

Spring 3-1-2012

# Information Security Policy Compliance: A User Acceptance Perspective

Ahmad Al-Omari  
*Dakota State University*

Follow this and additional works at: <https://scholar.dsu.edu/theses>

---

## Recommended Citation

Al-Omari, Ahmad, "Information Security Policy Compliance: A User Acceptance Perspective" (2012). *Masters Theses & Doctoral Dissertations*. 278.  
<https://scholar.dsu.edu/theses/278>

This Dissertation is brought to you for free and open access by Beadle Scholar. It has been accepted for inclusion in Masters Theses & Doctoral Dissertations by an authorized administrator of Beadle Scholar. For more information, please contact [repository@dsu.edu](mailto:repository@dsu.edu).

# **INFORMATION SECURITY POLICY COMPLIANCE: A USER ACCEPTANCE PERSPECTIVE**

A dissertation submitted to Dakota State University in partial fulfillment of the  
requirements for the degree of

Doctor of Science

in

Information Systems

May, 2012

By

Ahmad Al-Omari

Dissertation Committee:

Dr. Omar El-Gayar

Dr. Amit Deokar

Dr. Wayne Pauli

Dr. Viki Johnson



## DISSERTATION APPROVAL FORM

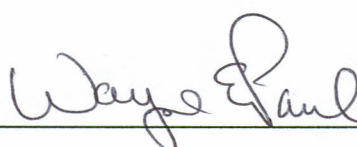
This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Science in Information Systems degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or the university.

Student Name: Ahmad Al-Omari

Doctorate's Dissertation Title: Information Security Policy Compliance: A User Acceptance Perspective

Dissertation Co-Chair: Dr. Omar El-Gayar  Date: 4/23/2012

Dissertation Co-Chair: Dr. Amit Deokar  Date: APRIL 23, 2012

Committee Member: Dr. Wayne Pauli  Date: Apr 23, 2012

Committee Member: Dr. Viki Johnson  Date: 4/23/12

## ACKNOWLEDGMENT

I want to express my deepest gratitude to Drs. Omar El-Gayar and Amit Deokar, my doctoral advisors and committee chair, for their encouragement, patience, and invaluable ongoing guidance. Their support and enthusiasm for my work over the past year has been an engine for my inspiration and progress. More than advisors and mentors, they were also truly distinguished friends who selflessly made themselves available for help without hesitation on both academic and personal matters. I cannot express enough my appreciation for their meritorious and wise support, guidance, patience, encouragement except to say that this study could have never come into existence without their help and support.

I would also like to thank my committee members, Dr. Wayne Pauli and Dr. Viki Johnson, who were extremely generous with their time and support at critical moments during the dissertation process. Their insight, recommendations and suggestions are truly appreciated. Also, a special thanks for all who helped me in my data collection, especially my dear friend Dr. Hasan Aleassa for administering the data collection process.

To my best friend, who was always there to help, support and encourage me, John Lee Holmes. I will never forget your kind assistance in helping me edit my work, often on short notice.

Further, this acknowledgment cannot be complete without a special thank you to the following individuals who assisted with the data collection for this study; Yahya Abu Al-Dahab, Hla Refaei, Fadi Alquraan, Mervat Ayoob, and my nephews Khalid and Firas Al-Omari. It goes without saying that while my dissertation has rested heavily on the indefatigable assistance of those named above and countless others, the mistakes are my own.

Most important of all has been the continuous support and encouragement I have received from my family. Words cannot describe my deep gratitude, love and respect for them. My brothers, sisters and my mother offered selfless support and unlimited prayers. To my dear father, whose soul departed before seeing the fruits of what he always motivated me to accomplish: at this moment, I stand speechless recalling your inspiration and encouragement in words and deeds. This work and all that follows are yours! No one but God can reward you for all that you offered me, emotionally and financially.

To my wife, Samar: all your life with me you have secured our love with patience, kindness, and understanding of our changing circumstances. Through it all you have fashioned the nurturing atmosphere I needed in which to study and to work and I will never forget your fortitude in support of our shared future. Despite scarcity of time and treasure, you have provided the best foundation I could ever hope for all the while prudently managing a family of seven. If I could speak all the world's languages I would still be unable to describe my wonderment and joy at all you are to me. I am so very blessed to have such a wonderful wife as you.

Truly, I will never forget the delight of my eyes, the joy of my soul, the light of my heart, and the fountain of my life and happiness that are my children: Deemah (my soul), Mohammad (my eyes), Jana (my heart), Zaid (my happiness), and Saja (my life). You have all displayed wisdom far beyond your tender years by so generously sacrificing entertainment and numerous other childhood delights and giving me the space I needed to finish this work. I promise to compensate every hour I have been away from you.

Praise be to God in the first and in the hereafter! Praise be to God who gives and prevents, who gives generously and wisely prevents. Praise be to God with gratitude and with thanks for setting forth for me the time, effort and fortune to complete this work. Praise and thanks be to God for all His blessings and for fashioning in me all that I am now.

## ABSTRACT

Information security policy compliance is one of the key concerns that face organizations today. Although, technical and procedural securities measures help improve information security, there is an increased need to accommodate human, social, and organizational factors. While employees are considered the weakest link in information security domain, they also are assets that organizations need to leverage effectively. Employees' compliance with Information Security Policies (ISPs) is critical to the success of an information security program. This study adapts the Technology Acceptance Model (TAM) and the Theory of Planned Behavior (TPB) to examine users' behavioral intention to comply with ISPs.

Compliance and systems misuse has been investigated heavily in the last couple of years. However, there are still huge gaps in this area, and more investigation is needed as the systems abuse dilemma is more likely to persist in the future. Different theories were borrowed from criminology, sociology, and other social and behavioral sciences to help understand the factors motivating either compliance or non-compliance behavior, or systems misuse intentions and behaviors. This study identifies the antecedents of employees' compliance with the information security policies (ISPs) of an organization. Specifically, the impact of structured and unstructured information security awareness on behavioral intentions to comply with an organization's ISP was investigated. Drawing on TAM and TPB, the study posits that along with perceived behavioral control (self-efficacy and controllability) and subjective norms, an employee's intention to comply with the requirements of the organization's ISP is associated with the degree to which s/he believes or perceives compliance to be difficult to understand, to learn or operate (perceived complexity; PC), and/or to the extent that safeguarding the organization's information technology resources will enhance his/her job performance (PUOP).

Data was collected using a survey instrument that captured employees' perceptions and intention regarding compliance with the organizations' ISPs. A sample of 878 employees working in nine different banks in Jordan was used to test the research model. Results indicated that employees' intention to comply is significantly influenced by PC, PUOP, and subjective norms. Employees' awareness of security countermeasures was found to

significantly affect perceived usefulness of protection and perceived complexity, and they, in turn, affect their intentions to comply with the requirements of organizations ISPs. General information security awareness and technology awareness were also found to significantly influence employees' intention to comply through PUOP and PC. Controllability was found to have no significant impact on PC and PUOP.

Overall, this study presents significant contributions toward explaining the role of Information Security Awareness (ISA) and employees' perceptions of the usefulness and complexity of the requirements of the organization's ISP to boost compliance behavior.

## DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,



---

Ahmad Al-Omari



## TABLE OF CONTENTS

ACKNOWLEDGMENT .....	iii
ABSTRACT .....	v
LIST OF FIGURES .....	xi
LIST OF TABLES .....	xii
CHAPTER ONE: INTRODUCTION .....	1
Background and Motivation.....	1
Information Security Policy Compliance.....	3
Problem of the Study.....	4
Research Questions .....	5
Significance and Contribution .....	6
Organization of the Dissertation .....	6
CHAPTER TWO: LITERATURE REVIEW .....	7
Information Security .....	7
Definition .....	7
Evolution.....	9
Threats and Vulnerabilities .....	14
Human Threats and Information Systems Misuse .....	16
Behavioral Information Security Literature .....	18
Information System Misuse Studies .....	18
Information Security Policy Compliance Studies .....	24
Protective and Preventive Technologies Studies .....	33
Limitations and Gaps in the Previous Literature .....	38

CHAPTER THREE RESEARCH MODEL AND HYPOTHESES .....	41
Theoretical Framework .....	42
Theory of Reasoned Action (TRA) vs. Theory of Planned Behavior (TPB).....	42
Technology Acceptance Model.....	45
The Role of Attitude in the TAM.....	47
Research Model and Hypotheses .....	49
Constructs Adapted from TAM .....	50
Constructs Adapted from the Theory of Planned Behavior .....	53
Information Security Awareness .....	56
User’s Awareness of Security Countermeasures .....	58
CHAPTER FOUR: RESEARCH METHODOLOGY.....	62
Research Design.....	62
Survey Instrument Design.....	64
Survey Instrument Validation .....	68
Face and Content Validity.....	68
Construct and Discriminant Validity .....	69
Sampling and Data Collection .....	71
Sample Size.....	71
Data Collection.....	72
CHAPTER FIVE: DATA ANALYSIS AND RESULTS.....	76
Sample Characteristics and Descriptive Statistics .....	76
Initial Assessment of Validity and Reliability .....	78
Exploratory Factor Analysis .....	78
Assessment of Reliability.....	83
Common Methods Bias.....	83

Data Analysis and Results.....	84
Assessment of Measurement Model .....	85
Structural Model Testing.....	89
CHAPTER SIX: DISCUSSION AND IMPLICATIONS .....	92
Overview of the Study and Findings.....	92
Discussion of Findings .....	95
Theoretical Contribution .....	100
Practical Contribution .....	101
Limitations .....	104
Conclusion .....	106
References .....	108
Appendix A .....	127
Appendix B .....	128
Appendix C .....	132

## LIST OF FIGURES

Figure 1: Theory of Reasoned Action (Ajzen, 1988).....	43
Figure 2: Theory of Planned Behavior (Ajzen, 1988).....	45
Figure 3: Technology Acceptance Model (TAM) adopted from (Davis et al., 1989) .....	46
Figure 4: Research Model - Security Acceptance Model (SAM) .....	50
Figure 5: The Results of the Structural Model Testing.....	90

## LIST OF TABLES

Table 2.1: Security Elements .....	9
Table 2.2: Information Security Threats .....	15
Table 2.3: Computer abuse empirical studies .....	21
Table 2.4: Information security policy compliance empirical studies .....	31
Table 2.5: Protective and Preventive Technologies Studies .....	36
Table 4.1: Sources of Measurement Items .....	64
Table 4.2: Composite Reliability, AVE, and Latent Variable Correlations.....	71
Table 5.1: Sample Characteristics.....	77
Table 5.2: Measurement Items and Item Loadings .....	80
Table 5.3: Reliability of Construct.....	83
Table 5 4: Harmon’s Single-factor Results.....	84
Table 5 5: Measurement Items and Item Loadings .....	86
Table 5 6: Composite Reliability, AVE, and Latent Variable Correlations.....	88
Table 5 7: Main Effect Path Coefficient (Structural Model Results).....	91

# CHAPTER ONE

## INTRODUCTION

### **Background and Motivation**

Information security and data protection has become one of the most important concerns and challenges facing organizations and users today. Despite the effort and money these organizations spend to secure their assets, many incidents of data breaches and information loss continue to happen every year (CSI, 2009). Today, organizations realize that securing information is a continuous and complex task. The burden of keeping information secure is not only the responsibility of the IT department; it lies on the shoulders of all people of the organization (Herath & Rao, 2009a; Kraemer & Carayon, 2005; Thomson & von Solms, 1998; Werlinger, Hawkey, & Beznosov, 2008). In view of that, users must be aware of their roles and responsibilities in protecting information assets and how to respond to any potential threat (NIST 800-16 R1). From here came the security awareness programs to focus on addressing the needs to enlighten users on how to effectively protect information assets (Aytes & Conolly, 2003; Bray, 2002; Chen, Shaw, & Yang, 2006; Hansche, 2001; Kruger & Kearney, 2006; McCoy & Fowler, 2004).

To secure information assets and to reduce the risk associated with these systems, organizations typically concentrate on technical and procedural security measures (e.g. Besnard & Arief, 2004; Kraemer, Carayon, & Clem, 2009; Schlienger & Teufel, 2003). Although these solutions help improve information security (Straub, 1990), relying on them alone is not enough to eliminate risk (Bulgurcu, Cavusoglu, & Benbasat, 2010a; Siponen, 2005). Even though organizations are investing more in information security technology-based solutions (Bulgurcu et al., 2010a), evidence from empirical surveys found that respondents reported large increases in information security incidents in 2009 (Richardson, 2009). Organizations need to effectively manage and control security threats, beyond reliance

on the deployment of security technologies software and hardware such as anti-virus, firewalls, intrusion detection, etc. (Aytes & Conolly, 2003; Bernard, 2007; Dinev & Hu, 2007; Zhang, Reithel, & Li, 2009). In addition human, social and organizational factors must be considered as well (Beznosov & Beznosova, 2007; Werlinger et al., 2008). Technology is an important factor but inadequate to the success of security. Technology is dependent on the users' behavior (Ng & Xu, 2007). In a study aimed at mapping the current information systems and security research, Dhillon and Backhouse (2001) found that the use of socio-organizational factors to understand information systems security is still at the theory building stage.

Recently, information security researchers realized that management's attention to secure information resources is required (Dutta & McCrohan, 2002) to design effective security policies (Siponen, Pahlila, & Mahmood, 2007; Whitman, Townsend, & Aalberts, 2001), and to motivate human and organizational factors to enhance users' security awareness to comply with information security policies (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009). Information security policies must be designed to provide employees with guidelines on how to address the integrity, availability, and confidentiality of information resources while they use information systems in performing their jobs (Straub, 1990; Whitman et al., 2001). Despite creating comprehensive information security policies and guidelines that govern and control employees' behavior to implement secure practices in an organization being a first priority matter, compliance with these policies is still lacking. Therefore, defining the factors that motivate employees' awareness to comply with an organization's information security policies is an important step in helping information security managers to understand and solve individual behavioral issues in information security management.

Most of the security awareness programs available to date may not be effective to fill the gap between perception and behavior as most of security awareness programs failed to prepare users with the ability of projecting potential security risks (Shaw, Chen, Harris, & Huang, 2009), some researchers believe this gap is due to the lack of a pre-defined methodology to deliver these programs (Valentine, 2006). In order to fill this gap, attention has been directed toward deploying behavioral theories to understand and change users' behavior to be more security-conscious (e.g. Dinev & Hu, 2007; Layton, 2005; Ng & Xu, 2007; Rhee, Kim, & Ryu, 2009; Zhang et al., 2009).

## **Information Security Policy Compliance**

Studies showed that the majority of security problems are caused by employees' non-compliance behavior or violation of security policies of their organizations (Myyry, Siponen, Pahlila, Vartiainen, & Vance, 2009; Trevino, 1986), which may be due to the fact that information security policies (ISPs) fail to impact the users on the ground, or to address the ignorance of users of the policies existence (Mason, 1986). Protecting an organization's IT assets against theft of proprietary information and from other forms of crimes and destruction begins with developing comprehensive ISPs (Whitman et al., 2001). However, creating best security systems, guidelines, and policy focusing on the basic security goals of confidentiality, integrity, and availability, will ensure maximum protection in return for the organization's security investment (Cohen & Cornwell, 1989; Whitman et al., 2001), but are not enough to ensure employees' compliance (Bulgurcu et al., 2010a; Herath & Rao, 2009b), and will not eliminate threat if these policies are not used properly.

Information security policies are designed to provide employees with the appropriate rules and guidelines for the protection of the information assets of the organization while they utilize information systems to perform jobs (Bulgurcu et al., 2010a; Whitman, 2008). According to Kwok and Longley (1999), ISP includes a definition of information security; a statement of management intention supporting the goals and principles of information security; an explanation of the specific security policies, standards and compliance requirement; a definition of general and specific responsibilities for all aspects of information security, and an explanation of the process for reporting suspected security incidents. ISP sets the strategic direction, scope, and tone for all security efforts within the organization, and it also assigns responsibilities for the various areas of security and addresses the legal compliance (Whitman, 2008). The ISP typically addresses compliance in two areas; general compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components, and the use of specified penalties and disciplinary actions (Schou & Shoemaker, 2007). Accordingly, a person is said to comply with the ISPs if she/he acts according to the behavior, guidelines, rules, and procedures specified by the security policy (Verizon, 2009).



