0.7 or greater is considered acceptable (Gefen et al. 2000; Nunnally and Bernstein 1994). As reported in Table 6, the composite reliability values for all the constructs in the research model are greater than 0.92 and Chronbach's alpha values are greater than 0.88, demonstrating that all constructs have adequate reliability assessment scores.

The formative measurement items do not necessarily correlate to each other because they are operationalized to create an emergent factor (Jarviset et al. 2003). Hence, the procedures used for the validation of the reflective measurement items do not apply to formative measurements (Chin 1998). Instead, the weight of an item used to measure a formative construct can be used to evaluate the extent to which the item contributes to the formation of its posited underlying factor (Chin 1998). Table 5 in Appendix B displays the questionnaire items as well as the descriptive statistics of all the constructs

including means and standard deviations, and the level of each item's contribution to the overall factor. The statistics and factor loadings of the formative constructs proposed for intention to comply variable can be found in that table.

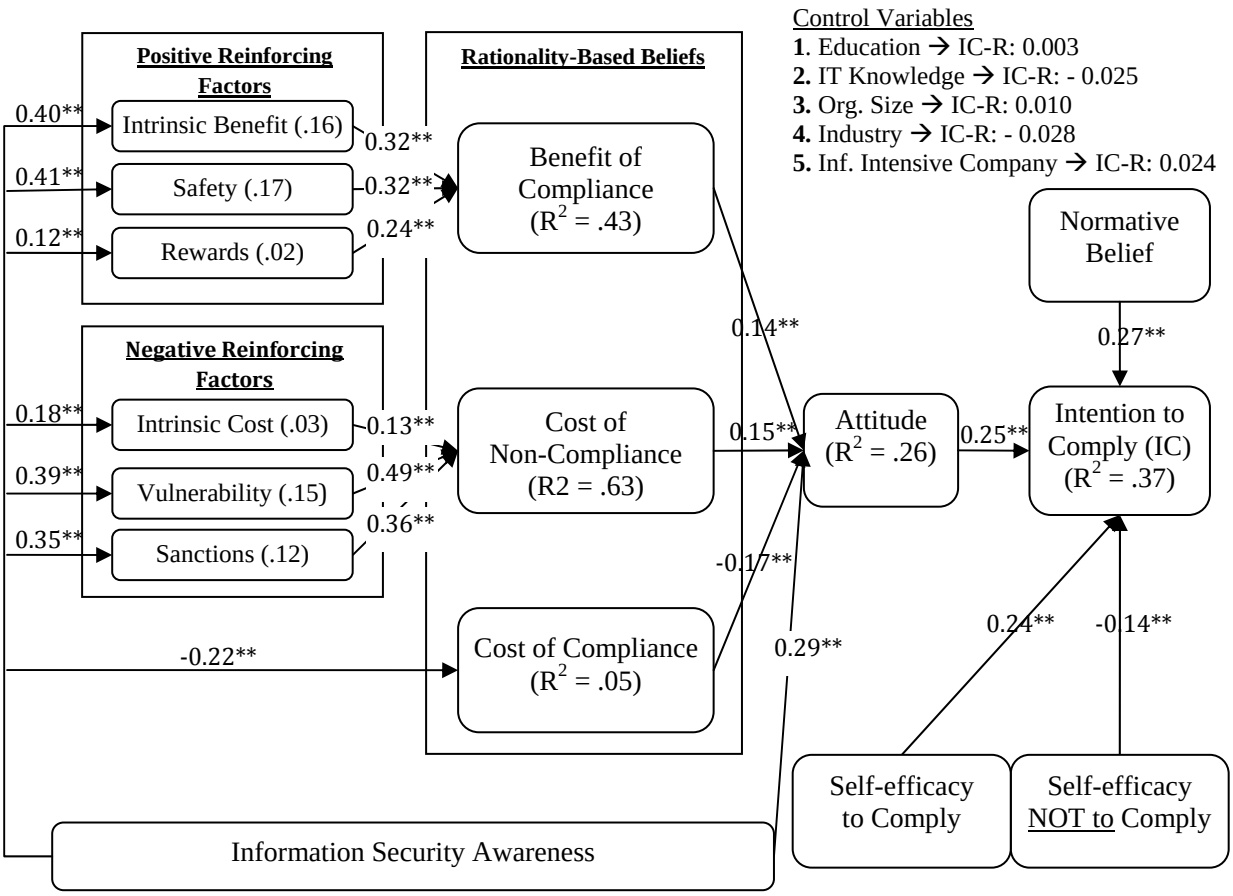
Lastly, we considered the Harman (1967) one-factor extraction test to see if common method bias is a potential concern. No single factor explained a majority of the variance, thus concluding that common method bias was not a threat to this study.

6.2. Structural Model Testing

The measurement of the structural model, as proposed in our research model, was estimated by using PLS approach to structural equation modeling. Bootstrapping resampling method with 464 samples was used for the estimation of the structural model. The results of the model estimation including standardized path coefficients, significance of the paths based on two-tailed t-test and the amount of variances explained (R^2) are presented in Figure 2.[2]

[2] The results presented in Figure 2 were obtained by using the reflective measurement items of Intention to Comply. Using the formative measurement items of the construct did not result in any significant difference in the measurement model.

Figure 6.1: The Results of the Structural Model Testing



* p < .05; ** p < .01 (two tail)

Based on the significant path coefficients (Figure 2), all hypotheses were supported (p<0.01). Approximately 37% of the variance is explained for the intention to comply. Since we conceptualized information security awareness as a second order construct formed from two sub-constructs, we looked at weights of sub-constructs used as indicators for the formative information security awareness construct. We found that weights are significant, suggesting that each sub-constructs significantly contributed to the underlying overall factor.

7. DISCUSSIONS, IMPLICATIONS, AND FUTURE RESEARCH

7.1. Discussion of the Findings

This study identifies three broad classes of rationality-based beliefs – benefit of compliance, cost of non-compliance, and cost of compliance – to provide theoretical explanations for antecedences of an employee's attitude towards compliance with the ISP, which positively influences his/her intention to comply with the ISP. Furthermore, the direct impact of an employee's information security awareness, which is hypothesized to be formed by his/her general security awareness and ISP awareness, on the employee's attitude to comply with the ISP as well as its indirect impact on the rationality-based beliefs was investigated. Overall, we found strong empirical support for our theoretical model that explains the antecedents of ISP compliance, with the emphasis placed on the influences of three distinct rationality-based beliefs and information security awareness. All the hypotheses were supported based on data collected from 464 employees who had some familiarity with the requirements of the ISP of their organizations.