Compliance with ISPs incorporates activities related to the initial execution of the policy to comply with its requirements; it is defined as the “process of ensuring that security policies are being followed” (Wetzels, Odekerken-Schroder, & Van Oppen, 2009, p. 24). This will include working with organizational personnel and staff to best implement the policy in different situations and ensure that the policy is understood by all who are required to implement, monitor and by those required to enforce the policy through monitoring, tracking, and reporting (Molok, Chang, & Ahmad, 2010). In contrast to compliance, researchers investigated system abuse and misuse (e.g. D'Arcy & Hovav, 2009; Harrington, 1996; Siponen & Vance, 2010; Straub, 1990). Various definitions have been utilized to describe inappropriate or illegal activities involving information systems. Straub (1990, p. 257) used the term computer abuse to comprise “the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against hardware, program, data, and computer services”. Hu, Xu, Dinev, and Ling (2010, p. 1379) focused on internal computer offense and defined it as “any act by an employee using computers that is against the established rules and policies of an organization”, which include “unauthorized access to data and systems, unauthorized copying or transferring of confidential data, or selling confidential data to third party for personal gains, etc...”.

Thus, achieving effective information security requires that employees are not only aware of, but also comply with information security policies and guidelines (Pahnila, Siponen, & Mahmood, 2007). Few definitions of information security compliance were introduced in the literature, so for the purpose of this study we define ISP compliance as the activities incorporated to the execution of the policy to ensure that employees act according to the behavior, guidelines, rules, and procedures specified by the security policy.

### **Problem of the Study**

Various studies have investigated employees' compliance behavior from different perspectives. In a newly published study, drawing from the Theory of Planned Behavior (TPB), Bulgurcu et al. (2010a) have identified antecedents of employee compliance with information security policy. They traced employees' attitudes toward compliance with ISP back to its underlying set of compliance-related beliefs rooted in the rational choice theory (RCT). The role of information security awareness and its effect on employees' attitudes

toward compliance is also examined. Herath and Rao (2009b) investigated motivational factors rooted in protection-motivation theory (PMT), deterrence theory, and organizational behavior to examine the adoption of information security practices and policies. Siponen and Vance (2010) suggest a model for policy compliance drawn from neutralization theory and deterrence theory. They argue that neutralization techniques influence employees' intentions to violate ISP. This study will complement the work of others and extend the knowledge about employees' compliance with ISPs by examining the role of information security awareness in enhancing employees' compliance with ISPs.

### **Research Questions**

Drawing on the technology acceptance model (Davis, Bagozzi, & Warshaw, 1989) it is proposed that an employees' intention to comply with the organization's Information Security Policies (ISPs) is influenced by perceived complexity (PC) and Perceived Usefulness of Protection (PUOP). Perceived behavioral control (PBC); self-efficacy and controllability, was traced back to its set of compliance perceptions, which are rooted in the theory of planned behavior. Also the role of information security awareness has been investigated and it is postulated that it will influence employees' PU and PC toward compliance. This model will help identify factors that shape an employee's decision to comply with ISPs and the process leading to this action. Specific hypothesis that identify relationships between each of the constructs are empirically tested. Data was collected using a survey instrument designed specifically to test this model. The study will try to answer the following questions

1. How can employees' security behavior toward compliance with ISPs be improved in order to reduce security incidents?
2. What is the role of information security awareness in forming employees' behavior toward compliance with ISPs?
3. What are the employees' perceptions about their roles and responsibilities, as set in the ISPs, in safeguarding an organization's information resources toward compliance with ISPs?
4. What are the employees' perceptions about the degree of difficulty in complying with ISPs?

## **Significance and Contribution**

The results of this study will help senior management understand the factors that influence employees to comply with Information Security Policies (ISPs), and encourage positive behaviors and decrease the human errors which will eventually reduce the cost of security. The results will also be very helpful in developing appropriate information security training and education programs to enhance positive behaviors based on different socio-technical and organizational variables that were used in this model, and in employing satisfactory technology and better utilizing the benefits of current technology within the organization.

This study will contribute to the understanding of the theoretical background of the existing IS security awareness approaches, and will also point out to what extent IS security awareness approaches incorporate empirical evidence on their practical effectiveness. Eliciting such information will benefit practitioners, since approaches based on empirical evidence can be considered more credible in terms of their practical usefulness and efficiency than approaches lacking such evidence. IS security practitioners would benefit from concrete guidance on how to implement the approaches in their organizations.

From an academic perspective, this study will contribute to the library of security awareness research. The field of security awareness research is lacking in studies that look at this concept from a behavioral perspective and that employ behavioral theories, such as TRA, TPB, TAM, and others. This study will be the first to research the behavioral intention of users toward the adoption of security measures using the original TAM with the effect of external variables included as predictor variables.

## **Organization of the Dissertation**

The rest of the dissertation is arranged as follows. The next chapter presents a review of the relevant literature and highlights this study's contributions. The third chapter presents the research theoretical foundation; and discusses the research model and develops research hypotheses to be tested. The fourth chapter describes the research methodology, survey instrument, sample, and data collection method. The fifth chapter presents and discusses the results of the study. The final chapter concludes the dissertation and discusses the limitations of the study.

## **CHAPTER TWO**

### **LITERATURE REVIEW**

This chapter reviews the information security compliance literature that is relevant for the development of the study's research model. It begins with a definition of the information security then an overview of information security evolution in the last few decades is presented. Different kinds of threats and vulnerabilities are defined concentrating on the insider threat to information security. A review of behavioral information security literature was categorized based on the dependent variable; systems misuse/abuse studies, information security policy compliance studies, and protective and preventive technologies studies. The chapter concluded by defining the gap in the literature review and explaining how this study will bridge this gap.

#### **Information Security**

##### **Definition**

The terms information security and information systems security were used interchangeably by some researchers, while others differentiated between them. Hill and Pemberton (1995) describe information security as "... systems and procedures designed to protect an organization's information assets from disclosure to any person or entity not authorized to have access to that information, especially information which is considered sensitive, proprietary, confidential, or classified" (p. 15). In the same context, the National Institute of Standards and Technology (NIST) defined information security as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (NIST, 2009, p. B4). The principle of information security is to ensure business continuity and to minimize business damage by preventing and minimizing the impact of security

incidents (von Solms, 1998). To overcome problems inherent in other definitions and to create a firm foundation for further practical work in the measurement of information security, Anderson (2003, p. 310) defines information security as “a well-informed sense of assurance that information risks and controls are in balance”.

The core concept of information security is to establish and maintain programs that ensure availability, integrity, and confidentiality of the organization’s information resources (Hansche, Berti, & Hare, 2004). Other research took a different perspective on information security by focusing on “behavioral information security” which is defined as “the complexes of human action that influence the availability, confidentiality, and integrity of information systems” (Stanton, Stam, Guzman, & Caldera, 2003, p. 4). Based on the goal of information, Parker (1998) sees that information security base should be set to meet an organization’s need to maintain the security of information from intentional and unintentional misuse and abuse.

Most of the widely used definitions of information security signify the importance of confidentiality, integrity, and availability of information, which is known as the CIA triad (Hansche et al., 2004; McCumber, 2005; Swanson, Hash, & Bowen, 2006). This triad has been criticized because it fails to relate information security in an organizational and business context, it is insufficient in response to the new challenges that are emerging for information security, and it lacks the adequate emphasis on the organizational actors’ roles in working with information security (Kolkowska, Hedström, & Karlsson, 2009). Therefore, new definitions and new concepts were introduced to replace the information security concepts. According to von Solms & von Solms (2005), security is not merely preserving and protecting information and sensitive data of the organizations, but protection of the business itself. On the other hand, Dhillon (1997) views the entire information system as a protection object. Information security is considered an important division of information security that includes all forms of information storage and processing (Schweitzer, 1990), and in whatever form the information is exchanged or stored, it should always be properly protected (ISO/IEC17799, 2005). In this context, Schweitzer (1990, p. 62) defines information security as “the protection of the operations and data in process in an organization’s computing systems.”

All of these have introduced a description and definition of information security that involve protecting the availability, integrity, authenticity, and confidentiality of information. Definitions of these four elements are presented in Table 2.1 (McCumber, 2005).

Table 2.1: Security Elements

Security Elements	Description
Confidentiality	Making information available only to those people who need it, when they need it, and under the appropriate circumstances.
Integrity	Ensuring the information is accurate, complete, and robust.
Availability	Having the information when it is needed.
Authenticity	The quality of being genuine or original, rather than reproduction or fabrication.

## Evolution

Information security has been a management concern since the introduction of computer to the business world. Early studies of computer security discussed the consequences of poor security to organizations. Allen (1968) described the kinds of threats a security system must deal with, and indicated the directions security measures ought to take. Management should take appropriate actions for security; controlled access, production control, duplicates files, and internal security group. Wasserman (1969) proposed different security controls and audits for electronic data processing activities that include; punched cards, magnetic tapes, and disks which help companies create significant procedures to guard computer programs and data against error, malice, fraud, disaster, or system breakdowns. The computer environment of the 1960s and 1970s consisted of stand-alone mainframes computing that were used when computers were first introduced in business (Thomson & von Solms, 1998). These computers were extremely large and vulnerable to environmental conditions and hence, had to be housed in a completely separate building. Securing these computers was needing to access the computer building was kept under physical security control. Although the system only allowed one user to work on it at a time, and did not grant access to the data, making it nearly impossible for unauthorized users to have access to the data. Environmental issues were the major threats to a computer; i.e., floods, earthquakes, fires, and civil disorders, so it was relatively easy to take precautions to minimize these threats (Thomson & von Solms, 1998). Information security was very basic in its early days, mostly comprised of simple document classification schemes, and due to the primary idea that the main threat to security was physical theft of equipment, no application classification projects for computers or operating systems were found (Whitman & Mattord, 2009).

Then along came a multi-users computing environment that brought with it new threats, specifically, more people were able to work on the machine outside the confines of the computer center at the same time (Thomson & von Solms, 1998). In addition, as workstations were situated in the users' work environment, access control was no longer sufficient to verify users' validity; users were electronically granted access to computer systems, and system components were shared, e.g. memory, databases, printers, etc. (Whitman & Mattord, 2009). Elimination of these threats was surmounted by the implementation of security controls such as a user authentication system that is embedded within mainframe operating systems. Consequently, information security from the senior executives was mainly viewed as the management of log-in IDs and passwords, and therefore it was located within the IT departments and typically buried somewhere within the data center operations management (Fitzgerald, 2007). In this computing stage, workstations used were considered dumb terminals (all intelligence resided on the central computer) and restricting users to work in certain areas was relatively easy. Therefore, physical and technical security measures were adequate to ensure effective information security (Thomson & von Solms, 1998). Information technology (IT) at this stage was considered an overhead expense to support organization functions; also it was considered a technical theme and hardly understood by the senior management, yet still important (Fitzgerald, 2007). In this "Zone Security" stage, as (Shimazu, 2007) called it, security meant a wall surrounding entire company systems and forcefully controlling the gates of the wall so the data and machines behind those walls was secure.

In the early 1980s, with the introduction of the personal computer, a significant change occurred to information security (Fitzgerald, 2007); information was now an asset to be valued, traded, and, most of all, protected (Hurd, 2001). The introduction of the personal computer and the growth of end user computing (EUC) brought new security concerns for organizations; end-users control their own inputs, processing, outputs, and even software development (Goodhue & Straub, 1991). Contrasted to the stand-alone computing environment where knowledgeable IS professionals were controlling the computing environment, computer security partly shifted to end users themselves (D'Arcy, 2005), which was found to be the sixth most critical issues facing IS executives (Brancheau & Wetherbe, 1987). The proliferation of end-user computing offers the promise of improved productivity,

but also entails risks; e.g. inadequate data integrity, “orphan” applications, and fragmented systems. Alavi and Weiss (1985) identify data integrity, unauthorized access, and data security as the main risks associated with EUC. Little or lack of security training for end users was another concern (Leitheiser & Wetherbe, 1986). Benson (1983) considered lack of data security and integrity, database access control, significant training to users, inadequate documentation, and poor data backup procedures as critical issues associated with EUC.

Despite the increased number of threats to information systems as a result of the growth of EUC, management still underestimated the importance of information security at this stage. In a study conducted by Ball and Harris (1982), among eighteen management issues that MIS management might address, data security was ranked in the twelfth place and information privacy was in fourteenth place. According to Brancheau and Wetherbe (1987), information system executives did not rank security and control among the top twenty critical issues of management. While out of eight problem areas, Hackathorn (1987) found that general executives ranked security of data in fourth place and they thought of it as less important than the incompatibility of hardware and software, while MIS executives thought that data security was the most important issue. Hoffer and Straub (1989) indicated that an estimated 60% of organizations assigned full or part-time members to administer security, but still legislators have paid more attention to computer crime and abuse reports in the media than to managers, as evidenced by laws dealing with computer crimes in all fifty states.

The advent of the personal computer (PC), and the increasing complexity and reliability of networks environment, has brought about a great challenge in the area of information security (Thomson & von Solms, 1998). The systems that used to be protected by a data center have been moved to a shared network environment; wide area networks (WAN) and local area networks (LAN) were utilized, and recently the Internet, extranets, and intranets all accelerated the multi-user and EUC environment (D'Arcy, 2005; Fitzgerald, 2007). While it is still considered as mainly an IT issue, it is during this stage that information security came to the forefront, since information systems are becoming the central hub to the successful of many organizations' daily operations (Fitzgerald, 2007; Thomson & von Solms, 1998). Despite the fact that many organizations have become heavily dependent on computer-based and information systems, and that the interruption of either may lead to outcomes ranging from inconvenience to disaster (Loch, Carr, & Warkentin, 1992), information security



continues to be ignored by top managers, middle managers, and employees (Straub & Welke, 1998).

With the low cost of producing PCs and portable computers, along with networking resources “the Internet” was made available to the public in the late 1990s for accessing internal systems remotely, and new security concerns were introduced (Fitzgerald, 2007). Due to the competitive nature of business, users’ profiles changed significantly and developed into a situation where managerial people often needed access to information on a “must have now” basis. This situation, along with other similar situations, resulted in people gaining access to or modifying data that they were not supposed to have, whether intentional or unintentional (Thomson & von Solms, 1998). The growing computer literacy has created increasingly sophisticated users of technology, who are becoming more skillful at committing different types of computer abuse (Straub & Nance, 1990).

Today network and computer attacks have become pervasive. The exponential growth in network-centric connectivity brought different kinds of threats to information systems; any computer at home or business that is connected to the Internet is under threat from viruses, worms, hackers attacks, theft, defacement, and other forms of internal and external security threats (D'Arcy, 2005; Hansman & Hunt, 2005). Although countermeasures, such as anti-viruses, firewalls, security patches, and passwords control systems, and other technologies and techniques that can be automated, are available to improve information security, they are not well utilized by users even if they are freely available (Workman, 2007; Workman, Bommer, & Straub, 2008). Threats cause different damages to the information systems; a denial-of-service can result in stopping an organizations’ operations for a period of time, which might cause a financial loss to these companies (Hovav & D'Arcy, 2003). Damages due to security incidents such as the Code Red virus in 2001 was estimated at \$2.1 billion and at \$1.1 billion due to the Melissa virus in 1999 (Telang & Wattal, 2007).

Recent industry research indicates the importance of security threats to information systems, although, security breaches have become very common in today’s network environment. In a recent survey by Ernst and Young (2010), results show that many organizations recognize the risks associated with current trends and new technologies; 46% of respondents indicated that their annual investment in information security is increasing. The Symantec Global Internet

Security Threats Report specifies that more than 16 million new malicious code threats were reported in 2008, (265% increase over 2007). The 2009 CSI Computer Crime and Security survey reported big jumps in incidence of financial fraud (19.5 percent an increase of over 12 percent from last year); malware infection (64.3 percent and increase of over 50 percent from last year); denials of service (29.2 percent, an increase of over 21 percent from last year), password sniffing (17.3 percent, an increase of over 9 percent from last year); and Web site defacement (13.5 percent an increase of over 6 percent from last year) (Richardson, 2008). The 2009 Ponemon Institute benchmark study (2010) found that data breach incidents cost U.S. companies \$204 per compromised customer record in 2009, compared to \$202 in 2008. Despite an overall drop in the number of reported breaches (498 in 2009 vs. 657 in 2008 according to the Identity Theft Resource Center), the average total per-incident cost in 2009 was \$6.75 million, compared to an average per-incident cost of \$6.65 million in 2008. Financial losses were not the only consequence facing organizations as a result of security threats, other detrimental impacts included negative publicity, competitive disadvantage, and even reduced organizational viability (Kankanhalli, Teo, Tan, & Wei, 2003).