As hypothesized, we found significant evidence regarding the effect of attitude, normative beliefs, self-efficacy to comply and self-efficacy not to comply on an employee's intention to comply, explaining 36.6 % of the variance of the construct. Thus, hypotheses 1, 2, 3, and 4 were fully supported. In addition to the significant positive contributions of the constructs adopted from theory of planned behavior, our analysis suggests that an employee's capacity for not complying (i.e., self-efficacy not to comply) has a significant negative impact on his/her intention to comply. This result extends literature on information security which solely focused on the positive impact of self-efficacy on intention by highlighting importance of the negative impact of self-efficacy.

Consistent with the proposed research model, we showed that three broad dimensions of rationality-based beliefs exert significant influences on an employee's positive attitude towards compliance and explain 25.6 % of the variance of the construct. Hence, hypotheses 5, 6, and 7 were fully supported. Our findings indicate that rationality-based beliefs almost evenly influence an employee's attitude towards compliance, suggesting that no single belief is predominant on attitude. Furthermore, the reinforcing factors which were postulated to constitute the rationality-based beliefs were found to exert strong influence on the level of their pertinent constructs. Among the three positive reinforcing factors, intrinsic benefit and safety of resources were found to have a larger influence on an employee's perception of benefit of compliance. Similarly, among the three negative reinforcing factors, vulnerability of resources has the largest influence on cost of non-compliance. However, unlike the intrinsic positive reinforcing factor, the intrinsic negative reinforcing factor (intrinsic cost) was found to have the weakest influence on an employee's perception of cost of non-compliance.

Furthermore, we found that an employee's information security awareness not only have a direct significant influence on his/her attitude towards compliance, but also plays a major role in shaping perception of reinforcing factors and rationality-based beliefs. Strikingly, an employee's information security awareness has the largest influence on his/her attitude towards compliance, confirming the existing literature that highlights the importance of information security awareness. We showed that information security awareness positively influences an employee's perception of six reinforcing factors helping him/her form his/her beliefs about benefit of compliance and cost of non-compliance and negatively influences his/her belief about the cost of compliance. Thus, as hypothesized, we concluded that information security awareness systematically influences attitude, perceived positive and negative reinforcing factors as well as cost of compliance.

Although we controlled for employee's level of education and his/her technology knowledge, the size and the industry type of the organization he/she works , and how information intensive his/her organization is, we did not found any significant impact of control variables on employee's intention to comply with the ISP. Interestingly, industry type has also no significant impact on explaining employee's intention on compliance. Although some industries such as financial sector are known to be more vulnerable to security-related crimes (Schneier 2005), our results suggest that the compliance behaviour can be better explained by factors rooted in our theoretical reasoning (rationality beliefs and ISA) rather than whether the organization operates in a particular industry or not.

7.2. Theoretical Contributions and Practical Implications

Our study makes important contributions to the emerging body of knowledge on the behavioral and organizational issues of information security. First, this, to the best of our knowledge, is the first study offering a theoretical explanation, along with empirical support, to investigate the impact of an employee's rationality-based beliefs about compliance and non-compliance with the ISP on his/her attitude towards compliance with the ISP. Second, while the extant literature discussed the roles of rewards and sanctions, which are the notions relevant to benefit of compliance and cost of non-compliance in our conceptualization, in compliance behaviour, this study is the first one to empirically investigate the role of cost of compliance in compliance behaviour. Although rationality-based beliefs are shown to exert comparable influence on attitude, the impact of cost of compliance is higher than that of benefit of compliance and that of cost of non-compliance; highlighting the importance of the construct in the context of information security. Therefore, as a practical implication, one might argue that organizations should simplify procedures of compliance and provide training to their employees so that employees will not perceive requirements and procedures dictated by the ISP as burdensome.

Third, supplementary to the existing literature whose focuses are confined to mainly sanctions and recently rewards, our study identifies six reinforcing factors, including rewards and sanctions. Of those, intrinsic benefit, safety of resources, and rewards are positive reinforcing factors exerting positive influence on an employee's perception of benefit of compliance and intrinsic cost, vulnerability of resources, and sanctions are negative reinforcing factors exerting positive influence on an employee's perception of cost of non-compliance. Consequently, the results suggest that factors that provide positive or negative reinforcement about compliance extend beyond sanctions and rewards.

Furthermore, among the proposed reinforcing factors all of which found significant, intrinsic benefit and safety exert more impact on an employee's belief about benefit of compliance than rewards. Likewise, vulnerability exerts more impact on an employee's belief about cost of non-compliance than sanctions. Our findings suggest that other motivational factors can be as effective mechanisms as sanctions and rewards to reinforce an employee's compliance behaviour. Since reinforcing factors play an important role in shaping an employee's rationality-based beliefs that are showed to positively influence his/her attitude towards compliance, one would suggest that information security awareness programs should be designed to emphasize these reinforcing factors. Unlike Boss and Kirsch (2007) who found that rewards do not significantly contribute to the mandatoriness of ISP compliance, we found that rewards exert a significant impact on an employee's perception of benefit of compliance. While found significant, rewards' influence on the benefit of compliance was lower than the other positive reinforcing factors. Based on our results, we believe that employees should know that they will be rewarded for their pro-security behaviors.

Fourth, this study identifies two types of self-efficacy: self-efficacy to comply and self-efficacy not to comply. As one might expect, an employee's self-efficacy about compliance positively influence

his/her intention to comply. As a practical implication, this finding suggests that organizations should provide training to their employees about what they need to do in order to comply with information security rules and regulations so that employees would have capacity to comply with them. We also found that an employee's self-efficacy about non-compliance exerts a significant negative influence on his/her intention to comply. This is a new and interesting finding. It suggests that if employees are capable of not complying with the requirements without being detected, they may have a lower intention to comply with the rules and regulations. Thus, as a practical implication, organizations must be cautious about these employees who are capable of violating the requirements of ISP without being noticed and possibly consider taking extra precautions to prevent their actions.

Finally, our study is, to our best knowledge, the first one study that investigates the role of information security awareness on shaping an employee's perceptions of rationality-based factors and beliefs. Our study shows that information security awareness exerts a significant positive influence on the reinforcing factors and negative influence on cost of compliance. Since cost of compliance has not been studied, this study is the first study that empirically shows that an employee's belief about cost of compliance can be reduced by information security awareness. Our findings indicate that an employee's belief sets about compliance with the ISP can be directly and indirectly altered by ensuring their awareness of information security. As an important practical implication of results, we strongly suggest that organizations should create a security-aware culture within the organization in order to improve information security. In short, our results suggest that organizations should seriously contemplate the ways of creating the security aware culture. We suggest that they should start to create appropriate training and security awareness programs which ensure information security awareness of employees as well as their self-efficacy about compliance.