The increased numbers of information security incidents stimulated academic and practitioner interests in information security. In today's information intensive society, the secure management of information systems has become critically important (Herath & Rao, 2009b). In defining the 10 key issues for IT executives, Luftman and Ben-Zvi (2010) found that security and privacy is still one of the top 10 IT management concerns; it was ranked ninth in 2009, eighth in 2008, and second in 2005. On the other hand, security technology lags behind IT management expectations, having traditionally been ranked in the top 10, but in 2009, it is not even in the top 20 (Luftman & Ben-Zvi, 2010). Although 90 percent of organizations view information security as a highly important factor for achieving their overall objectives (Ernst & Young, 2010), only 53 percent of the surveyed organizations allocated 5 percent or less of their overall IT budget to information security (Richardson, 2008).

In summary, as organizations became more and more dependent on computer-based and telecommunications intensive information systems and with the evolution of information technology, this created a panacea of threats to information systems assets. Today organizations in both the public and the private sectors are aware of the needs of information security to protect their information systems and corporate systems (Hawkins, Yen, & Chou,

2000). In essence, management's concern with information security has changed over years making it one of the top 10 issues of IT management.

### **Threats and Vulnerabilities**

Every day the world witnesses new information security incidents, which cost millions of dollars annually, as a result of computer theft, fraud, abuse, and other security threats. In its 1.6 dictionary release (2011), Common Attack Pattern Enumeration and Classification (CAPEC) introduced 460 different attacks to information systems classified into 15 categories based on the attack mechanism. The 2008 Computer Security Institute (CSI) survey on Computer Crime and Security Survey found that 43% of respondents detected computer security incidents in the last 12 months; 47% of them reported 1-5 security incidents, and 26% did not know the number of security incidents they had. Studies showed neglect of information security in the past by management created a less secure system that led to more frequent and damaging security breaches (Straub & Welke, 1998; Whitman & Mattord, 2008). Management, practitioners, and employees alike must understand the threat facing their organization's information systems and examine the vulnerabilities inherent in those systems because of such threats (Whitman, 2004).

The literature shows a paucity of empirical research in information security threats classifications, effects, types, management strategies, and determinants. Some of this research is summarized in Table 2.2. The results of Whitman (2004) study illustrate the need for increased levels of awareness, education, and policy in information security to address the threats. A security threat taxonomy is essential to the threat inventory process because it helps to keep the threat inventory complete and representative (Im & Baskerville, 2005). Different security threats classifications were introduced to help with managing risk and setting the appropriate controls. Peltier (2005) classified threats into two categories; common and accidental. CAPEC (2011) classified risk into 15 categories based on the attack mechanism. In an empirical study Whitman (2003) found that, deliberate software attacks, technical software failures or errors, acts of human error or failure, deliberate acts of espionage or trespass, and deliberate acts of sabotage or vandalism are the top security threats to information systems.

Table 2.2: Information Security Threats

	Type of threats Identified
Peltier (2005)	Common and accidental threats
CAPEC (2011)	Data Leakage Attacks, Resource Depletion, Injection, Spoofing, Time and State Attacks, Abuse of Functionality, Probabilistic Techniques, Exploitation of Authentication, Exploitation of Privilege/Trust, Data Structure Attacks, Resource Manipulation, Physical Security Attacks, Network Reconnaissance, Social Engineering Attacks, and Supply Chain Attacks
Whitman and Mattord (2008)	Acts of Human Error, Compromises to Intellectual Property, Deliberate Acts of Espionage, Deliberate Acts of Information Extortion, Deliberate Acts of Sabotage, Deliberate Acts of Theft, Deliberate Software Attacks, Deviations in Quality From ISP, Forces of Nature, Technical Hardware Failures or Errors, Technical Software Failure or Errors, and Technological Obsolescence
McCumber (2005)	Environmental, Internal; Hostile and Non-Hostile, and External
Schou and Shoemaker (2007)	Outsider and Insider Threats
Hansman and Hunt (2005)	Threats that use a single attack vector and threats that do not use an attack vector or are too trivial such as Viruses, Worms, Trojans, Buffer overflow, DOS, Network attack, Physical attack, Password attack, and Information gathering attack Target of the attack; Hardware and Software (Operating System, Application and Network). Vulnerabilities and exploits that the attack uses.
Loch et al. (1992)	Sources (Internal and External), Perpetrators (Human and Non-human), Intent (Accidental and Intentional) and consequences (Disclosure, Modification, Destruction and Denial of Use)
Workman et al. (2008)	Unauthorized Interception of Information; Unauthorized Modification of Information; Exposure of Information to Unauthorized Individuals; Destruction of Hardware, Software and/or Information
Mármol and Pérez (2009)	Attack intent Attack target Required knowledge Attack cost Algorithm dependence Detectability

Markus (2000) argued that IT-related risk is fragmented, and the appropriate IT security management considerations are through IT-related risk rather than security by itself. To capture the view of IT management about threats to information systems and resident data, Loch et al. (1992) classified threats to information systems based on the source (internal vs. external), perpetrators (human vs. non-human), intent (accidental vs. intentional), and consequence (disclosure, modification, destruction, and denial of use). To better understand the numerous threats facing organizations, Whitman and Mattord (2008) developed a scheme that group threats based on their respective activities. Their model consisted of 12 general

threat categories; acts of human error, compromises to intellectual property, deliberate acts of espionage, deliberate acts of information extortion, deliberate acts of sabotage, deliberate acts of theft, deliberate software attacks, deviations in quality from ISP, forces of nature, technical hardware failures or errors, technical software failure or errors, and technological obsolescence.

Hansman and Hunt (2005) classify threats into three categories, first based on the means by which the attack reached its target; threats that use a single attack vector and threats that do not use an attack vector or that are too trivial, such as viruses, worms, Trojans, buffer overflow, DOS, network attack, physical attack, password attack, and information gathering attack, second based on the attack target; hardware and software, and finally attacks based on vulnerabilities and exploits. On the other hand, Mármol and Pérez (2009) classified threats based on the attack intent, targets, required knowledge, cost, algorithm dependence, and detectability.

### **Human Threats and Information Systems Misuse**

In a very simple classification, threats to information security were classified as internal and external threats (e.g. McCumber, 2005; Schou & Shoemaker, 2007). All of the previous classifications rest under this taxonomy. One of the most important classifications is human error (insider threats), either intentional or unintentional, which is a vital internal threat category. It is recognized by information security researchers that insider threats represent one of the most critical threats to information security (e.g. D'Arcy & Hovav, 2009; Dhillon, 1999; Whitman, 2003). Verizon (2009) reported that the results of 600 incidents over five years showed that insiders are behind the majority of breaches, whether intentionally or unintentionally. Human attack is not a new issue for organizations, but might be of less concern than external threats for an organization (Stanton, Caldera, Isaac, Stam, & Marcinkowski, 2003). Human threats are often ignored (Wood & Banks, 1993), but are always present and evident in many ways and should be examined in the context of changing technical, social, business, and cultural factors (Colwill, 2009). The legitimate and privileged access to an organization's information assets lends a strong power to the insiders to have the highest potential risk to cause damage to the organization (Colwill, 2009; Dugo, 2007).

People are recognized to be the weakest link in information security (Bresz, 2004; Thomson & von Solms, 2005; Zhang et al., 2009), but they also can be great assets in the effort to reduce information security threats (Bresz, 2004; Bulgurcu et al., 2010a). Human threats have been ongoing concerns for organizations as the literature shows; Wasserman (1969) was one of the earliest researchers to discuss the importance of human errors and its effect on the company. Insiders can accidentally or intentionally compromise information confidentiality, integrity, and availability (Colwill, 2009), which can cost millions of dollars without criminal intent on anyone's part (Wasserman, 1969). The 2010/2011 CSI Computer Crime and Security survey reported that 40.9 percent of respondents stated that at least some of their losses were attributable to malicious insiders, but clearly non-malicious insiders are the greater problem, since 14.5 percent of respondents estimated that nearly all their losses were due to the non-malicious careless behavior of insiders, and 46 percent estimated between 20 to 80 percent of their losses were due to careless behavior of non-malicious insiders (Richardson, 2011). Organizations usually are reluctant to disclose security incidents fearing negative publicity that might destroy their image, and only a fraction of security incidents are actually discovered and reported, suggesting that the magnitude of the problem might be underestimated (D'Arcy, Hovav, & Galletta, 2009; Hoffer & Straub, 1989).

Recently, more attention was directed toward the human side of computer abuse (Lee, Lee, & Yoo, 2004), as a more important step toward effective information security management (Hu et al., 2010). A plethora of research has been conducted to explore "negative" or improper computing behavior in the last years. The majority of the information security research to understand employees' misconduct or misuse, and even criminal acts toward the organization's IT systems, has been conducted from different theoretical lenses (Hu et al., 2010). General Deterrence Theory (GDT) was one of the most used theories to study employees' behavior since their misconduct or misuse against information systems is related to criminal behavior (D'Arcy et al., 2009; Hu et al., 2010; Kankanhalli et al., 2003; Straub, 1990). In light of the turbulent future, security managers hold the key to the success or failure of a company's well-being, and since systems are used by people, information security is an organizational and social issue (Dhillon & Backhouse, 2000). Thus, people who use the systems are responsible for them, and play a key role in the security of individual and organizational systems (Lee et al., 2004).

## **Behavioral Information Security Literature**

Behavioral information security research has become an important component of the information security literature. Stanton, Caldera, et al. (2003, p. 3) defined behavioral information security as “the complexes of human action that influence the availability, confidentiality, and integrity of information systems”. Industry research helped to signify the importance of human factors in securing organizations’ information assets. Information security success depends in part upon the effective behavior of the people involved in its use (Stanton, Caldera, et al., 2003). Thus, the development of effective protective information technologies is not enough strategy to fight the threats, but understanding user attitudes, intention, and behavior, in addition to policies, are also important to successfully defend against information security threats (Dinev, Goo, Hu, & Nam, 2009). Appropriate (compliance) and improper (abuse) use of information systems has been explored in the existing behavioral information security literature (D’Arcy, 2005). The literature shows different approaches to studying employees’ behavior toward information security; some studies employed behavioral theories to examine information system abuse (e.g. Bulgurcu, Cavusoglu, & Benbasat, 2010b; D’Arcy et al., 2009; Harrington, 1996; Hu et al., 2010; Kankanhalli et al., 2003; Lee et al., 2004; Straub, 1990), while other studies employed behavioral theories to examine employees’ compliance with ISPs (e.g. Anderson & Agarwal, 2010; Greene & D’Arcy, 2010; Siponen, Pahnla, & Mahmood, 2010), and other studies examined a protective approach (e.g. Boss et al., 2009; Dinev & Hu, 2007; Puhakainen & Siponen, 2010; Workman et al., 2008).

### **Information System Misuse Studies**

Since computer abuse and employee misconduct against IS are considered criminal behavior, IS scholars have been attracted to the field of criminology to understand employees’ misconduct behavior and criminal acts against organizational IT systems (Hu et al., 2010). A number of studies adopted GDT to examine the impact of security countermeasures on information systems abuse or misuse (D’Arcy & Hovav, 2009; D’Arcy et al., 2009; Harrington, 1996; Herath & Rao, 2009a, 2009b; Hu et al., 2010; Kankanhalli et al., 2003; Lee et al., 2004; Pahnla et al., 2007; Straub, 1990), since it provide a theoretical explanation for the use of security countermeasures as a process to reduce IS misuse (D’Arcy & Hovav,

2009). Other studies adopted other theories such as fairness theory, neutralization theory and organizational justice theory, to examine the misuse behavior (Posey, Roberts, Lowry, & Bennett, 2010; Siponen & Vance, 2010; Warkentin, Willison, & Johnston, 2011). Table 2.3 presents a summary of these studies.

Straub (1990) was the one of the first IS scholars to use GDT in IS security. He argued that information security procedures can deter potential computer abusers from violating organizational policy. A survey of 1,211 randomly selected IS managers from different organizations indicated that different preventive and deterrent techniques were found to be effective in lowering computer abuse; such as weekly and overall weekly hours dedicated to data security, use of multiple methods to disseminate information about penalties and acceptable system usage, a statement of penalties for violation, and the use of security software. Moreover, the more that preventive security software is used, fewer abusers are expected as they become aware that IS security is actively monitoring their systems activity, preventing actual abuse and deterring possible violations of others. D'Arcy et al. (2009) suggested that security countermeasures; encompassing security policies; Security, Education, Training, and Awareness (SETA) programs; and computer monitoring, to be effective tools to reduce users' IS misuse. A sample of 269 computer users from different companies was used to test the model. Results showed that users' awareness of security controls has an impact on sanctions perceptions, which in turn reduced IS misuse intentions. It was also found that perceived severity of sanctions is more effective than perceived certainty of a sanction in reducing IS misuse intentions. Regarding users' awareness of SETA programs, the study provides evidence that these programs help to reduce IS misuse because they increase perceptions of the certainty and severity of punishment for such behavior. It was found that users' awareness of security policies reduce users' perceptions of the possibility of getting caught for misusing the system. Users' awareness of computer monitoring has a significant effect on users' perceived certainty and severity of sanctions that help deter IS misuse.

Hu et al. (2010) tested a model of computer offences that adopted three popular criminology theories; general deterrence theory, rational choice theory, and individual propensity. A sample of 207 employees from five large Chinese companies was used to test the research model. The study found that when an individual is ruminating whether to abuse (offence) the computer systems, the perceived benefits dominate the perceived risks in the rational decision



making process. Deterrence was found to have a limited impact on the offensive intentions through increased perceived risk. The study results suggested that computer offences are a result of overestimating the benefits and underestimating the risk by employees when the situations for committing the offences are present and they have the means to conduct the offensive acts.

Harrington (1996) employed deterrence theory from an ethical perspective, and assessed whether general and IS-specific codes of ethics affect computer abuse judgments and employees' intentions to abuse information systems. Computer abuse was defined as any action of writing or distributing viruses, cracking, computer fraud, illegal software copying, and corporate sabotage. The study found that general codes of ethics had no effect on computer abuse judgments and abuse intentions of all employees, but it was found to affect those IS personnel who tend to deny responsibility. As compared to general codes, IS-specific codes of ethics had a direct effect on computer sabotage judgments and intentions, but had no contrasting effect on those high in denial of responsibility. Based on the Theory of Planned Behavior (TPB), Lee et al. (2004) tested the effectiveness of an integrative model of GDT and Social Control Theory (SCT) to address computer abuse intention by insiders. Security policy, security awareness, and security programs were hypothesized to impact intention by acting as deterrent factors. In addition, organizational trust factors; attachment, commitment, involvement, and norms, were also assumed to have impact on intention and were expected to reduce computer abuse. A sample of 182 MBA students and middle managers from six Korean companies were used to test the model. The study found that security policies and security systems had no impact on the computer abuse behaviors. Results also showed that involvement (participation in informal meetings, personal relationships with many people, and loyalty to the company) was found to be effective in reducing computer abuse intention, as was the belief by employees that computer abuse is unacceptable and reduce computer abuse.

Table 2.3: Computer abuse empirical studies

Author (s)	Dependent Variable	Predictors	Theories	Findings and Comments
Straub (1990)	Computer abuse	Deterrents and preventive security software	GDT	Deterrents and preventive security software lower level of computer abuse
D'Arcy et al. (2009)	IS misuse intention	Security countermeasures (security policies, SETA programs, and computer monitoring), severity and certainty of sanctions	GDT	User awareness of security countermeasures reduced IS misuse intention through perceived certainty and severity of sanctions
Hu et al. (2010)	Intention to commit computer offense	Low self-control, perceived deterrence, perceived extrinsic benefits, perceived intrinsic benefits, perceived informal risks, and perceived formal risks	GDT, RCT, SCT	Rational choice framework has strong effect on intention to commit computer offense. Deterrence was less effective in predicting intention to commit computer offense.
Harrington (1996)	Computer abuse intention	Codes of ethics, Denial of Responsibility	GDT	General codes did not affect the computer abuse judgments and intentions. IS-specific codes had a minor effect on computer abuse judgments and intentions.
Lee et al. (2004)	Computer abuse	Security policy, security awareness, physical security system, attachment, commitment, involvement, norms, self-defense, and induction control	GDT, SCT	Deterrence factors (security system) have a significant effect on Self Defense Intention related to computer abuse
D'Arcy and Hovav (2009)	IS misuse intention	Security policies, SETA programs, and computer monitoring	GDT	SETA and computer monitoring has low effect on intention to system misuse.
Posey et al. (2010)	Internet Computer Abuse	Advanced Notification, Organizational SETA Efforts, Explanation Adequacy Organizational Trust	Fairness Theory	Advance notification, SETA programs, organizational trust, and explanation adequacy significantly decreases internal computer abuse incidents.
Siponen and Vance (2010)	Intention to violate IS security policies	Neutralization techniques, formal and informal sanctions, shame	Neutralization theory, GDT	Neutralization and informal sanction are excellent predictors of intention to violate ISPs.
Dugo (2007)	INFOSEC violation intention	PBC, SN, attitude, perceived punishment certainty, perceived punishment severity, organizational commitment, and security culture	TPB GDT	Attitude, SN, perceived punishment certainty, and severity are good predictors of behavioral intention to violate. INFOSEC Organizational commitment and security culture are not significant predictors of violation intention.