7.3. Limitations of the Study

This study is not without limitations. One limitation relates to the selection of participants for this study. In the beginning of the survey questionnaire respondents were asked whether their organization had provided an established ISP and whether they were aware of the requirements of the ISP. The participants who were not aware of the ISP of their organizations were excluded from participation in the survey. The selection of information security aware participants could have created a favorability bias in the responses. However, the investigation of this study would be impracticable with participants who were completely unaware of the requirements of the ISP. Furthermore, to tease out the impact of awareness, we captured the degree of participants' perceived general information security awareness as well as ISP awareness in the survey.

Another limitation of the study is the potential common method bias that may cause by collecting data from a single respondent through survey questionnaires at a time with the self-report method. Common method variance may inflate the relationship between predictor and criterion variables. However, statistical presence of the common method bias was not found through the application of statistical and procedural remedies. We applied Harman's one factor test (1967) and performed an exploratory factor analysis with all the items of our research model. No single factor explained a majority of the variance, thus suggesting that any potential common method bias was not a serious threat to this study.

7.4. Future Research Directions

Our study highlights the importance of an employee's rationality-based beliefs and his/her information security awareness in shaping his/her attitude towards compliance. One possible research direction is to investigate whether the employee's other beliefs can play a role in shaping his/her

attitude towards compliance. If other beliefs are significantly identified, they can be compared to the rationality-based beliefs in terms of their contribution to the employee's attitude. Another fruitful future research direction is to better understand information security awareness as we found that information security awareness plays a crucial role in employee compliance behaviour. In particular, we believe that the identification of the factors leading the information security awareness would be an important contribution to academics since there is a gap in the literature in this direction, and to practitioners since they can use those factors to formulate their information security awareness programs.

REFERENCES

Ajzen, I. 1991. "The theory of planned behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.

Armstrong, S. J., & Overton, T. S. 1977. "Estimating nonresponse bias in mail surveys," *Journal of Marketing Research* (14:3), pp. 396-402.

Bandura, A. 1992. "Self-efficacy," in *Encyclopedia of human behavior,* V. S. Ramachaudran (Ed.), New York: Academic Press, Vol. 4, pp. 71-81.

Bandura, A. 1997. *Self-efficacy: The exercise of control,* New York: W. H. Freeman.

Bandura, A. 1977. "Self-efficacy: Toward a unifying theory of behavioral change," *Psychological Review* (84), pp. 191-215.

Barclay, D., Higgins, C., & Thompson, R. 1995. "The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration," *Technology Studies* (2:2), pp. 285-309.

Becker, G. S. 1968. "Crime and Punishment: And Economic Approach," *The Journal of Political Economy* (76:2), pp. 169-217.

Boss, S. R., & Kirsch, L. J. 2007. "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guideliness," in *International Conference on Information Systems*, Montreal, pp. 1-18.

Bottom, N. R. 2000. "The human face of information loss," *Security Management* (44:6), pp. 50-56.

Brancheau, J. C., Janz, B. D., & Wetherbe, J. C. 1996. "Key issues in information systems management: 1994-95 SIM Delphi results," *MIS Quarterly* (20:2), pp. 225-242.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. 2004. "Economics of IT Security Management: Four Improvements to Current Security Practices," *Communications of the Association for Information Systems* (14), pp. 65-75.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. 2008. "Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers," *UBC Working Paper*.

Cavusoglu, H., Mishra, B., & Raghunathan, S. 2004. "A Model for Evaluating IT Security Investments," *Communications of the ACM* (47:7), pp. 87-92.

Cavusoglu, H., Mishra, B., & Raghunathan, S. 2004. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce* (9:1), pp. 69-104.

Chin, W. W. 1998. "Issues and Opinion on Structural Equation Modeling," *MIS Quarterly (*22:1), pp. vii-xvi.

Computer Security Institute. 2006. "CSI/FBI Computer Crime and Security Survey," May 11, 2007 (http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf).

CSI Survey. 2007. "The 12th Annual Computer Crime and Security Survey," Computer Security Institute, May 11, 2008 (http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf).

CSO Magazine. 2006. "E-Crime Watch Survey," 2006 eCrime Watch Survey, January 11, 2007 (http://www.cert.org/archive/pdf/ecrimesurvey06.pdf).

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

Deloitte. 2005. "Global security survey," *Deloitte Touche Tohmatsu* .

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

Dinev, T., Goo, J., Hu, Q., & Nam, K. 2008 "User behaviour towards protective information technologies: the role of national cultural differences," *Info Systems Journal*, January

Doherty, N. F., & Fulford, H. 2006. "Aligning the information security policy with the strategic information systems plan," *Computers and Security* (25:1), pp. 55-63.

Ehrlich, I. 1973. "Participation in Illegitimate Activities: A Theoretical and Empirical Investigation," *The Journal of Political Economy* (81:3), pp. 521-565.

Ernst & Young. 2005. "Global information security survey 2005: Report on the widening gap," *Ernst & Young* .

Fishbein, M., & Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research,* MA: Addison-Wesley.

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

Furnell, S. M., Gennatou, M., & Dowland, P. S. 2002. "A prototype tool for information security awareness and training," *Logistics information management* (15:5), pp. 352-357.

Gefen, D., & Straub, D. 2005. “A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example,” *Communications of the Association for Information Systems* (16), pp. 91-109.

Gefen, D., Straub, D. W., & Boudreau, M.-C. 2000. “Structural Equation Modeling And Regression: Guidelines For Research Practice,” *Communications of The AIS* (4), pp. 1-77.

Harman, H. H. 1967. *Modern Factor Analysis*, Chicago: University of Chicago Press.

Hentea, M. 2005. “A Perspective on Achieving Information Security Awareness,” in *The Information Universe: Issues in Informing Science and Information*, E. Cohen (Ed.), Informing Science Institute, Vol. 2, pp. 169-178.

Hirschi, T. 1969. *Causes of Delinquency*, Berkeley, CA: University of California Press.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. 2003. “A critical review of construct indicators and measurement model misspecification in marketing and consumer research,” *Journal of Consumer Research* (30:2), pp. 199-218.

Kahneman, D., & Tversky, A. 1979. “Prospect Theory: An Analysis of Decision under Risk,” *Econometrica* (47:2), pp. 263-292.

Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K.-K. 2003. “An integrative study of information systems security effectiveness,” *International Journal of Information Management* (23:2), pp. 139–154.

Lee, J., & Lee, Y. 2002. “A holistic model of computer abuse within organizations,” *Information management & computer security* (10:2/3), pp. 57-63.

Lee, S. M., Lee, S. G., & Yoo, S. 2003. “An integrative model of computer abuse based on social control and general deterrence theories,” *Information & Management* (41:6), pp. 707-718.

Lohmeyer, D. F., McCrory, J., & Pogreb, S. 2002. “Managing Information Security,” *The McKinsey Quarterly, Special Edition: Risk and Resilience* (2), pp. 12-16.

Mitnick, K. D., & Simon, W. L. 2002. *The art of deception: Controlling the human element of security*, Indianapolis, IN: Wiley.

Moore, G. C., & Benbasat, I. 1991. “Development of an instrument to measure the perceptions of adopting an information technology innovation,” *Information Systems Research* (*2*:3), pp. 192-222.

Neumann, P. G. 1999. “Risks of Insiders,” *Comunications of the ACM* , (42:12), pp. 160.

Nunnally, J. C., & Bernstein, I. 1994. *Psychometric Theory* (3rd edition ed.), New York: McGraw Hill.

Pahnila, S., Siponen, M., & Mahmood, A. 2007. "Employees' Behavior towards IS Security Policy Compliance," in *Proceedings of the 40th Hawaii International Conference on System Sciences*, IEEE, p. 156-166

Peltier, T. R. 2005. "Implementing an Information Security Awareness Program," *The EDP Audit, Control, and Security Newsletter*, pp. 1-18.

Petty, R. E., & Cacioppo, J. T. 1986. *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*, New York: Springer-Verlag.

PricewaterhouseCoopers. 2008. "Employee behaviour key to improving information security, new survey finds," June 23, 2008 (http://www.ukmediacentre.pwc.com/Content/Detail.asp?ReleaseID=2672&NewsAreaID=2).

Puhakainen, P. 2006. "A Design Theory for Information Security Awareness," *Faculty of Science, University of Oulu*.

Ransbotham, S., & Mitra, S. 2008. "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Forthcoming in Information Systems Research*.

Ringle, C. M., Wende, S., & Will, A. 2005. SmartPLS. (2.0 (beta)). Hamburg, Germany, (http://www.smartpls.de).

SANS Institute. 2007. "Understanding the Importance of and Implementing Internal Security Measures," March 11, 2007, (https://www2.sans.org/reading_room/whitepapers/policyissues/1901.php).

Schneier, B. (2005). *Attack Trends: Beyond the Numbers*, Counterpane Internet Security Inc.

Siponen, M. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management and Computer Security* (8:1), pp. 31-41.

Siponen, M. 2005. "An analysis of the traditional IS security approaches: implications for research and practice," *European Journal of Information Systems* (14:3), pp. 303-315.

Siponen, M. 2001. "Five Dimensions of Information Security Awareness," *Computers and Society* (31:2), pp. 24-29.

Siponen, M., & Iivari, J. 2006. "Six Design Theories for IS Security Policies and Guidelines," *Journal of the Association for Information Systems* (7:7), pp. 445-472.

Skinner, B. F., & Holland, J. G. 1961. *The Analysis of Behavior: A Program for Self-Instruction*, McGraw-Hill College.

Soo Hoo, K. J. 2000. “How much is enough: a risk management approach to computer security,” *Working Paper*, Stanford, CA, USA: Stanford University.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. 2004. “Analysis of end user security behaviors,” *Computers & Security* (24:2), pp. 124-133.

Straub, D. W. 1998. “Coping with Systems Risk: Security Planning Models for Management Decision Making,” *MIS Quarterly* (22:4), pp. 441-469.

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

Straub, D. W., & Nance, W. D. 1990. “Discovering and disciplining computer abuse in organizations: a field study,” *MIS Quarterly* (14:1), pp. 45-60.

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

Thomson, M. E., & Solms, R. v. 1998. “Information security awareness: educating your users effectively,” *Information management & computer security* (6:4), pp. 167-173.

von Neumann, J., & Morgenstern, O. (1944). *Theory of Games and Economic Behavior*. NJ: Princeton University Press.

West, R. 2008. “The Psychology of Security,” *Communications of the ACM* (51:4), pp. 34-40.

Whitman, M. E., Townsend, A. M., & Aalberts, R. J. 2001. “Information systems security and the need for policy,” in *Information Security Management - Global Challenges in the Next Millennium*, G. Dhillon, London: Idea Group, pp. 9-18.

Willison, R. 2006. “Understanding the Perpetration of Employee Computer Crime in the Organisational Context,” *Information and organization* (16:4), pp. 304-324.

Woon, I. M., & Kankanhalli, A. 2003. “Measuring Factors that Infleunce Information Security Effectiveness in Organizations,” in *Proceedings of the Thirteenth Annual Workshop on Information Technologies and Systems*, Seattle, Washington: WITS, pp. 19-24.

APPENDICES

APPENDIX A: Sample Demographics

Table 0.1: Exclusion Criteria

	Frequency	Percentage
Has your employer established Information Security Policies?		
Yes	464	100
No	0	0
To what extent are you aware of the regulations prescribed by the Information Security Policy (ISP) of your organization?		
1 (Completely Unaware)	0	0
2	0	0
3	50	11
4	87	19
5	101	22
6	114	24
7 (Completely Aware)	112	24

Table 0.2: Profiles of Responding Participants

	Frequency	Percentage
Gender		
Men	221	48
Women	243	52
Highest Level of Education		
Less than high school	1	0
High school degree	114	25
College degree	106	23
Undergraduate degree	100	21
Graduate degree	117	25
Other	26	6
Age		
20-25	11	2
26-35	159	34
36-45	169	36
46-55	93	20
56-65	30	7
66-75	0	0
76-85	2	1

	Frequency	Percentage
Knowledge of computers and IT of the Participant		
1 (Very Low)	1	0
2	7	2
3	41	9
4	84	18
5	171	37
6	104	22
7 (Very High)	56	12
Size of the Company (# of employees)		
Fewer than 500	100	21
500-999	47	10
1000 – 4,999	100	22
5,000-10,000	70	15
More than 10,000	147	32
Annual Sales Revenue of the Company		
Less than 1 million	79	17
1 million-5 million	54	12
5 million-10 million	49	10
10 million-50 million	46	10
50 million-200 million	50	11
200 million-500 million	26	6
500 million -1 billion	37	8
1 billion – 5 billion	63	13
More than 5 billion	60	13
Information Intensiveness of the Company		
1 (Not information intensive at all)	37	8
2	25	5
3	28	6
4	78	17
5	79	17
6	86	19
7 (Highly information intensive)	131	28
Industry		
Education	63	14
Financial Services	45	10
Government	52	11
Food/Beverage/CPG	10	2
Heath Care	64	14
Manufacturing	33	7
Non-Profit	23	5
Medical, Bio-Technology, Pharmacology	8	2
Real Estate	4	1
Services	13	3