GDT-General Deterrence Theory, RCT-Rational Choice Theory, SCT-Self-Control Theory, TPB-Theory of Planned Behavior

Researchers in criminology and social psychology suggested that the security countermeasures deterrent effect is not uniform across individuals due to personal and organizational differences that impact the perceived strength of sanctions. To investigate this issue, D'Arcy and Hovav (2009) presented a model grounded in GDT to explore the moderating impact of computer self-efficacy and virtual status on sanction perceptions. Their model contains user awareness of security policies, the SETA program, and computer monitoring, and is built on the assumption that the deterrence mechanism of security countermeasures depends on the actions and awareness of end users, and therefore it is not important to understand the impact of these controls from the user's perspective. Researchers also assume that end users are not fully aware of the existence of many security countermeasures. Total samples of 507 participants were used to test their model; 238 MBA students and 269 employees. Two IS misuse scenarios, unauthorized access and unauthorized modification, were designed to capture respondent's intentions. Study results found that the moderating influence of computer self-efficacy has a significant negative affect on the relationships between computer monitoring and IS misuse intention. The results showed that deterrent effectiveness of SETA programs and computer monitoring is not consistent across all individuals; computer savvy individuals are less deterred, and these countermeasures are also less effective on employees that spend more working days outside of the office. As a result, the study recommended that security education and training programs should take into consideration the employee's level of computer understanding.

Posey et al. (2010) used fairness theory to explain why security policy sometimes backfires, and actually increases security violations. Fairness theory assumes that employees have an immanent need to blame the decision maker or have accountability to the decision maker when they experience a negative organizational event (Posey et al., 2010). The study expected explanation adequacy to increase employees' trust in their organization, and this trust should also increase internal computer abuse incidents following the security changes implementation. A sample of 397 full time employees from banking, financial, and insurance industries was used to obtain data for testing the study model. The study found that giving employees advance notification for future information security changes positively influenced employees' perceptions of organizational communication efforts. The adequacy of these explanations is also maintained by SETA programs, and explanation adequacy and SETA

programs worked in harmony to foster organizational trust, which significantly decreased internal computer abuse incidents. The findings show how organizational communication can influence the overall effectiveness of information security changes among employees, and how organizations can avoid becoming a victim to their own efforts.

Siponen and Vance (2010) argued that employees' violation of IS security policies, based on research in criminology, is not always best deterred by fear of sanctions, since employees may use neutralization techniques which allow them to reduce the perceived harm of their policy violation. Therefore, they proposed a theoretical model in which the effects of neutralization techniques could be tested with those of sanctions described by deterrence theory. The study used six techniques of neutralization; denial of responsibility, denial of injury, metaphor of the lodger, condemns the condemners, appeal to higher loyalties, and defense of necessity. They also used informal and formal sanctions and shame from the deterrence theory to examine employees' intention to violate IS security policy. A hypothetical scenario method was used to assess the research model, and a sample of 1449 administrative personnel from three organizations in Finland was used. The study found that neutralization is an excellent predictor of employees' intention to violate IS security policies. Intention was considered as a measured reflection of a predisposition to commit an act, so neutralization significantly affected the predisposition to violate IS security policy. As for the deterrence effect of sanctions, the study found that informal sanctions are insignificant predictors of intention to violate IS security policies in the presence of neutralization, and formal sanctions were also found to be insignificant predictors of IS security policy violation intention.

Drawing on the TPB and GDT, as well as organizational commitment, Dugo (2007) developed a model to examine information security (INFOSEC) violation intention. The study examined the effect of organizational security culture on violation intention. A sample of 113 participants (mostly students) from a professional government school was used to test the study model. The study found that the greater the attitude and subjective norm toward intentional INFOSEC policy violations, the greater the intention is to commit intentional INFOSEC policy violations. Perceived punishment certainty and perceived punishment severity were found significant in reducing intention to violate the INFOSEC policy. Organizational commitment and security culture were not significant predictors of INFOSEC policy violation intention.

### **Information Security Policy Compliance Studies**

Employees' compliance with Information Security Policies (ISPs) is an important concern for organizations (Puhakainen, 2006) to prevent and reduce information system resources misuse and abuse by insiders (Straub, 1990). Taking different perspectives, various studies (see Table 2.4) employed behavioral theories to examine employees' compliance with ISPs to reduce systems misuse and abuse. Drawing on TPB, Bulgurcu et al. (2010a) argue that along with normative belief, self-efficacy, information security awareness (ISA), an employee's attitude toward compliance will determine compliance intention with the ISP. Building on that, they trace employee attitude toward compliance with ISP back to its underlying set of compliance-related beliefs rooted in the rational choice theory (RCT); benefits of compliance, cost of compliance, and cost of noncompliance. The role of information security awareness also investigated. A sample of 464 employees, who used the IT resources of their organizations and had access to the Internet, was used to test the study model. It was found that attitude, normative belief, and self-efficacy has a significant effect on employee's intention to comply with the ISP. Also, it was found that outcome beliefs significantly affected the beliefs about overall assessment of consequences, which in turn significantly affected an employee's attitude. Information security awareness also was found to have significant effects on both attitude and outcome beliefs.

Likewise, Li, Zhang, and Sarathy (2010) employed the Rational Choice Theory (RCT) to examine the factors that influence Internet Use Policy (IUP) compliance. The study concentrated on defining the major costs and benefits that factor into employees' intention to comply with the IUP and the relationships among these factors, and the mechanisms that could facilitate IUP compliance. The study developed a model in which IUP compliance is examined as a cost-benefit-based behavior influenced by personal norms and organizational context factors. A sample of 246 employees from different organizations with IUPs was used to test the research model. The study found that employees are more likely to comply with the IUP when perceived benefits are outweighed by potential risks from formal sanctions and security threats. Sanction severity was found to be an ineffective mechanism for the majority of employees, except for employees with very low personal norms against Internet abuses. Also, social influence from subjective norms was not a significant predictor of an employee's

intention to comply with the IUP. Besides the cost–benefit analysis, compliance intention was also influenced by employees' personal norms or moral standards against Internet abuses.

To explore the aptitude of moral reasoning and values to encourage compliance with IS security policies, Myyry et al. (2009) developed a theoretical model that combines the Theory of Cognitive Moral Development (TCMD) (Which consists of three levels; Preconventional level: Focus is on self, Conventional level: Focus is on relationships, and Postconventional level: Focus is on personally held principles) and the Theory of Motivational Types of Values (TMTV) (which consists of a two-dimensional continuum; Openness to Change versus Conservation.). They argue that theories of moral reasoning are related to information security policies (ISPs) as the intention or decision to violate an ISP can be interpreted in terms of moral conflict. To test their model, data from a sample of 132 individuals in Finland, technical service center employees and part-time master students with work experience, was collected. In regard to moral reasoning, the study found that preconventional moral reasoning, which focuses on fear of sanctions and ‘What’s in it for me?’ thinking, is positively related to both hypothetical and actual compliance in the information security context, while conventional moral reasoning, which focuses on acts to please others and on following the laws and norms for their own sake, correlates negatively with compliance behavior. Of the value dimensions, the study found that openness to change was negatively related to behavioral choice in the information security context, while conservation was found to be positively related to behavioral choice in the information security context.

Siponen et al. (2007) combined the PMT with the modern GDT and TRA to explain how employees’ compliance with information security policies and guidelines can be improved. The study argued that the stronger the intention is to comply with ISPs, the more likely it is that the individual will actually comply with the ISPs. It was hypothesized that threat appraisal, self-efficacy, and response efficacy would positively affect employees’ intention to comply with the ISPs, and also it was hypothesized that intention to comply with ISPs and sanctions would positively affect actual compliance with ISPs. A sample of 917 employees from four Finnish companies was collected to test the research model. The results showed that threat appraisal, response efficacy, self-efficacy, and sanctions had a significant effect on employees’ intention to comply with an organization’s ISP. Talib and Dhillon (2010) have a different view, suggesting that emancipation leads to better protection of information. Their

study suggests that emancipating employees with respect to information access would make them more likely to comply with an organization's security policies. The higher the privilege granted to employees to access information, the higher the commitment toward the organization, and the tendency to comply with the ISP.

Similarly, Herath and Rao (2009b) adopted PMT, GDT, and organizational behavior to develop and test an integrated Protection Motivation and Deterrence model of security policy compliance under the umbrella of Decomposed Theory of Planned Behavior (DTPB). Drawing upon PMT the study incorporated an evaluation of threat appraisal and coping appraisal to identify attitudes toward security policies. The study also assessed the effect of employees' organizational commitment on security policy compliance intentions, and the influence of environmental factors such as deterrence, facilitating conditions, and social influence. A sample of 310 employees from 78 organizations was used to test the research model. The study found that employees' understanding of the severity of the threat significantly affected their concern regarding security breaches, but certainty of security breaches was found to have no significant impact on the security concern. Results suggest that if employees believe that complying with policies is an obstacle to their day to day job activity, they are less likely to comply with ISPs. It was also found that resource availability, self-efficacy, and perceived effectiveness of employee actions played a significant role in behaviors related to ISP compliance, while the impact of attitude on employees' compliance intention was found insignificant. In another study which builds upon Principal Agent Theory, Herath and Rao (2009a) investigated the impact of extrinsic incentives (penalties and social pressures) and intrinsic incentives (perceived value or contribution) on policy compliance intention. Using responses from 312 employees, the study found that intrinsic and extrinsic motivators have a strong influence on policy compliance intention. Severity of penalty was found to have a negative effect on compliance intention.

Greene and D'Arcy (2010) incorporated elements from moral development research models, the TRA and TPB, as well as criminological perspectives including Social Bond Theory (SBT), differential association, and neutralization theory, to examine the influence of security-related and employee organization relationship factors on users' IS security compliance decisions. Specifically they presumed that security culture, job satisfaction, and perceived organizational support have a positive effect on users' IS security. Data were

collected using two online surveys, and a sample of 127 computer-using professionals located in various organizations in the US. The results found that the relationship between security culture and security compliance intention supported the notion that security culture is an important factor for supporting and guiding information security programs, while perceived organizational support, was not found to be a significant predictor of compliant behavior intention. Using Social Learning Theory (SLT), Warkentin, Johnston, and Shropshire (2011) examined the influence of an informal social learning environment on individual compliance outcomes. The study argued that self-efficacy mediates the effect of external cues (situational support, verbal persuasion, and vicarious experience) on employees' behavioral intentions to comply. A sample of 202 healthcare professionals from nine separate and diverse healthcare organizations was used to test the research model. The study found strong evidence of the influence of an informal social learning environment on employees' perceptions of information privacy policy compliance intentions.

Based on compensation theory, Zhang et al. (2009) combined perceived technical security protection into the TPB to examine the impact of technical protection mechanisms on end-user security behavioral intentions to comply with security policies. The study was built on the assumption that the attitude toward the behavior, subjective norms (SN), and perceived behavioral control (PBC), determine an individual's intention to comply. An online survey was conducted, and a sample of 176 computer end-users from various industrial organizations in the United States was used to examine the research model. Both PBC and attitude were found as significant predictors of users' intention to comply with ISPs, and perceived technical protection was also found to have a significant impact on intention to comply with the ISPs. Regarding subjective norms, the study found that it plays a larger role with users who have less experience. In addition, the existence and effectiveness of technical support enhanced users' compliance intentions. To study individual intentions to engage in security-related behavior, Anderson and Agarwal (2010) employed PMT, along with TRA and TPB, to examine the behavioral intentions of individuals who are motivated to take the necessary precautions under their direct control to secure their own computer and Internet in a home setting. They theorized that intentions are determined by attitudes toward security related behavior, social influence in the form of subjective and descriptive norms, and psychological ownership of the relevant object. A survey and an experiment were conducted to test the



research model. A sample from subscribers of a locally based ISP and undergraduate students enrolled in an introductory business course at a large university were collected. The study found that home computer users' intentions to perform security-related behavior are formed by a combination of cognitive, social, and psychological components.

Developing their fear appeals model based on the PMT, and fear appeal theory, Johnston and Warkentin (2010) examined the influence of fear appeals on end users' intention to perform recommended individual computer security actions, specifically compliance behavior. A sample of 275 experienced computer users (faculty, staff, and students) from multiple sites at a large university was used to examine the research model. The study found that fear appeal has an inconsistent impact on end users' behavioral intention to comply with recommended individual security acts. Behavioral intention was found to be determined in part by perceptions of self-efficacy, response efficacy, threat severity, and social influence. Similarly, Chenoweth, Minch, and Gattiker (2009) developed a model that applies PMT to the spyware domain. The model hypothesized that maladaptive coping is mediating the relationship between behavioral intention and threat appraisal and coping appraisal. Based on data collected from 204 undergraduate students, the study found that perceived vulnerability, perceived severity, response efficacy, and response cost were found to be significant predictors of users' intention to adopt antispyware protective technology.

Siponen et al. (2010) took a different approach, by building a model based on PMT, GDT, TRA, innovation diffusion theory (IDT), and rewards to understand why some employees comply with their organization's ISPs and why other do not. The study argues for clear language in ISP documents, and for overall visibility of information security. Data from a sample of 917 employees was collected from four Finnish companies in the area of information and communications technology business operations, information security, logistics, and supermarket chains. The results showed that threat appraisal, self-efficacy, normative beliefs, and visibility of information security policies are significant predictors of intention to comply with organizations' ISPs. Deterrence was found to have a significant impact on actual compliance with ISPs, whereas rewards did not have a significant impact on actual compliance. In another study also aimed to understand why one would or would not follow a well-specified ISP, Pahnla et al. (2007) developed a theoretical model that combines GDT, PMT, TRA, Information Systems Success, and Triandis' Behavioral Framework and

Rewards. Based on a sample of 245 employees from a Finnish company, the study found that information quality has a strong effect on actual compliance with ISPs; while employees' attitude, normative beliefs, and habits have a significant effect on intention to comply with IS security policy. Sanctions were also found to have no significant effect on intention to comply, and rewards had no significant effect on actual compliance.

Bulgurcu, Cavusoglu, and Benbasat (2008) focus on demotivational factors (burden of compliance), and motivational factors (ISP awareness, fairness of the ISP, and facilitating conditions), to investigate its influence on employees' attitudes toward ISP compliance intention. They argue that demotivational factors have a negative impact on employees' attitude toward ISP compliance. They developed their study model based on the TPB to understand how employees perceived ISP compliance as a burden. An online survey administered by a professional market research company was conducted to collect data, and a sample of 464 employees from US companies, which have written ISPs that their employees are aware of, was collected. The study found that the perceived burden of compliance has a significant negative impact on employees' attitudes toward ISP compliance, whereas motivational factors (ISP awareness, ISP fairness, and facilitating conditions) were found to have a positive significant impact. In another study which also drew on TPB, Bulgurcu, Cavusoglu, and Benbasat (2009) investigated the role of employees' ISA and perceived fairness of the requirements of the ISP in shaping their attitude toward their compliance intention with the organization's ISP. Their study argued that employees' willingness to comply with the rules is motivated by intrinsic desires that stimulate internal motivation to comply/not to comply with ISP. The study found that ISA had a significant positive influence on an employee's perceived fairness of the ISP, which in turn leads to a higher positive attitude and intention toward compliance.

To investigate the impact of the characteristics of the ISP on employees' compliance intention, Bulgurcu et al. (2010b) proposed two factors ,ISP fairness and ISP quality (clarity, adoptability, and consistency), as predictors of employees' compliance intention with the ISP. The study argues that employees' perceived ISP Quality has a positive impact on their compliance perceptions. An online survey was conducted by a third party and a sample of 464 employees who are aware of the existence of written ISPs in their organization was used to test the research model. The study found that both ISP fairness and ISP quality were shown to

positively affect employees' compliance intention. Taking another approach, Xue, Liang, and Wu (2010) examined the relationship between punishment and IT compliance in mandatory settings. The study extended TAM by drawing on punishment research and justice theory to investigate how punishment affects employee compliance intention in mandatory settings. Their model suggests that compliance intention is affected by PU, satisfaction, punishment expectancy, perceived justice of punishment, and actual punishment. Perceived ease of use was hypothesized to affect compliance intention indirectly; through satisfaction and through PU. A sample of 118 accounting professionals from one of China's top 500 companies that implemented a large-scale ERP system was used to test the research model. Perceived justice of punishment was found to be a strong predictor of IT compliance intention in mandatory settings. Punishment expectancy and PU were found insignificant determinants of compliance intention. Actual punishment and PEOU were found to significantly affect compliance intention indirectly.

Chan, Woon, and Kankanhalli (2005) examined the effects of social contextual factors on employees' compliance intention. The study developed a model based on the social information processing approach, and posits that organizational climate (information security climate) will mediate the relationship between compliance behavior and social contextual factors (management practices, supervisory practices, and coworker socialization). Self-efficacy was also hypothesized to affect compliance behavior. The study found that all social contextual factors (management practices, supervisory practices, and coworker's socialization) indirectly had positive impacts on compliance behavior, but self-efficacy was found to be a strong predictor of employees' behavioral compliance intention.

Table 2.4: Information security policy compliance empirical studies

Author (s)	Dependent Variable (DV)	Predictors	Theories	Findings and Comments
Bulgurcu et al. (2010a)	Intention to comply	ISA, Belief about outcomes, Belief about overall assessment of consequences, Attitude, self-efficacy, and normative belief	TBP and RCT	Attitude, normative belief, and self-efficacy have a significant effect on employee's intention to comply. Outcome of beliefs significantly affected the employee's attitude
Li, Zhang, et al. (2010)	Internet use policy compliance intention	Organizational norms, organizational identification, perceived risk, perceived benefits, and personal norms	RCT	Perceived benefits, formal sanctions, and security risk are significant predictors of compliance intention with IUP.
Myyry et al. (2009)	Hypothetical and actual compliance with ISP	Preconventional reasoning, conventional reasoning, postconventional reasoning, openness to change, and conversation.	TCMD and TMTV	Preconventional moral reasoning, openness to change, and conversation are positively related to compliance with ISP.
Siponen et al. (2007)	Actual compliance with ISP	Threat appraisal, response efficacy, self-efficacy and sanctions	PMT, GDT, and TRA	Threat appraisal, response efficacy, self-efficacy, and sanctions positively affect actual compliance with ISP.
Herath and Rao (2009b)	Security policy compliance intention	Punishment severity, detection certainty, perceived probability of security breach, perceived severity of security breach, security breach concern level, response efficacy, response cost	PMT, GDT, and DTPB	Severity of breach, social influence, resource availability, response efficacy, organizational commitment, and self-efficacy has a positive effect on attitudes toward compliance with ISP.
Herath and Rao (2009a)	Policy compliance intention	Severity of penalty, certainty of detection, normative beliefs, peer behavior, and perceived effectiveness	Principal Agent Theory	Severity of penalty negatively affects policy compliance intention, whereas certainty of detection, normative beliefs, peer behavior, and perceived effectiveness have a positive effect.
Greene and D'Arcy (2010)	Security compliance intention	Security culture, job satisfaction, and perceived organizational support.	TRA, TBP, and SBT	Security culture and perceived organizational support are significant determinants of compliance intention with ISP.
Warkentin, Johnston, et al. (2011)	Behavioral intention to comply	Situational support, verbal persuasion, and vicarious experience	SLT	Self-efficacy mediates the effect of external cues on employees' intentions to comply with ISP.
Zhang et al. (2009)	Behavioral intention to comply	Perceived security protection mechanism, SN, PBC, and attitude	Compensation Theory and TPB	PBC, attitude, and perceived technical protection were found as significant predictors of intention to comply with ISP

Table 2.4: Information security policy compliance empirical studies (Continued)

Author (s)	DV	Predictors	Theories	Findings and Comments
Anderson and Agarwal (2010)	Intention to perform security-related behavior	Concern regarding security threats, perceived citizen effectiveness, self-efficacy, attitudes, SN, descriptive norm, and psychological ownership	PMT, TRA, TBP	Computer users' intentions to perform security-related behavior are formed by a combination of cognitive, social, and psychological components.
Johnston and Warkentin (2010)	Behavioral intention to comply	Perceived threat severity, perceived threat susceptibility, response efficacy, social influence, and self-efficacy	PMT and Fear Appeal Theory	Perceived threat severity and susceptibility, response efficacy, social influence, and self-efficacy positively affect intention to comply with ISP.
Chenoweth et al. (2009)	Behavioral intention to comply	Perceived vulnerability, Perceived severity, fear appraisal, response efficacy, self-efficacy, response cost, and maladaptive coping	PMT	Perceived vulnerability and severity, fears appraisal, response efficacy and cost, and maladaptive coping are significant determinants of compliance behavior.
Siponen et al. (2010)	Actual compliance with ISP.	Normative beliefs, threat appraisal, and self-efficacy, response efficacy, visibility, deterrence, and rewards	TRA, PMT, IDT, and GDT	Threat appraisal, self-efficacy, normative beliefs, deterrence, and visibility of information security policies are significant predictors of intention to comply.
Pahnila et al. (2007)	Intention to Comply	Negative reinforcement (i.e., sanctions, normative beliefs), positive reinforcement (i.e., information quality and habit), and attitude.	GDT, PMT, and TRA	Negative and positive reinforcement have a significant effect on actual IS security policy compliance.
Bulgurcu et al. (2008)	Intention to comply	Burden of compliance, ISP awareness, fairness of the ISP, and facilitating conditions	TPB	Perceived burden of compliance negatively impacts employees' attitude towards ISP compliance, and motivational factors and facilitating conditions have a positive impact.
Bulgurcu et al. (2009)	Intention to comply	Information security awareness, fairness, and attitude	TPB	ISA positively influences employees' perceived fairness of the ISP, which in turn leads to compliance.
Bulgurcu et al. (2010b)	Intention to comply	ISP quality and ISP fairness.	TPB	ISP fairness and ISP quality positively affect employees' compliance intention.
Chan et al. (2005)	Compliance behavior	information security climate (coworker specialization, direct supervisory practices, upper management practices), and self-efficacy		Social contextual factors (management practices, supervisory practices, and coworker's socialization) positively impact compliance behavior.

GDT-General Deterrence Theory, RCT-Rational Choice Theory, SCT-Self-Control Theory, TPB-Theory of Planned Behavior, TCMD- Theory of Cognitive Moral Development, TMTV- Theory of Motivational Types of Values, DTPB-Decomposed Theory of Planned Behavior, SBT- Social Bond Theory, SLT- Social Learning Theory, IDT-Innovation Diffusion Theory, PMT-Protection Motivation Theory.

### **Protective and Preventive Technologies Studies**

Preventive and protective technologies are used to protect systems, and data and information from viruses, spywares, unauthorized access, disruptions, and many other threats which have become very important to secure information assets (Dinev et al., 2009). The use of protective information technologies has attracted the attention of researchers, and many studies (see Table 2.5) that present theoretical insight into the users' behavior toward these technologies have emerged (Dinev & Hu, 2007). To examine the ability of security countermeasures to protect information assets against deliberate and unauthorized misuse by users, Kankanhalli et al. (2003) built a model based on GDT to test the effect of deterrent and preventive measures, in addition to organizational factors (organizational size, top management support, and industry type), on IS security effectiveness. A survey was conducted and data from 63 IS managers from different sectors was collected. The study found that greater deterrent efforts (measured in employee hours spent on IS security effort) and greater preventive efforts (measured in more advanced IS security software) appear to contribute to better IS security effectiveness, while enforcing more severe penalties for IS abusers does not seem to prevent IS abuses.

Based on TPB and TAM, Dinev and Hu (2007) studied the factors that influence intentions to use protective technologies and how they contribute to the formation of this intention. The study integrated the role of technology awareness with TPB and TAM variables. A sample of 332 IS professionals and students was used to test the research model. Results show that higher awareness leads to higher confidence in preventing negative technologies in the systems, and also enhances users' belief that they have the necessary skills and tools, by using protective technologies, to successfully combat the effect of negative technologies. Regarding PU and PEOU, results showed that they are not significant predictors of users' intention to use protective technologies, and computer self-efficacy was also insignificant in the context of protective technologies. In another study aimed at examining the effect of cross-cultural differences between the US and South Korea in user behavior toward protective technologies, Dinev et al. (2009) tested a model built on TPB that integrated cultural effects as a moderator variable of the key relationships. A sample of IS professionals and students from the US and South Korea was collected to examine the research hypothesis. The study found that cultural factors moderate the key relationships and play a significant role in the formation of user

attitude and behavior toward using protective technologies. South Korean computer users were found to exhibit a stronger relationship between the subjective norm and behavioral intentions than American users.

Boss et al. (2009) examined employees' security preventive behavior from an organizational control perspective. The study argued that organizational control elements (specification of sets of ISPs, evaluation of compliance with ISPs, and reward for compliance) are associated with individuals' perceived mandatoriness, which will influence the security precautions behavior. A sample of 1682 computer users working at a large medical center in the US was collected to test the research model. The study found that specifying policies and evaluating behaviors significantly influenced the perceived mandatoriness of security policies. Perception of mandatoriness was also found to be an effective motivator to individuals to take security precautions. Along the same lines, Ng, Kankanhalli, and Xu (2009) established a model based on Health Belief Model (HBM) to study users' preventive security behavior and to measure self-reported actual behavior. The study argued that individuals' behavior depends on their perceptions of security threats (perceived susceptibility to the threat and perceived severity of the threat), and evaluation of behavior to resolve the threat (perceived benefits of the security behavior, and perceived barriers to performing the preventive security behavior). A sample of 134 employees from different organizations was used to test the hypothesis. When applied to exercising care with email attachments, the study found that perceived susceptibility, perceived benefits, and self-efficacy are strong determinants of individuals' computer security behavior, while perceived severity, perceived barriers, cues to action, and general security orientation are not significant predictors of users' behavior. Results also indicated that cues to action, such as awareness programs, are not significant in triggering an individual to behave in a secure manner.

To investigate how personal computer users cope with an IT threat, Liang and Xue (2009) proposed a theoretical model that helped to explain individual IT users' behavior of avoiding the information security threats. Drawing on Cybernetic Theory and Coping Theory, Technology Threat Avoidance Theory (TTAT) defines the avoidance behavior as a dynamic positive feedback loop in which users go through two cognitive processes; threat appraisal (perceived susceptibility and perceived severity) and coping appraisal (perceived effectiveness, perceived costs, and self-efficacy). Later Liang and Xue (2010) derived a model

based on Technology Threat Avoidance Theory (TTAT) to elucidate how individuals develop threat perceptions, evaluate safeguard measures, and engage in avoidance behavior. The study argues that individuals' IT threat avoidance behavior is determined by avoidance motivation, which, in turn, is affected by perceived threat, which is influenced by perceived severity and susceptibility as well as their interaction. The model also suggests that avoidance motivation is directly affected by safeguard effectiveness, safeguard cost, and self-efficacy. A sample of 152 business students in a major American university was used to test the hypothesis. The study found that avoidance motivation is a strong predictor of users' IT threat avoidance behavior, which is determined by perceived threat, safeguard effectiveness, safeguard cost, and self-efficacy. The study found that users develop a threat perception when they believe that the malicious IT is likely to attack them (perceived susceptibility) and the consequences will be severe if they are attacked (perceived severity). When threatened, users are more motivated to avoid the threat if they believe that the safeguarding measure is effective (safeguard effectiveness) and inexpensive (safeguard cost), and if they have confidence in using it (self-efficacy).

In an environment where employees who are trained and aware of security threats and countermeasures, but choose not to comply with ISPs and implement security protections, Workman et al. (2008) developed a Threat Control Model (TCM) based on PMT and social cognitive theory, as an explanation for the gap between knowing and doing, and to test why individuals omit security precautions. The study hypothesized that threat assessment and coping assessment are predictors of individuals' behavior. They argued that people with either high perceived severity or high perceived vulnerability, or who have high self-efficacy or an internal locus of control, are less likely to omit security precautions than people who have either lower perceived severity or perceived vulnerability, or lower self-efficacy or an external locus of control, to cope with an IS security threat. A field study using a sample of 612 people from a large technology-oriented services corporation was conducted to investigate the TCM. The study found that both threat assessment and coping assessment have a large influence on the individual's subjective and objective omissive behavior, and that factors drawn from social cognitive theory (self-efficacy and locus of control) also have a significant influence on omissive behavior.



Table 2.5: Protective and Preventive Technologies Studies

Author (s)	Dependent Variable	Predictors	Theories	Findings and Comments
Kankanhalli et al. (2003)	IS effectiveness	Organizational size, top management support, industry type, deterrent efforts, deterrent severity, and preventive effort	GDT	Deterrent efforts, organizational size, top management support, industry type, and preventive efforts contribute to better IS security effectiveness.
Dinev and Hu (2007)	Behavioral intention to use protective technology	Technology awareness, PU, PEOU, self-efficacy, controllability, attitude, SN, and PBC	TPB and TAM	Technology awareness, controllability, attitude and PBC are significant determinant of intention to use protective technologies.
Dinev et al. (2009)	Behavioral intention to use protective technology	Technology awareness, PU, PEOU, self-efficacy, controllability, attitude, SN, and PBC	TPB and TAM	Cultural factors moderate the key relationships and play a significant role in the formation of user attitude and behavior towards using protective technologies.
Boss et al. (2009)	Precautions taking behavior	Control element (specification, evaluation, and reward), and perceived mandatoriness.		Specifying policies and evaluating behaviors significantly influence the perceived mandatoriness of security policies. Perception of mandatoriness is an effective motivator to individuals to take security precautions.
Ng et al. (2009)	Computer security behavior	Perceived susceptibility, perceived benefits, perceived barriers, cues to action, general security orientation, self-efficacy, and perceived severity.	Health Belief Model	Perceived susceptibility, perceived benefits, self-efficacy, and perceived severity are strong determinants of individuals' computer security behavior.
Liang and Xue (2010)	Avoidance behavior	Perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, and avoidance motivation	Cybernetic Theory and Coping Theory	Perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, and avoidance motivation all found to have a significant influence on avoidance behavior.
Workman et al. (2008)	Omissive behavior	Perceived severity, perceived vulnerability, locus of control, self-efficacy, perceived response efficacy, and response cost-benefit	Social Cognitive Theory and PMT	Threat assessment and coping assessment have high influence on the individual's subjective and objective omissive behavior, also self-efficacy and locus of control have significant influence on omissive behavior.

GDT-General Deterrence Theory, RCT-Rational Choice Theory, SCT-Self-Control Theory, TPB-Theory of Planned Behavior, PMT-Protection Motivation Theory

Security awareness education and training was and is still one of the most important fundamentals to information security practices (Furnell, Gennatou, & Dowland, 2002; Puhakainen & Siponen, 2010; Shaw et al., 2009). Unfortunately, security awareness is often poorly managed due to the fact that it is descriptive in nature; organizations' approaches for delivering security awareness take the form of "informing" their employees of their security policies, guidelines, and procedures (Layton, 2005). This approach only informs users that they must act in accordance with policies and procedures because the management desires them to do so (Layton, 2005). Information security awareness programs should be designed to change users' attitude and behavior to be more security-conscious (Ng & Xu, 2007; Thomson & von Solms, 1998).

A few studies took a different approach, other than prohibition and sanctions, to study employees' compliance with ISPs by concentrating on education and training to encourage desirable behavior. Puhakainen and Siponen (2010) proposed a training program, based on the universal constructive instructional theory and the elaboration likelihood model, to promote information security policy compliance. They found that in order to enhance employees' IS security policy compliance, information system security communication processes and training programs are needed. These programs are assumed to utilize methods and learning tasks that motivate employees to process information in accordance to policy. Karjalainen and Siponen (2011) contended that IS security training needs a theory that lays down elementary characteristics and explains how these characteristics shape IS security training principles in practice. They developed a theory that suggests that IS security training has certain elementary characteristics that distinguish it from other types of training, and needs to be understood before educational principles for IS security training can be selected. To enforce compliance with information security policy, Gupta and Zhdanov (2006) suggested a compliance bonus, and found that providing employees with proper economic incentives and building trust between organizational entities are good incentives for compliance. Choi, Kim, Goo, and Whitmore (2008) examined the influence of managerial information security awareness (MISA) on managerial actions toward information security (MATIS). The study argued that creation of ISPs, execution of information security training and education, implementation of information access control, updating information security systems, and the retainment of an information security team will have a significant positive effect on MISA. A

sample of 1773 Korean enterprises participated in the study, which found that MISA is one of the major constructs influencing managerial actions, and the subsequent security performance of the organization.