	Frequency	Percentage
Information Technology	16	3
Telecommunications	9	2
Travel	11	2
Wholesale/Retail	34	7
Other	79	17
	Mean	**STD**
Years of computer usage	17.60	6.46
Years of Internet usage	12.16	4.11
Hours of computer usage per day for work	7.06	6.56
Years of working time for the company	7.73	7.63
Years of working time in the current position in the company	4.71	5.14

APPENDIX B: Measurement Items

Table 0.3: Measurement Items and Item Loadings

Items	Dimensions/ Questions	Scale	Mean	STD	Loading
IC - F	**Intention to comply *with ISP – General Questions on Resources (Formative)***				
	I intend to comply with the requirements of the ISP in regards to protection of the _____ of my organization.				
	computing resources	a	6.390	1.058	0.895
	software resources	a	6.371	1.102	0.890
	data and information resources	a	6.478	0.997	0.907
	Internet resources	a	6.231	1.183	0.839
	network resources	a	6.416	1.032	0.898
	electronic communications	a	6.356	1.048	0.880
	private, strategic and sensitive information	a	6.593	0.922	0.862
	trade secrets	a	6.504	1.123	0.794
IC - F	**Intention to comply *with ISP – Technical Questions (Formative)***				
	I intend to comply with the requirements of the ISP by _____to protect the resources of my organization.				
	appropriately selecting and updating passwords	a	6.412	1.076	0.820
	using and updating anti-virus software	a	6.425	1.099	0.758
	adhering to the rules of remote access to internal networks	a	6.485	1.005	0.886
	alerting security personnel when I find out potential security threats	a	6.472	1.005	0.878
	getting rid of viruses or spyware or getting help from other if necessary	a	6.491	1.027	0.835
	learning the skills and methods to protecting my information system	a	6.433	1.001	0.860
	updating security patches to software resources	a	6.379	1.145	0.796
	paying attention to the physical security of resources	a	6.450	0.980	0.854
IC - R	**Intention to comply *with ISP (Reflective)***				
	I intend to comply with the requirements of the ISP of my organization in the future.	a	6.532	0.915	0.974
	I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future.	a	6.573	0.908	0.975
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future.	a	6.550	0.926	0.982

Items	Dimensions/ Questions	Scale	Mean	STD	Loading
GSA	***General Information security awareness***				
	Overall, I am aware of the potential security threats and their negative consequences.	b	6.106	1.062	0.898
	I have sufficient knowledge about the cost of potential security problems.	b	5.739	1.370	0.838
	I understand the concerns regarding information security and the risks they pose in general.	b	6.304	0.962	0.851
	I know how to identify and respond to security threats in general.	b	5.716	1.232	0.868
ISPA	***ISP Awareness***				
	I know the rules and regulations prescribed by the ISP of my organization.	b	5.890	1.130	0.930
	I understand the objectives of the rules and regulations prescribed by the ISP of my organization.	b	6.000	1.100	0.917
	I have received adequate training about the ISP of my organization.	b	5.441	1.568	0.880
	I know my responsibilities as prescribed in the ISP to enhance the IS security of my organization.	b	5.718	1.355	0.939
A	**Attitude**				
	To me, complying with the requirements of the ISP is _____.				
	unnecessary .....……necessary	c	6.278	1.132	0.891
	unbeneficial ..... beneficial	c	6.131	1.275	0.935
	unimportant ..... important	c	6.246	1.269	0.928
	useless ..... useful	c	6.054	1.397	0.924
NB	**Normative Beliefs**				
	_____ think that I should comply with the requirements of the ISP.				
	My colleagues	a	5.966	1.358	0.851
	My executives	a	6.457	1.055	0.927
	My managers	a	6.351	1.183	0.945
SE-NC	**Self Efficacy Not to Comply**				
	If I wanted <u>not to comply</u> with the requirements of the ISP, I have the necessary _____ to do so without being detected.				
	skills	d	3.528	1.982	0.980
	knowledge	d	3.599	1.971	0.988
	competencies	d	3.612	1.985	0.981

Items	Dimensions/ Questions	Scale	Mean	STD	Loading
SE-C	**Self Efficacy to Comply**				
	I have the necessary _____ to fulfill the requirements of the ISP.				
	skills	d	5.987	1.170	0.969
	knowledge	d	5.955	1.181	0.977
	competencies	d	6.002	1.143	0.974
CC	**Perceived Cost of Compliance**				
	Complying with the requirements of the ISP _____.				
	holds me back from doing my actual work	b	2.655	1.776	0.961
	slows down my response time to my colleagues, customers, managers etc.	b	2.745	1.798	0.954
	hinders my productivity at work	b	2.692	1.794	0.971
	impedes my efficiency at work	b	2.733	1.812	0.971
IB	**Intrinsic Benefit**				
	My compliance with the requirements of the ISP would make me feel _____.				
	content	b	5.530	1.437	0.945
	satisfied	b	5.558	1.452	0.959
	accomplished	b	5.455	1.544	0.958
	fulfilled	b	5.291	1.595	0.937
R	**Rewards**				
	_____ I comply with the requirements of the ISP.	b			
	My pay raises and/or promotions depend on whether	b	3.093	2.053	0.873
	I will receive personal mention in oral or written assessment reports if	b	2.847	2.017	0.910
	I will be given monetary or non-monetary rewards if	b	2.364	1.909	0.906
	My receiving tangible or intangible rewards are tied to whether	b	2.504	1.923	0.924
SR	**Safety of Resources**				
	Complying with the requirements of the ISP _____ my resources at work.				
	would strengthen the security controls over	b	5.259	1.650	0.869
	would enhance safety of	b	5.478	1.531	0.926
	would improve protection of	b	5.532	1.551	0.936
	would eliminate the risk of damage to	b	5.409	1.590	0.919
	would prevent potential security related risks concerning	b	5.616	1.459	0.929
	would lead to less security related problems associated with	b	5.509	1.532	0.922