### **Limitations and Gaps in the Previous Literature**

A thorough analysis of the previous literature showed the various behavioral theories that have been employed to study employees' attitudes toward compliance with information security policies or to prevent systems misuse and abuse. While these studies have highlighted either the deterrent effect of sanctions or the role of incentives in encouraging employees' desirable behavior, none of the studies have addressed this problem as a system that employees must accept first, as Davis (1986) did with the ordeal of accepting the technology. Based on the analysis of the existing literature, it is evident that these theories have been effective in defining the factors that enhance compliance behavior or prevent system abuse. However, the limitation of previous literature is that it addresses the research problem only from an organizational perspective, without considering the users' perspective.

Information security researchers adapted different behavioral theories to study compliance behavior with ISPs or systems abuse or misuse. Theories such as TRA, TPB, RCT, PMT, GDT, SCT, TAM, and others were adopted as a theoretical foundation for their studies in order to predict behavioral intention. Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TPB), and its extension, is a general model *per se* that does not specify the beliefs that are operative for a particular behavior (Davis et al., 1989). Rational Choice Theory (RCT) posits that an individuals' decision to engage in a criminal behavior is a function of their perceptions of cost and benefits of deviant behaviors in deciding whether or not to offend (Hu et al., 2010; McCarthy, 2002; Paternoster & Simpson, 1996). RCT's criticism stems from the confusion accompanied with its key concepts, premises, and predictions (Bulgurcu et al., 2010a; McCarthy, 2002). General Deterrence Theory (GDT) posits that individuals choose to go into crime when the benefits outweigh the costs (Forsyth, 1980; Siponen & Vance, 2010), and while they may not be completely rational, they are reasonably aware of the benefits and potential costs associated with criminal behavior (Agnew, 1993). GDT is criticized as being salient because of its implicit and explicit embrace by lawmakers aimed at solidifying the punishments for virtually all types of crime (Agnew,

1993). At the macro-level, Alder, Schminke, Noel, and Kuenzi (2008) found that many of the variables specified to test the deterrence perspective were regularly among the weakest predictors of crime rates across nearly all levels of aggregation. The results of studies that adopt GDT are inconclusive, and many authors have called for further research to better understand what factors influence the effectiveness of security countermeasures (D'Arcy & Hovav, 2009). Although the literature shows that employees' perceptions of sanctions produce a decrease in internal systems abuse by employees (D'Arcy et al., 2009; Lee et al., 2004; Straub, 1990), different researchers found that deterrent factors are less effective in predicting or reducing system abuse (Hu et al., 2010), while others point to an increased frequency of computer abuse after changes to security policies and procedures are made (Moore, Cappelli, & Trzeciak, 2008). These conflicting findings indicate there are likely scenarios where increased deterrence measures may create negative results and a paradox of increased internal system abuse.

Researchers argued that people make decisions based on simplifying strategies and heuristics, which often lead to biases and errors in the resulting decision. In addition, they argue that RCT is inadequate to explain how individuals make decisions in real life, and because of their limited information-processing capacities, people tend to rely on some heuristic principles, which enable them to reduce the complexity of problems (McCarthy, 2002; Shumarova & Swatman, 2006). In contrast, the Technology Acceptance Model (TAM) is specifically designed for modeling user acceptance of information systems, and more importantly, it provides a basis for tracing the impact of external factors on internal beliefs and intentions (Davis et al., 1989). The TAM is also reported to be easy and simple to use, has the ability to predict, and posits the power of explanation, which gives practitioners and researchers the ability to recognize why certain systems might be acceptable or unacceptable (Davis et al., 1989; Hubona & Cheney, 1994; Lee, Kozar, & Larsen, 2003). Specifically, my study is different than the work of Bulgurcu et al. (2010a) in the primary focus which is built on how the inherent characteristics of the policies, as perceived by the users, affect their intention to comply, while the primary focus of the Bulgurcu et al. (2010a) is on how the incentive structures (e.g., rewards, benefits, cost, and sanctions) affect the users' intention to comply. Moreover, my Security Acceptance Model (SAM) captures the complexity of the ISPs while Bulgurcu et al. (2010a) did not, and from an abstract point of view, and regardless of rewards,

SAM is driven by acceptance of the intrinsic characteristics of the ISPs, and therefore is expected to be easy to understand.

Based on the above arguments, the TAM was adopted as the foundation for my model as it is better than TRA in explaining the acceptance intention of users (Davis et al., 1989; Lee et al., 2003), simpler and easier to use, more powerful than TPB and RCT (Bulgurcu et al., 2010a; Hubona & Cheney, 1994; Lee et al., 2003), and TAM's instrument is reliable and valid, which will enhance the value of research (Lee et al., 2003). Moreover, TAM is designed to be used with voluntary and mandatory systems (Davis et al., 1989), and is valid for application in different cultures and with different systems (Lee et al., 2003; Straub, 1994). It is also designed to be used alone, without needing another theory to support it, to understand why people accept or reject using a system, unlike previous studies which adopted more than two theories to build their models (e.g. Anderson & Agarwal, 2010; Bulgurcu et al., 2010a; Dinev & Hu, 2007). Therefore, SAM can be used to understand users' compliance behavior, and is expected to possess all of TAM's distinctiveness, as well as being easy, simple, valid, and applicable in different cultures and with all ISPs.

## **CHAPTER THREE**

### **RESEARCH MODEL AND HYPOTHESES**

Employees can impose excessive damage to the confidentiality, integrity, or availability of information security (IS) through deliberate activities (e.g., espionage), or they may present a potential threat through passive noncompliance with security policies, laziness, poor training, or lack of motivation to intensely ensure information security (Warkentin & Willison, 2009). In order to foster employees' rule adherence, Tyler and Blader (2005) classified studies in organizational behavior that classify employees' rule-following behavior into two motivation approaches of human behavior. The first is the command-and-control approach, which is linked to extrinsic motivational models of human behavior, where individuals respond to external contingencies such as reward and punishment, and breaking the rules. The second approach is the self-regulatory approach, which is linked to intrinsic motivational models, and which emphasizes that individuals follow the rules as connatural drivers of behavior. The intrinsic motivational model of human behavior was found to explain employees' rule-following behavior better than the extrinsic motivational model, which has been built on GDT, RCT, PMT, and other extrinsic behavioral theories (Son, 2011).

The command-and-control model symbolizes a conventional approach to animate rule-following; it is based on the idea that people abide by the rules as a function of the costs and benefits they associate with doing so (Blair & Stout, 2001; McCarthy, 2002). This approach is well represented in different theories such as GDT (e.g. D'Arcy & Hovav, 2009; Siponen & Vance, 2010; Straub, 1990), RCT (e.g. Bulgurcu et al., 2010a; Hu et al., 2010; Li, Zhang, et al., 2010), and PMT (e.g. Herath & Rao, 2009b; Johnston & Warkentin, 2010; Siponen et al., 2007). The approach contends that employees are materialistically motivated and will be basically interested in the resources and outcomes they obtain from their organizations, and

therefore in order to enforce policies, rules, and procedures, organizations must take an active role by providing incentives (to encourage desired behavior) and sanctions (to discourage undesirable behavior) (Tyler, Callahan, & Frost, 2007).

The question to ask at this point is do such techniques work? Studies indicated that these strategies often help shape employees' behavior (e.g. Bulgurcu et al., 2010a; D'Arcy & Hovav, 2009; Li, Sarathy, & Zhang, 2010; Straub, 1990). But such strategies also come with significant costs. For example, in order for sanctions and deterrence systems to work, organizations must be able to dedicate substantial resources to the surveillance needed to detect systems misuse or abuse so that people are deterred (Tyler et al., 2007).

In this study I focused on the self-regularity approach which represents an alternate approach to encouraging rule-following behavior, which is concentrated on employees' intrinsic motivations. This method identifies rule-following as an individual's innate desire to follow organizational rules, and not with external contingencies in the environment that are linked to rule-following, such as rewards, penalty, fear, outcomes, or social pressure (Tyler & Blader, 2005). Therefore, the Technology Acceptance Model (TAM) works to investigate employees' innate behavior toward complying with organizations' ISPs, since it concentrates on employees' desire and willingness to follow the rules, as described in the ISPs, for the sake of protecting the organization's security, and not to maximize any outcomes for themselves. Consequently, this study developed a Security Acceptance Model (SAM), analogous to the TAM.

Chapter Three introduces the study's research model, along with its theoretical base, and a description of each construct and its foundation in the information security (IS) literature. Specific hypotheses were identified, and related prior research that contributed to the development of these hypotheses is presented.

## **Theoretical Framework**

### **Theory of Reasoned Action (TRA) vs. Theory of Planned Behavior (TPB)**

Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TBP) are two of the most widely researched and popular conceptual frameworks for the study of human behavior (Ajzen, 2002b; Armitage & Conner, 2001). These theories are widely used in information

systems; they were adapted by Davis (1986) to develop the Technology Acceptance Model (TAM). Both theories are built on the assumption that human behavior is determined by behavioral intentions, and behavioral intentions are a function of an individual's attitude toward the behavior and subjective norms surrounding the performance of the behavior (Ajzen, 1991). A meta-analysis study conducted by Sheppard, Hartwick, and Warshaw (1988) to investigate the effectiveness of the TRA found strong evidence for the utility of the model in predicting behavioral intentions, and actions appropriate for detecting where and how to target strategies for changing behavior.

The Theory of Reasoned Action (TRA) (Figure 1) assumes that "since much human behavior is under volitional control, most behaviors can be accurately predicted from an appropriate measure of the individual's intention to perform the behavior in question" (Fishbein & Ajzen, 1975, p. 380). The theory posits that explicit behavior can be predicted from the individual's intention, where intentions are an indicator of how much time and effort people are willing to devote and planning to put forth to perform the behavior (Ajzen, 1991). Under volitional control, the theory postulates that "a person's intention to perform (or not perform) a behavior is the most important immediate determinant of that action" (Ajzen, 2005, p. 117), and intention alone is a sufficient predictor of the actual behavior (Fishbein & Ajzen, 1975) under circumstances where there are no constraints on action. Antecedents to behavioral intentions were divided into behavioral (personal in nature) and normative (social influence) factors; the personal factors are assumed to be the individual's attitude toward performing the behavior, whereas the normative beliefs influence the individual's subjective norm about performing the behavior (Ajzen, 1988; Madden, Ellen, & Ajzen, 1992). As explained by Fishbein and Ajzen (1975), external variables to the model are expected to influence intentions only to the extent that they affect either attitudes or subjective norms.

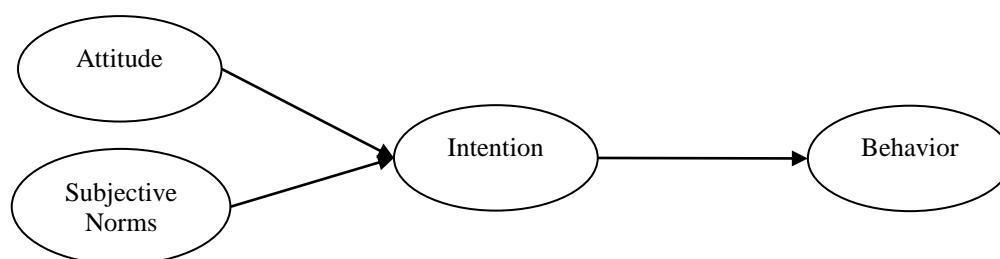


Figure 1: Theory of Reasoned Action (Ajzen, 1988)



Fishbein and Ajzen (1975) model was developed to deal with behaviors that are under volitional control and not outcomes or events that result from behaviors. This model holds well within the constraints they defined; however, researchers identify some situations that do not fit neatly within this framework (Armitage & Conner, 2001). Some behaviors are involitional, so intention alone is not a sufficient predictor of the future behavior (Sheppard et al., 1988). A behavioral criterion always contains an action element; intention implies that an individual will work forward to perform a certain behavior. However, the degree of success of achieving the required behavior depends not only on the person's intention, but also on other factors that are beyond the person's direct control. Thus, the volitional assumption restricted the applicability of the TRA to volitional behaviors (Ajzen, 2005).

Ajzen (2005) acknowledged that “complications are encountered, however, when we try to apply the theory to behaviors that are not fully under volitional control” (p. 127). To overcome this limitation, an extension of this model was developed, the Theory of Planned Behavior (TPB) (Figure 2), to address the possibility of incomplete volitional control by adding an additional construct, perceived behavioral control (Ajzen, 1991), which received a great deal of attention in different fields, including compliance with information security policy (e.g. Bulgurcu et al., 2010a; Herath & Rao, 2009b; Warkentin, Johnston, et al., 2011; Zhang et al., 2009). Perceived Behavioral Control (PBC) is defined as “people's perceptions of the ease or difficulty of performing the behavior of interest” (Ajzen, 1991, p. 183). As the theory assumes, PBC has a direct and indirect effect on behavior through intentions (Ajzen, 1991, 2005), and it aims to allow prediction of behaviors that were not under complete volitional control. In general this theory stands on the idea that “people intend to perform a behavior when they evaluate it positively, when they experience social pressure to perform it, and when they believe that they have the means and opportunities to do so” (Ajzen, 2005, p. 118).

In summary, the Theory of Reasoned Action (TRA) could sufficiently predict the behavior under volitional control under certain constraints, but the simple array of an intention is not enough to predict behavior (Armitage & Conner, 2001). TRA does not deal directly with the amount of control a person has in a given situation, and it considers the possible effects of perceived behavioral control (PBC) on achieving the behavioral goal (Ajzen, 2005). PBC has a different influence on intention. For instance, in some situations where attitudes are strong,

PBC's prediction power of intention might be low. Ajzen (1991, p. 188) state that "The relative importance of attitude, subjective norm, and perceived behavioral control in the prediction of intention is expected to vary across behaviors and situations". Accordingly, PBC will have lower predictive utility of intentions in situations where attitudes or normative influences are strong. Therefore, the magnitude of the PBC–intention relationship is dependent upon the type of behavior and the nature of the situation (Ajzen, 1991; Armitage & Conner, 2001).

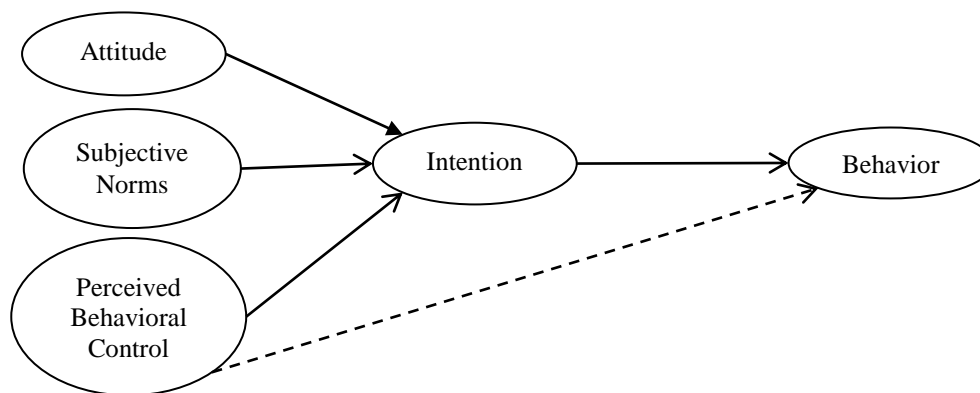


Figure 2: Theory of Planned Behavior (Ajzen, 1988)

### **Technology Acceptance Model**

The Technology Acceptance Model (TAM) proposed by (Davis, 1986) is one of the most frequently used models of IT adoption (Agnew, 1985, 1991). According to the TAM (Figure 3), actual adoption of technology is influenced by two perceptions; perceived usefulness (PU) and perceived ease-of-use (PEOU). PU is defined as "the degree to which a person believes that using a particular system would increase his or her performance", whereas PEOU refers to "the degree to which a person believes that using a particular system would be free of effort" (Davis et al., 1989, p. 320). TAM is an adaptation of TRA, specifically modified for modeling user acceptance of information systems (Davis et al., 1989). TAM is developed to provide a clarification of the general determinants of computer acceptances, which is capable of describing users' behavior. Beside the ability to predict, TAM posits the power of explanation, which gives the practitioners and researchers the ability to recognize why certain systems might be acceptable or unacceptable (Davis et al., 1989).

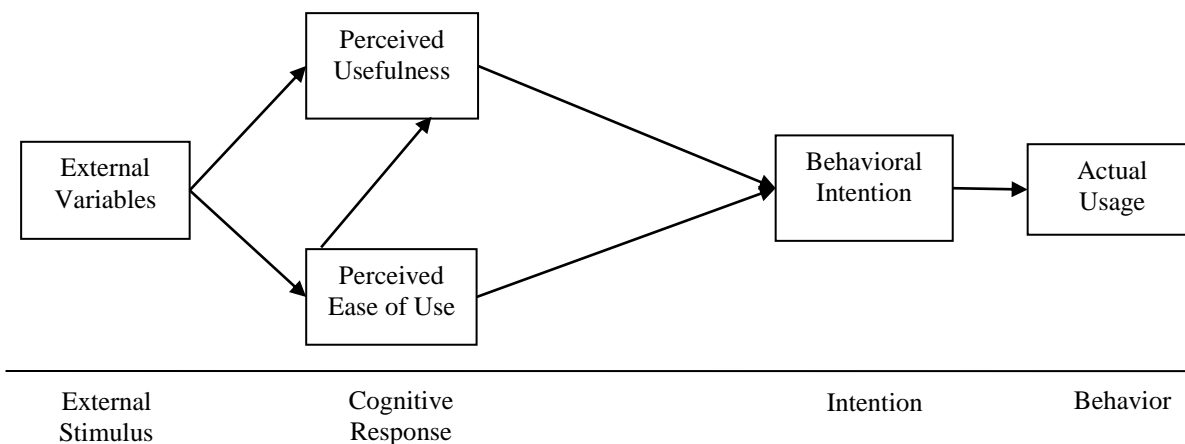


Figure 3: Technology Acceptance Model (TAM) adopted from (Davis et al., 1989)

The TAM consists of four variables; Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Behavioral Intention (BI), and Behavior or Actual Usage (B). PU is an independent variable as it predicts BI, and it is a dependent variable as predicted by PEOU. Studies show that there are strong relationships between these variables ; PU and PEOU are strong predictors of BI (Lee et al., 2003). This model assumes that BI is a strong determinant of computer usage, but differs from TRA in that BI is determined by a person's attitude toward using a system (A) and PU (Davis et al., 1989). TRA postulates that any other factors which influence behavior do so only indirectly by influencing Attitude (A) and Subjective Norms (SN); these factors are referred to as external variables (Peguero, Popp, Latimore, Shekarkhar, & Koo, 2011). This indicates that TRA mediates the impact of uncontrollable variables and controllable interventions on user behavior (Davis et al., 1989).

According to the TAM, PU can be affected more than PEOU by a variety of external variables, as well; PEOU is also hypothesized to be determined by external variables. Thus, the objective design of a system can have a direct and indirect effect, through PEOU, on PU (Davis et al., 1989). Studies show that when different external variables were introduced into TAM, the most frequent variables used as external variables, as Lee et al. (2003) found, are system quality, training, compatibility, computer anxiety, self-efficacy, enjoyment, computing support, and experience.

After the brief analysis of the TRA, TBP, and TAM, the question arises here is, which theory is better to explain and predict behavior? And what is the criterion for selecting the

appropriate theory? Ajzen (2005) stated that: “Volitional control is best defined as a continuum; ... purely volitional act ... and behavioral events which are completely beyond volitional control... Toward the volitional side of the continuum, it is possible to predict behavior with a great deal of accuracy on the basis of intentions to perform the behavior in question. Intentions also contribute to the attainment of behavioral goals that are only partly under volitional control .... Perceived behavioral control can reflect the presence of such factors and, to the extent that it does so accurately, contributes to the prediction of behavioral achievement” (p. 140). This statement implies that intention is a sufficient predictor of behavior under volitional control; therefore, TRA is preferred over TPB, but compliance with ISPs is not volitional, and therefore TRA will not be able to predict behavioral intention toward compliance if it is mandatory. The TAM is designed to explain and predict the behavior while TRA is designed merely to predict the behavior .TAM includes the external variables as a tested predictor, tools for explaining and predicting the behavior, and it was found to be an appropriate model in mandatory sittings (e.g. Venkatesh & Davis, 2000; Venkatesh, Morris, Davis, & Davis, 2003) . Therefore, TAM is a better model to predict and explain the users’ behavior toward the compliance with ISPs.

### **The Role of Attitude in the TAM**

Davis et al. (1989) distinguished between TAM and TRA. They are similar because they both posit that attitude is determined by one’s own belief, but they differ on two significant issues. First the TRA contends that beliefs are extracted further for each new context, while the TAM contends that PU and PEOU’s are based on theory and meant to be determinants of user acceptance. Second, the TRA is the sum of all the beliefs multiplied by weight into a single construct, whereas TAM deals with PEOU and PU as two separate constructs. Davis et al. (1989) stated that “TAM treats [P]U and [P]EOU as two fundamental and distinct constructs. Modeling beliefs in this disaggregated manner enables one to compare the relative influence of each belief in determining A[attitude], providing important diagnostic information.... From a practical standpoint, this enables an investigator to better formulate strategies for influencing user acceptance via controllable external interventions that have measurable influences on particular beliefs.” (p. 988).

Since its introduction, many empirical studies have been done on behavioral intentions to use different applications that give support for the TAM; communication systems such as email (Straub, 1994), general purpose systems such as e-commerce (Gefen & Straub, 2000), office systems such as spreadsheets (Venkatesh & Davis, 1996), specialized business systems such as case tools (Xia & Lee, 2000), and Decision Support Systems (DSS), Group Support Systems (GSS) and Group Decision Support Systems (GDSS) (Sambamurthy & Chin, 1994). The original model of TAM validated attitude as a mediator variable, while later studies eliminated attitude from the model (e.g. Adams, Nelson, & Todd, 1992; Davis & Venkatesh, 1996; Koufaris, 2003; Venkatesh, 2000; Venkatesh & Davis, 2000). Thus, a direct path, without attitude as a mediating construct, from PU and PEOU to BI, was proposed. The elimination of attitude as a mediating construct contradicts TRA and TPB which posit that attitude mediates the relationship between beliefs and intention. Davis et al. (1989) stated that “within organizational settings, people form intentions toward behaviors they believe will increase their job performance, over and above whatever positive or negative feelings may be evoked toward the behavior per se” (p. 986). These direct paths of PU-BI and PEOU-BI imply that even if employees may dislike the technology, they may still use it if they perceive it will enhance their job performance (Dinev & Hu, 2007). In addition, Venkatesh et al. (2003) eliminated the role of attitude in their Unified Theory of Acceptance and Use of Technology (UTAUT). They argued that attitude toward using technology is not to be a direct determinant of intention, and found that it is a significant predictor only when performance and expectancies constructs are not present in the model. Therefore, they assume any observed relationship between attitude and intention to be spurious and resulting from the exclusion of the other key construct.

Different empirical studies validated the original TAM in which attitude mediates the relationships between PU and PEOU, and behavioral intention. In studies that validated the complete mediation of attitude between PU and PEOU, and behavioral intention, results show that attitude was a significant mediator (e.g. Agarwal & Prasad, 1997; Karahanna, Straub, & Chervany, 1999; Taylor & Todd, 1995).

## Research Model and Hypotheses

Based on the TAM developed by Davis et al. (1989), a Security Acceptance Model (SAM) (Figure 4) is proposed, which will help explain employees' intention to comply with ISPs. TAM is built on the premise that the greater the readiness of the users to accept a new system, the more likely they are to make changes in their practices, and the more willing they are to spend the time and effort to actually start using the system. About 30 different types of IS were used as target systems in TAM studies (Lee et al., 2003). Analogous to this approach, SAM is based on similar premises, with recognition that information security policies are not a technology, but a system that users will use and comply with. In that regard, we draw on Bulgurcu et al. (2010a, p. 527) definition of information security policy as a "statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations".

This study will examine the effect of external variables, namely users' awareness of security protection mechanisms (security policies, Security Education, Training and Awareness (SETA) programs, and monitoring practices) proposed and tested by Straub (1990), D'Arcy et al. (2009), and D'Arcy and Hovav (2009); controllability (Dinev & Hu, 2007; Rhee et al., 2009); information security awareness (Bulgurcu et al., 2010a); and self-efficacy (Dinev & Hu, 2007; Workman et al., 2008), on perceived usefulness of protection and perceived complexity of ISPs. Information security awareness general security awareness, and technology awareness, is hypothesized to directly influence employees' perceived usefulness toward compliance with ISPs. The original relations in the TAM model are posited to hold in the context of ISPs too; perceived complexity and perceived usefulness of protection of ISPs are postulated to impact behavioral intention to comply.

As for the IT usage in the original TAM, I focused on intention to comply rather than intention to use, since it is more realistic in mandatory settings, and fits better in the sense of compliance. Users perceived compliance with organizations' ISPs as a compulsory action by the organization. The literature review raised a number of issues related to mandatory vs. volitional usage behavior; some suggest a continuum of voluntariness (e.g. Hartwick & Barki, 1994; Karahanna et al., 1999; Moore & Benbasat, 1991) in which individuals may perceive voluntary differently. Also usage can be variable in mandatory settings, but that depends on

how much the system/technology is integrated into one's job, producing a high correlation with job function but not necessarily with effect toward the system (Brown, Massey, Montoya-Weiss, & Burkman, 2002). Accordingly, and as the system (compliance with ISPs) must be used to complete one's own job that is also integrated with other employees' jobs, this study proposes that employees do not have a decision regarding use or not. Discussed below are the operationalization of the research constructs and the formation of the study hypotheses.

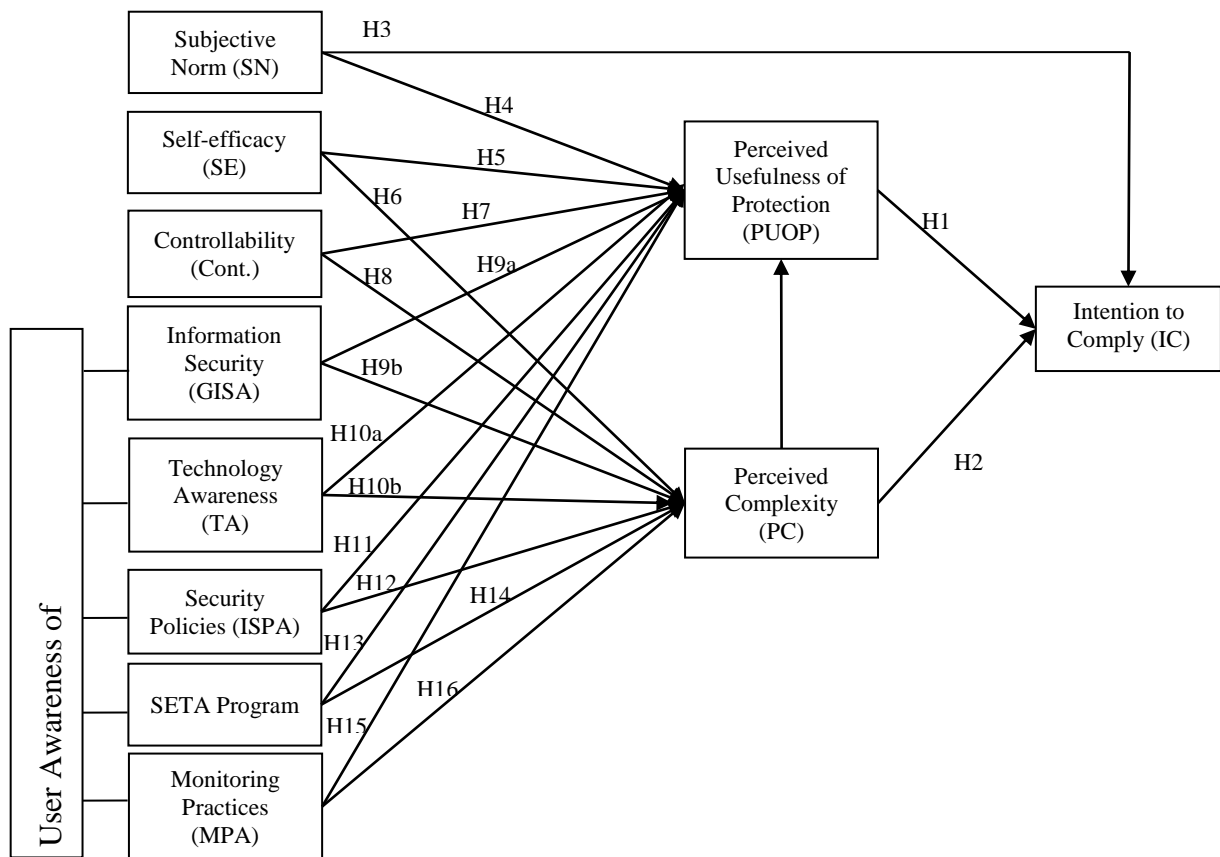


Figure 4: Research Model - Security Acceptance Model (SAM)

### Constructs Adapted from TAM

#### *Perceived Usefulness of Protection and Perceived Complexity*

Theoretically, perceived usefulness is defined as “the degree to which an individual believes that using a particular system would enhance his or her job performance” (Davis, 1989, p.

320), and perceived ease of use is defined as “the degree to which a person believes that using a particular system would be free of effort” (Davis, 1989, p. 320), whereas intention to comply is defined as an “employee’s intention to protect the information and technology resources of the organization from potential security breaches” (Bulgurcu et al., 2010a, p. 529).

In accordance with the existing literature, particularly TAM, it is assumed that an employee’s intention to comply with the requirements of the organization’s ISPs is associated with the degree to which the employee believes that using ISPs’ roles and responsibilities to safeguard the organization’s information technology resources will enhance his/her job performance (PUOP). PU is a key determinant of IT usage (acceptance) and it is described as the most prominent belief driving IT (Bhattacharjee & Premkumar, 2004). PU has always been shown to be a significant and strong determinant of behavioral intention, with predicted standardized coefficients typically around 0.6 (Venkatesh & Davis, 2000). The effect of PU on behavioral intention toward compliance with ISPs or using protective technologies to secure information assets was investigated by (Dinev & Hu, 2007), (Dinev et al., 2009), (Jones, 2009), and (Xue et al., 2010). Congruent with the original TAM, these studies proposed that PU positively affects behavioral intention to comply or to use protective technologies. The use of PU in this study is consistent with the literature (Davis et al., 1989; Dinev & Hu, 2007; Venkatesh & Davis, 2000; Venkatesh et al., 2003; Xue et al., 2010).

Based on the previous literature that has investigated the effect of PU on behavioral intention in the IS domain, and principally in information security compliance, the following is hypothesized in the context of ISP compliance:

*Hypothesis H1: An employee’s PU about complying with the organization’s ISP positively affects intention to comply with the requirements of the ISP.*

An employee’s intention to comply with the requirements of the organization’s ISP is associated with the degree to which an employee believes that using the ISP in practice, and undertaking related roles and responsibilities, is difficult to understand, learn, or operate. Perceived ease of use and perceived complexity (the opposite of ease of use) have been used interchangeably in innovation diffusion literature (Davis, 1989; Igbaria, Parasuraman, & Baroudi, 1996). Due to the nature of ISPs, this study will investigate perceived complexity of



compliance with ISPs rather than perceived ease of use. Perceived complexity was identified by (Rogers, 1995) as one of five perceived characteristics of an innovation that influences adoption; trialability, observability, compatibility, relative advantage, and complexity. According to (Rogers, 1995, p. 257), perceived complexity is defined as “the degree to which an innovation is perceived as relatively difficult to understand and use”.

Perceived complexity has been widely investigated in human computer interaction literature and captures users’ personal interpretations of the systems and their interaction with it (Nadkarni & Gupta, 2007). A meta-analysis study by Tornatzky and Klein (1982) found that out of the 25 innovation characteristics, complexity was one of the most frequently studied by researchers, and was always found to be a significant factor. Users’ involvement is expected to be more critical where task and/or system complexity are higher (Mahmood, Burn, Gemoets, & Jacquez, 2000). Studies found that the higher the complexity the less the intention or the behavior toward using the system. For example, Chang and Cheung (2001) found that complexity negatively affected intention to use the Internet, and Igbaria et al. (1996) found that perceived complexity negatively affected system usage and perceived usefulness. Thompson, Higgins, and Howell (1994) found that as individuals become more experienced, they perceive they can handle the complexity of a computer. In an earlier study Thompson, Higgins, and Howell (1991) also reported a strong negative affect of perceived complexity on utilization of PCs. The TAM also proposed an indirect relationship between PEOU and behavioral intention through PU (Davis, 1989), and this relationship is hypothesized the same except the direction of the affect will be negative since complexity is the opposite of PEOU.