Items	Dimensions/ Questions	Scale	Mean	STD	Loading
BC	Perceived Benefit of Compliance				
	My compliance with the requirements of the ISP would _____.				
	be favorable to me.	b	5.435	1.687	0.830
	result in benefits to me.	b	4.858	1.921	0.934
	create advantages for me.	b	4.647	1.965	0.952
	provide gains to me.	b	4.522	1.969	0.932
IC	Intrinsic Cost				
	Even if it won't be noticed, my non-compliance with the requirements of the ISP would make me feel _____.				
	guilty	b	5.073	2.068	0.947
	ashamed	b	4.728	2.117	0.975
	embarrassed	b	4.703	2.152	0.963
	stressed	b	4.849	2.104	0.957
S	Sanctions				
	_____ I don't comply with the requirements of the ISP.				
	I will probably be punished or demoted if	b	5.114	1.780	0.906
	I will receive personal reprimand in oral or written assessment reports if	b	5.125	1.823	0.906
	I will be incur monetary or non-monetary penalties if	b	3.657	2.266	0.785
	My facing tangible or intangible sanctions are tied to whether	b	4.446	2.104	0.899
VR	Vulnerability of Resources				
	If I don't comply with the requirements of the ISP, my resources _____.				
	will be at risk	b	5.526	1.638	0.938
	will be vulnerable	b	5.580	1.620	0.955
	can be exploited	b	5.543	1.639	0.948
	can be misused	b	5.608	1.591	0.956
	can be compromised	b	5.694	1.553	0.958
CNC	Perceived Cost of Non-Compliance				
	My non-compliance with the requirements of the ISP would _____.				
	be harmful to me.	b	5.002	1.903	0.925
	impact me negatively.	b	5.287	1.806	0.951
	create disadvantages for me.	b	5.138	1.893	0.964
	generate losses for me.	b	4.881	1.993	0.924

Scale

a. 1. Strongly Disagree – 7. Strongly Agree
b. 1. Not at all – 7. Very Much
c. 1. Extremely, 2. Quite, 3. Slightly, 4. Neither, 5. Slightly, 6. Quite, 7. Extremely
d. 1. Almost Never, 2. Very Rarely, 3. Rarely, 4. Occasionally, 5. Frequently, 6. Very Frequently, 7. Almost Always

APPENDIX C: Validity Analysis

Table 0.4: Composite Reliability, AVE, and Latent Variable Correlations

	CR	AVE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1. IC-R	0.984	0.955	**0.977**																
2. GSA	0.922	0.746	0.532	**0.864**															
3. ISPA	0.955	0.840	0.408	0.686	**0.917**														
4. A	0.956	0.846	0.479	0.367	0.382	**0.920**													
5. NB	0.934	0.826	0.486	0.398	0.378	0.490	**0.909**												
6. SE-NC	0.989	0.966	-0.143	0.099	0.092	-0.044	-0.090	**0.983**											
7. SE-C	0.982	0.947	0.395	0.545	0.583	0.369	0.341	0.175	**0.973**										
8. CC	0.981	0.930	-0.352	-0.200	-0.206	-0.261	-0.309	0.371	-0.186	**0.964**									
9. IB	0.973	0.902	0.328	0.369	0.364	0.391	0.368	-0.108	0.325	-0.218	**0.950**								
10. R	0.947	0.816	-0.144	0.062	0.154	-0.018	0.028	0.220	-0.002	0.274	0.230	**0.903**							
11. SR	0.969	0.841	0.333	0.357	0.393	0.427	0.386	-0.007	0.332	-0.095	0.492	0.234	**0.917**						
12. BC	0.952	0.834	0.208	0.271	0.254	0.326	0.330	0.010	0.239	-0.126	0.531	0.384	0.530	**0.913**					
13. IC	0.980	0.923	0.240	0.179	0.153	0.232	0.192	-0.045	0.116	-0.066	0.277	0.188	0.244	0.270	**0.961**				
14. S	0.929	0.767	0.202	0.305	0.332	0.295	0.312	-0.083	0.226	-0.089	0.338	0.332	0.335	0.394	0.409	**0.876**			
15. VR	0.979	0.904	0.363	0.352	0.362	0.392	0.382	-0.077	0.286	-0.199	0.415	0.185	0.638	0.526	0.326	0.465	**0.951**		
16. CNC	0.969	0.886	0.245	0.271	0.291	0.334	0.311	-0.094	0.210	-0.093	0.392	0.292	0.519	0.575	0.438	0.645	0.700	**0.941**	
17. ISA	0.941	0.669	0.508	0.905	0.930	0.409	0.422	0.103	0.615	-0.222	0.399	0.122	0.410	0.286	0.180	0.349	0.390	0.308	**0.818**

• **1. IC-R** = Intention to Comply - Reflective; **2. GSA** = General Security Awareness; **3. ISPA** = ISP Awareness; **4. A** = Attitude; **5. NB** = Normative Beliefs; **6. SE-NC** = Self-Efficacy Not to Comply; **7. SE-C** = Self-Efficacy to Comply; **8. CC** = Cost of Compliance; **9. IB** = Intrinsic Benefit; **10. R** = Rewards; **11. S** = Safety of Resources; **12. BC** = Benefit of Compliance; **13. IC** = Intrinsic Cost; **14. S** = Sanctions; **15. VR** = Vulnerability of Resources; **16. CNC** = Cost of Non-Compliance; **17. ISA** = Information Security Awareness
• **CR** = Composite Reliability; **AVE** = Average Variance Extracted
• Diagonal elements display the square root of AVE for factors measured with reflective items.

Table 0.5: Cross Loadings

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1. a	**0.97**	0.52	0.40	0.48	0.48	-0.14	0.40	-0.36	0.34	-0.14	0.33	0.21	0.24	0.21	0.37	0.25	0.50
1. b	**0.98**	0.51	0.40	0.45	0.44	-0.13	0.38	-0.34	0.29	-0.15	0.32	0.19	0.22	0.19	0.34	0.22	0.49
1. c	**0.98**	0.52	0.39	0.47	0.50	-0.14	0.38	-0.34	0.33	-0.14	0.33	0.21	0.23	0.19	0.36	0.24	0.50
2. a	0.52	**0.90**	0.60	0.35	0.40	0.04	0.46	-0.21	0.37	0.03	0.32	0.25	0.15	0.25	0.32	0.21	**0.80**
2. b	0.34	**0.84**	0.54	0.25	0.28	0.13	0.42	-0.08	0.30	0.11	0.23	0.23	0.13	0.29	0.22	0.23	**0.73**
2. c	0.59	**0.85**	0.57	0.38	0.37	0.00	0.46	-0.24	0.29	-0.03	0.35	0.21	0.19	0.26	0.35	0.25	**0.77**
2. d	0.39	**0.87**	0.66	0.28	0.32	0.17	0.54	-0.15	0.32	0.11	0.32	0.25	0.15	0.26	0.32	0.24	**0.82**
3. a	0.42	0.67	**0.93**	0.35	0.33	0.09	0.54	-0.21	0.33	0.07	0.35	0.18	0.13	0.27	0.31	0.23	**0.88**
3. b	0.45	0.69	**0.92**	0.36	0.33	0.09	0.57	-0.23	0.32	0.05	0.36	0.19	0.11	0.23	0.34	0.22	**0.88**
3. c	0.26	0.55	**0.88**	0.30	0.37	0.08	0.46	-0.13	0.35	0.28	0.34	0.29	0.18	0.39	0.34	0.32	**0.79**
3. d	0.36	0.60	**0.94**	0.38	0.36	0.08	0.56	-0.19	0.34	0.19	0.39	0.27	0.14	0.34	0.34	0.30	**0.85**
4. a	0.50	0.39	0.39	**0.89**	0.43	-0.05	0.36	-0.26	0.37	-0.06	0.37	0.26	0.22	0.25	0.35	0.28	0.42
4. b	0.43	0.33	0.35	**0.94**	0.44	-0.04	0.34	-0.25	0.36	0.00	0.39	0.31	0.20	0.28	0.38	0.31	0.37
4. c	0.42	0.30	0.31	**0.93**	0.45	-0.03	0.32	-0.22	0.32	-0.03	0.40	0.29	0.19	0.25	0.33	0.28	0.33
4. d	0.41	0.32	0.35	**0.92**	0.49	-0.04	0.32	-0.23	0.39	0.03	0.41	0.35	0.24	0.30	0.38	0.35	0.37
5. a	0.36	0.37	0.37	0.41	**0.85**	-0.10	0.29	-0.29	0.40	0.14	0.37	0.37	0.18	0.32	0.34	0.31	0.40
5. b	0.49	0.37	0.32	0.47	**0.93**	-0.06	0.32	-0.27	0.29	-0.07	0.34	0.25	0.17	0.25	0.35	0.25	0.38
5. c	0.46	0.34	0.35	0.45	**0.95**	-0.09	0.31	-0.28	0.33	0.03	0.36	0.30	0.17	0.30	0.35	0.30	0.38
6. a	-0.15	0.08	0.06	-0.06	-0.10	**0.98**	0.14	0.37	-0.13	0.21	-0.03	-0.01	-0.05	-0.09	-0.08	-0.09	0.08
6. b	-0.14	0.11	0.11	-0.04	-0.08	**0.99**	0.18	0.36	-0.10	0.22	0.00	0.03	-0.05	-0.07	-0.06	-0.09	0.12
6. c	-0.13	0.11	0.10	-0.04	-0.09	**0.98**	0.20	0.37	-0.08	0.21	0.01	0.01	-0.04	-0.08	-0.08	-0.10	0.11
7. a	0.40	0.52	0.56	0.37	0.35	0.18	**0.97**	-0.18	0.34	-0.01	0.32	0.23	0.12	0.22	0.29	0.21	0.59
7. b	0.38	0.54	0.58	0.35	0.33	0.17	**0.98**	-0.18	0.32	0.01	0.34	0.25	0.11	0.23	0.29	0.22	0.61
7. c	0.37	0.53	0.56	0.36	0.32	0.17	**0.97**	-0.18	0.30	-0.01	0.31	0.22	0.11	0.21	0.25	0.19	0.59
8. a	-0.37	-0.20	-0.21	-0.28	-0.35	0.36	-0.19	**0.96**	-0.22	0.26	-0.13	-0.13	-0.09	-0.10	-0.23	-0.12	-0.22
8. b	-0.32	-0.19	-0.20	-0.22	-0.29	0.36	-0.17	**0.95**	-0.18	0.27	-0.07	-0.12	-0.05	-0.09	-0.17	-0.08	-0.22
8. c	-0.34	-0.19	-0.19	-0.25	-0.28	0.36	-0.17	**0.97**	-0.22	0.27	-0.08	-0.12	-0.06	-0.08	-0.18	-0.08	-0.21
8. d	-0.33	-0.19	-0.18	-0.25	-0.26	0.35	-0.18	**0.97**	-0.22	0.25	-0.07	-0.11	-0.06	-0.07	-0.18	-0.07	-0.20
9. a	0.36	0.38	0.38	0.42	0.39	-0.11	0.34	-0.22	**0.95**	0.18	0.49	0.47	0.25	0.34	0.41	0.37	0.42
9. b	0.35	0.38	0.38	0.40	0.38	-0.10	0.32	-0.22	**0.96**	0.21	0.49	0.52	0.26	0.33	0.40	0.37	0.41
9. c	0.28	0.33	0.32	0.35	0.33	-0.10	0.30	-0.20	**0.96**	0.23	0.47	0.52	0.27	0.31	0.40	0.39	0.35
9. d	0.25	0.31	0.30	0.31	0.29	-0.10	0.27	-0.19	**0.94**	0.25	0.42	0.50	0.27	0.30	0.37	0.37	0.34
10. a	-0.07	0.10	0.20	0.04	0.10	0.12	0.05	0.15	0.23	**0.87**	0.25	0.37	0.18	0.35	0.20	0.29	0.17
10. b	-0.10	0.09	0.15	-0.02	0.04	0.20	0.03	0.24	0.24	**0.91**	0.21	0.37	0.16	0.29	0.17	0.27	0.14
10. c	-0.20	0.00	0.08	-0.04	-0.03	0.24	-0.07	0.31	0.18	**0.91**	0.19	0.31	0.17	0.28	0.13	0.24	0.05
10. d	-0.18	0.01	0.10	-0.06	-0.03	0.26	-0.04	0.32	0.17	**0.92**	0.18	0.33	0.17	0.28	0.15	0.25	0.07

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
11. a	0.26	0.31	0.34	0.37	0.30	0.02	0.29	-0.06	0.41	0.28	**0.87**	0.45	0.21	0.28	0.50	0.45	0.35
11. b	0.31	0.34	0.36	0.40	0.34	-0.02	0.27	-0.12	0.44	0.21	**0.93**	0.51	0.22	0.29	0.62	0.48	0.38
11. c	0.33	0.35	0.38	0.39	0.35	0.02	0.33	-0.08	0.44	0.22	**0.94**	0.47	0.21	0.29	0.60	0.47	0.40
11. d	0.28	0.28	0.33	0.37	0.36	-0.04	0.28	-0.09	0.46	0.20	**0.92**	0.48	0.24	0.32	0.56	0.48	0.33
11. e	0.33	0.34	0.36	0.39	0.38	0.00	0.31	-0.08	0.47	0.17	**0.93**	0.49	0.23	0.32	0.62	0.49	0.38
11. f	0.31	0.34	0.39	0.43	0.39	-0.01	0.34	-0.09	0.48	0.22	**0.92**	0.52	0.23	0.34	0.60	0.48	0.40
12. a	0.30	0.31	0.28	0.36	0.45	-0.07	0.30	-0.23	0.57	0.23	0.53	**0.83**	0.28	0.36	0.51	0.49	0.32
12. b	0.19	0.24	0.23	0.29	0.28	0.03	0.21	-0.09	0.46	0.35	0.46	**0.93**	0.22	0.34	0.48	0.52	0.25
12. c	0.13	0.21	0.20	0.27	0.24	0.05	0.18	-0.06	0.46	0.42	0.46	**0.95**	0.24	0.36	0.46	0.55	0.22
12. d	0.13	0.23	0.21	0.26	0.22	0.04	0.18	-0.07	0.45	0.41	0.47	**0.93**	0.23	0.37	0.46	0.53	0.24
13. a	0.27	0.19	0.15	0.23	0.20	-0.06	0.11	-0.08	0.24	0.15	0.24	0.26	**0.95**	0.35	0.31	0.38	0.19
13. b	0.24	0.17	0.15	0.23	0.20	-0.05	0.12	-0.08	0.28	0.20	0.24	0.26	**0.98**	0.41	0.30	0.42	0.17
13. c	0.22	0.17	0.16	0.22	0.16	-0.06	0.11	-0.07	0.28	0.19	0.23	0.27	**0.96**	0.42	0.31	0.45	0.18
13. d	0.20	0.17	0.13	0.21	0.18	-0.01	0.11	-0.03	0.26	0.18	0.23	0.25	**0.96**	0.39	0.32	0.43	0.16
14. a	0.25	0.31	0.32	0.33	0.32	-0.12	0.23	-0.15	0.31	0.22	0.31	0.34	0.41	**0.91**	0.45	0.57	0.34
14. b	0.24	0.34	0.36	0.31	0.32	-0.09	0.28	-0.13	0.31	0.24	0.34	0.36	0.37	**0.91**	0.46	0.60	0.38
14. c	0.06	0.16	0.21	0.14	0.17	-0.02	0.11	0.03	0.26	0.43	0.21	0.33	0.33	**0.78**	0.32	0.50	0.21
14. d	0.14	0.23	0.26	0.23	0.26	-0.05	0.16	-0.03	0.30	0.32	0.29	0.35	0.32	**0.90**	0.39	0.58	0.27
15. a	0.34	0.33	0.37	0.38	0.38	-0.09	0.27	-0.20	0.39	0.19	0.61	0.51	0.31	0.48	**0.94**	0.69	0.38
15. b	0.36	0.35	0.36	0.40	0.39	-0.07	0.29	-0.22	0.38	0.16	0.61	0.50	0.29	0.46	**0.95**	0.66	0.39
15. c	0.34	0.33	0.32	0.36	0.34	-0.07	0.27	-0.17	0.41	0.19	0.59	0.50	0.32	0.41	**0.95**	0.66	0.35
15. d	0.33	0.32	0.32	0.35	0.34	-0.08	0.26	-0.18	0.39	0.18	0.60	0.49	0.29	0.42	**0.96**	0.64	0.35
15. e	0.35	0.34	0.35	0.37	0.36	-0.06	0.28	-0.18	0.40	0.16	0.62	0.50	0.34	0.44	**0.96**	0.68	0.38
16. a	0.23	0.23	0.25	0.31	0.31	-0.11	0.18	-0.10	0.39	0.26	0.47	0.53	0.41	0.59	0.63	**0.92**	0.26
16. b	0.26	0.30	0.31	0.33	0.30	-0.06	0.24	-0.10	0.37	0.25	0.50	0.51	0.44	0.62	0.69	**0.95**	0.33
16. c	0.24	0.28	0.30	0.33	0.31	-0.09	0.21	-0.10	0.38	0.27	0.52	0.56	0.40	0.62	0.68	**0.96**	0.31
16. d	0.19	0.21	0.24	0.28	0.25	-0.11	0.15	-0.05	0.34	0.32	0.46	0.56	0.39	0.59	0.63	**0.92**	0.25

APPENDIX D: UBC Research Ethics Board certificate of approval

The University of British Columbia
Office of Research Services
Behavioural Research Ethics Board
Suite 102, 6190 Agronomy Road, Vancouver, B.C. V6T 1Z3

CERTIFICATE OF APPROVAL - MINIMAL RISK AMENDMENT

PRINCIPAL INVESTIGATOR:	**DEPARTMENT:**	**UBC BREB NUMBER:**
Hasan Cavusoglu	UBC/Sauder School of Business	H07-02124

INSTITUTION(S) WHERE RESEARCH WILL BE CARRIED OUT:

Institution	Site
N/A	N/A

Other locations where the research will be conducted:

The research will be conducted as an online survey. We will use panel members of a market research company. The panel of the market research company is formed by individuals who have interests in participating academic or non-academic surveys. An invitation letter will be sent by the market research firm to panel members. Those who decide to participate in the study will visit the Internet address of our online survey. The panel members' identities are kept confidential by the market research firm. We will not be given any personal details about participants. There is no way to match the survey responses with the identities of the participants since neither we collect personal information nor we are given such information by the market research firm. Basically, we will be collecting anonymous answers to our survey questions. Participants will be able to participate in the study by any computer with Internet access and from any location at their own convenience.

CO-INVESTIGATOR(S):
Izak Benbasat
Burcu Bulgurcu

SPONSORING AGENCIES:
Social Sciences and Humanities Research Council of Canada (SSHRC)

PROJECT TITLE:
A Model of the Antecedents of Information Security Policy Compliance

Expiry Date - Approval of an amendment does not change the expiry date on the current UBC BREB approval of this study. An application for renewal is required on or before: January 29, 2009

AMENDMENT(S):	AMENDMENT APPROVAL DATE: June 17, 2008	
Document Name	**Version**	**Date**

Other:

The web site is under development. The web site will contain the consent form and the survey questions provided in sections 9.2. and 9.6.

The amendment(s) and the document(s) listed above have been reviewed and the procedures were found to be acceptable on ethical grounds for research involving human subjects.

Approval is issued on behalf of the Behavioural Research Ethics Board

Dr. M. Judith Lynam, Chair
Dr. Ken Craig, Chair
Dr. Jim Rupert, Associate Chair
Dr. Laurie Ford, Associate Chair
Dr. Daniel Salhani, Associate Chair
Dr. Anita Ho, Associate Chair