Based on the previous literature that has investigated the effect of PEOU (opposite of PC) on behavioral intention in an IS domain and principally in information security compliance, and the discussion above, the following is hypothesized in the context of ISP compliance:

*Hypothesis H2a: An employee’s PC of ISPs will negatively affect intention to comply with the requirements of ISPs.*

*Hypothesis H2b: An employee’s PC about complying with the organization’s ISPs negatively affects PUOP to comply with the requirements of ISPs.*

## **Constructs Adapted from the Theory of Planned Behavior**

### ***Subjective Norm***

Under the assumptions of TPB, an intention to perform a behavior is guided by three factors: beliefs about the likely consequences or other attributes of the behavior (behavioral beliefs), beliefs about the normative expectations of other people (normative beliefs), and beliefs about the presence of factors that may further or hinder performance of the behavior (control beliefs) (Ajzen, 1988, 2002b). Normative beliefs result in perceived social pressure or subjective norms (SN) (Ajzen, 2002a) which are defined as “the person’s perception of social pressure to perform or not perform the behavior under consideration” (Ajzen, 1988, p. 117). Davis et al. (1989) did not include subjective norm (SN) in the TAM as it is the least understood aspect of TRA, and it was also assumed that computer use was voluntary. Despite that, many studies incorporate the construct thereafter, where it was found to have a significant effect on intention in mandatory settings but not voluntary ones (Hartwick & Barki, 1994; Venkatesh & Bala, 2008; Venkatesh & Davis, 2000; Venkatesh et al., 2003). Venkatesh and Davis (2000) refer to the causal mechanism underlying this effect as compliance. They posit that the direct compliance effect of SN on intention is theorized to operate whenever a person perceived that an important referent(s) wants him/her to perform a specific behavior, and that referent(s) has the ability to reward behavior or punish non-behavior.

Based on TRA and TBP, the direct relationship between subjective norm and behavioral intention is established on compliance, while TAM does not include SN. Technology Acceptance Model 2 (TAM2) incorporates two additional theoretical correlations by which SN has an influence on intention directly and indirectly through PU (Venkatesh & Davis, 2000). Under this theoretical base, if a superior suggests that a particular system is useful, a person might believe it is actually useful and then form an intention to use it. Venkatesh and Bala (2008) found that the effect of subjective norm on behavioral intention was stronger in a mandatory setting and SN was a significant determinant of PU. In the information security domain, subjective norm was found to be a significant predictor of behavioral intention to comply or use protective security measures (e.g. Anderson & Agarwal, 2010; Bulgurcu et al., 2010a; Dinev & Hu, 2007; Herath & Rao, 2009b). Therefore based on the literature that has

investigated the relationships among the TBP, TAM2, and Technology Acceptance Model 3 (TAM3) constructs, the following hypotheses are proposed:

*Hypothesis H3: An employee's subjective norm about complying with the organization's ISPs positively affects intention to comply with the requirements of ISPs.*

*Hypothesis H4: An employee's subjective norm in complying with the organization's ISPs positively affects PUOP to comply with the requirements of ISPs.*

### ***Self-Efficacy and Controllability (Perceived Behavioral Control)***

Perceived behavioral control (PBC) can function as a surrogate for actual control and contribute to the prediction of the behavior in question to the degree that people are realistic in their judgments of a behavior's difficulty, and under the condition they have actual control over the behavior (Ajzen, 1991, 2002b). The concept of PBC was introduced to the TPB to overcome situations where behavior is mandatory or nonvolitional (Ajzen, 1991, 2002b). Empirical evidence shows that self-efficacy (SE) and controllability (C) can be manipulated and distinguished across behaviors (Pavlou & Fygenson, 2006), however Ajzen (2002b, p. 678) asserts that "the fact that it is possible to distinguish reliably between two different types of control - SE and controllability - does not invalidate the unitary nature of the [PBC] construct". C and SE are separable components of *Perceived Behavioral Control* (PBC) (Ajzen, 2002b), which will allow for a more detailed examination of external control beliefs (Pavlou & Fygenson, 2006). These beliefs can reflect internal as well as external factors (Ajzen, 2002b).

Self-efficacy (SE) is a construct that has been examined in an exploratory sense in studies pertaining to an individual's use of IS (Rhee et al., 2009). Studies found that SE is a significant predictor of behavioral intention (e.g. Pavlou & Fygenson, 2006; Rhee et al., 2009; Venkatesh, 2000; Venkatesh & Davis, 1996). In the information security domain, SE was found to be a significant predictor of behavioral intention to comply with ISPs or to use protective security measures (e.g. Bulgurcu et al., 2010a; D'Arcy & Hovav, 2009; Dinev & Hu, 2007; Herath & Rao, 2009b; Johnston & Warkentin, 2010; Pahnla et al., 2007). Self-efficacy (SE) is defined as a "subjective probability that one is capable of executing a certain course of action" (Ajzen, 1988, p. 105). Consistent with this definition, this study defines SE as an employee's confidence in their ability, skills, and knowledge about satisfying the

requirements of ISPs. Previous studies have empirically validated that SE has a significant positive effect on the PEOU (e.g. Agarwal, Sambamurthy, & Stair, 2000; Venkatesh, 2000), and on PU (Lai, 2009; Ong, Lai, & Wang, 2004; Ong & Lai, 2006). The confidence in one's security related knowledge and abilities can be expected to serve as the basis for judgment about how easy or difficult compliance with an organization's ISP will be, meaning that individuals with a high computer SE magnitude might expect themselves to be able to accomplish more difficult tasks or to complete them with less support and assistance (Venkatesh, 2000). In the same vein of TAM, PU reflects the person's beliefs or expectations; therefore, SE might be an important factor affecting PU (Chau, 2001). Therefore, it is hypothesized:

*Hypothesis H5: An employee's self-efficacy in complying with the organization's ISPs positively affects PUOP to comply with the requirements of ISPs.*

*Hypothesis H6: An employee's self-efficacy in complying with the organization's ISPs negatively affects PC to comply with the requirements of ISPs.*

Controllability (C) is defined as "individual judgments about the availability of resources and opportunities to perform the behavior" (Ajzen, 2002b, p. 672; Pavlou & Fygenon, 2006, p. 119). The definitions of self-efficacy and controllability revealed that SE reflects internal personality factors, while C reflects beliefs about external factors (Dinev & Hu, 2007), however, there is no evidence to support this view (Ajzen, 2002b). According to Ajzen (2002b), some studies employed either one item or a mixture of both items, and debate surrounding the conceptualization of SE and C, and their relationship to PBC, still exists (Trafimow, Sheeran, Conner, & Finlay, 2002). Previous studies have demonstrated the combined set to be a better predictor of intentions (Ajzen, 2002b). Pavlou and Fygenon (2006) viewed PBC as a formative two-dimensional construct formed by two underlying indicators; SE and C. Controllability was found to be significant in predicting behavior but not intentions, while SE was found to be significant in predicting intentions (Ajzen, 2002). Relationships between C and PU and PEOU have been examined in previous studies. Kim, Park, and Oh (2008) found C to have an indirect impact on a respondent's continued intention to use through its impact on PEOU. Trafimow et al. (2002) argue that if a behavior is not controllable, then there is not much need to consider performing it, suggesting that a higher

degree of controllability is an indication of a higher degree of certainty (Hu & Dinev, 2005), making individuals feel more comfortable to comply. Therefore, the following is hypothesized:

*Hypothesis H7: An employee's controllability positively affects PUOP to comply with the requirements of ISPs.*

*Hypothesis H8: An employee's controllability negatively affects PC to comply with the requirements of ISPs.*

## **Information Security Awareness**

### ***User Awareness of Information Security***

Goodhue and Straub (1991) were the first scholars to denote the importance of awareness as a factor in users' beliefs about information security. They believed that computer abuse is a key problem that will not dwindle on its own, because "a lack of awareness of the danger may lead to weak vigilance by users and greater potential for abuse" (p. 14). They also argued that "... people who are more aware of the potential for abuse would be sensitized to the dangers of inadequate security and would more likely feel that security was unsatisfactory" (p. 15). Information Security Awareness (ISA) is defined as an "employee's overall knowledge and understanding of potential issues related to information security and their ramifications" (Bulgurcu et al., 2010a, p. 532). Employees are expected to be aware and knowledgeable of information security and cognizant of security technology, and should be able to formulate a general perception of what it entails. This definition is coherent with the belief that ISA is used to "refer to a state where users in an organization are aware of and ideally committed to their security mission" (Siponen, 2000, p. 31).

An individual's awareness and knowledge of information security is built from life experiences, such as having been attacked by a virus, opening unknown emails, being penalized for not complying to security policies and regulations, or obtaining information from external resources such as the Internet, newspapers, or security journals (Bulgurcu et al., 2010a; Goodhue & Straub, 1991). Goodhue and Straub (1991) associated awareness to computer literacy and define awareness as years of experience, managerial level, and user/systems staff status. However, results reveal weak support of their hypothesis that users'

awareness of the technology will cause them to have higher concern for security, and they attributed that to the fact that years of experience with information systems is a weak measure of security awareness. Fishbein (2008) argues that there are an infinite number of variables that may directly or indirectly influence the performance (or nonperformance) of any behavior. TPB posits that background factors (e.g., social, demographic, experience, knowledge, and values) may be related to or influence behavior indirectly by affecting behavioral, normative, and control beliefs (Ajzen, 2005). In this context, it can be argued that employees' ISA, conceived of as a background factor, may play a role in the development of their outcome beliefs, along with compliance behavior. Therefore, it is hypothesized:

*Hypothesis H9a: An employee's general ISA positively affects PUOP toward complying with the requirements of ISPs.*

*Hypothesis H9b: An employee's general ISA negatively affects PC toward complying with the requirements of ISPs.*

### **Technology Awareness**

The second component of information security awareness (ISA) is users' awareness of technological issues. Dinev and Hu (2007) define technology awareness as a "user's raised consciousness of and interest in knowing about technological issues and strategies to deal with them" (p.391). It sounds very logical for employees to be aware of all issues surrounding compliance with ISPs before they form either negative or positive beliefs about that. Employees must make themselves aware of all potential threats and how compliance with ISPs help protect information assets, and they also must be aware of the consequences of noncompliance, and of the availability and effectiveness of protective technology (Dinev & Hu, 2007). As the concept of awareness first appeared in the innovation diffusion theory (Rogers, 1995), general information security awareness and technology awareness was explained in the framework of an innovation-decision process, in which knowledge influences persuasion, which in turn influences decisions. In this context, ISA can be viewed as knowledge, perceptions (usefulness and complexity) as persuasion, and intention to comply as a decision. Building on this process, employees can gain significant "awareness knowledge" about different information security threats and protective technologies, along with knowledge about how and what they are supposed to do with regard to information security,

which will subsequently lead to compliance behavior (Bulgurcu et al., 2010a). Accordingly, knowledge of information security threats can be viewed as general information security awareness, and knowledge about what employees are supposed to do can be viewed as technology awareness.

Based on this argument, as ISA (knowledge) influences perceptions of usefulness and complexity (persuasion) which, in turn, influences the decision to comply with the ISP, the following is hypothesized:

*Hypothesis H10a: An employee's Technology Awareness positively affects PUOP toward complying with the requirements of ISPs.*

*Hypothesis H10b: An employee's Technology Awareness negatively affects PC toward complying with the requirements of ISPs.*

## **User's Awareness of Security Countermeasures**

### ***Security policies***

According to Straub (1990), security countermeasures include both deterrent and preventive controls. Security policies, SETA programs, and monitoring practices were identified as deterrent controls that can be used by organizations to prevent information systems misuse (Straub, 1990). The direct effect of these countermeasures on IS misuse intention has been reported by D'Arcy and Hovav (2009) and D'Arcy et al. (2009). Information security policy is defined as a "state of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations" (Bulgurcu et al., 2010a, pp. 526-527). Organizations develop security policies to ensure the security of information assets and to encourage end-user behavior that helps protect information assets from threats posed to them. Accordingly, if an organization's end-users are not eager or are unwilling to comply with security policies, then these efforts are useless (Herath & Rao, 2009b). Literature in information security policies shows a need for empirical studies on security compliance (Herath & Rao, 2009b).

Previous studies have shown that awareness of ISPs will decrease the behavioral intention to systems misuse (D'Arcy & Hovav, 2009; D'Arcy et al., 2009; Straub, 1990). Herath and Rao (2009b) found that if users perceive that their compliance has a positive effect on the

organization, they are more likely to have a positive attitude toward the security policies. Security policy can be best utilized by making sure that users understand it and accept necessary precautions (D'Arcy et al., 2009). So in order to improve security efforts, policies regarding proper and improper use of IS should be established, and then should be taught to the users. The more detailed these policies are, and the more the users are aware and educated about acceptable system use (Straub, 1990), the greater the employees' perceptions about the usefulness of protecting the IS, and the less their perception of complexity. Therefore, it is hypothesized:

*Hypothesis H11: An employee's awareness of IS security policies positively affects PUOP toward complying with the requirements of ISPs.*

*Hypothesis H12: An employee's awareness of IS security policies negatively affects PC toward complying with the requirements of ISPs.*

### **SETA Program**

Organizations develop different measures to manage and control systems misuse; SETA programs are a form of security countermeasure that educating users about has significant security benefits (Dhillon, 1999; Straub & Welke, 1998). Awareness campaigns and education help modify certain behaviors such as illegal drunk driving and shoplifting (D'Arcy et al., 2009). Such training and awareness programs are extremely important in developing "trusted" members of the organization (Dhillon, 1999). In the same context, the ongoing SETA programs convey knowledge about threats in the organizational environment; they help reduce system abuse and promote compliance with the ISPs by providing information about the appropriate use of IS, as well as the disciplinary actions taken by the firm, including policies and sanctions for violations. They also provide the necessary knowledge of enforcement activities, and reveal threats to local systems and their vulnerability to attack (D'Arcy et al., 2009; Straub & Welke, 1998; Wybo & Straub, 1989). According to Straub and Welke (1998, p. 445), the wisdom behind SETA programs is to "convince potential abusers that the company is serious about security and will not take intentional breaches of this security lightly".

To increase users' awareness, ongoing education and training programs should be developed and maintained (Goodhue & Straub, 1991). According to Whitman and Mattord (2009),



SETA programs are designed to improve an organization's information security by improving employees' awareness of the needs to protect information resources, and developing users' knowledge and skills to perform more secure tasks. SETA programs are rooted in information security policy (D'Arcy et al., 2009; Peltier, 2005) and can take many forms, such as reviewing an organization's code of conduct (Harrington, 1996), or more general strategies that promote awareness of day-to-day security issues (Furnell et al., 2002). Based on that, and on the fact that SETA programs are designed to enhance employees' awareness, knowledge, and education of all security issues that will help them to comply with the requirements of the ISPs, we posit that SETA programs will increase employees' perceptions about the usefulness of compliance with ISPs and help overcome the hurdles and complexity with compliance. Therefore, it is hypothesized:

*Hypothesis H13: An employee's awareness of SETA programs positively affects PUOP toward complying with the requirements of ISPs.*

*Hypothesis H14: An employee's awareness of SETA programs negatively affects PC toward complying with the requirements of ISPs.*

### ***Monitoring Practices***

Managers seek to reduce the sources of noncompliance behaviors with ISPs and look for solutions to help with this quest. In response to that, organizations use monitoring practices to increase and enforce employees' compliance with rules and regulations (Urbaczewski & Jessup, 2002) and distribute information about organizational guidelines for acceptable system usage (Straub, 1990). Monitoring practices has two basic uses; providing feedback and implementing control. The feedback function intends to monitor employees so as to provide them with necessary suggestions for improvement. Monitoring for control is aimed at employee observation in order to foster compliance with rules and regulations (Urbaczewski & Jessup, 2002). When monitoring was used to give employees feedback on productivity while ignoring the control scenario, Chalykoff and Kochan (1989) found that for some employees the negative effects of monitoring are inherent, while for others its negative impact can be mitigated by attention to feedback processes. Another study found that employee task performance improved when they were monitored; either by a person or through computer monitoring (George, 1996). A question to be asked here is; can monitoring be conducted to

increase employees' perceived usefulness of protection and eventually form a desirable behavior toward compliance with ISPs?

To gain conformity with rules and regulations, organizations adopt monitoring practices (D'Arcy et al., 2009; Urbaczewski & Jessup, 2002) using different techniques to achieve this, including security audit, tracking users' internet usage, and recording network activities (D'Arcy et al., 2009). Studies have found that monitoring practices lead to a decrease in information resource misuse as it enables the detection of serious and deliberate misuse incidents that are likely subject to severe punishment (D'Arcy et al., 2009; Straub & Nance, 1990).

In this study, monitoring practices have been investigated as a security countermeasure ; "policing" in order to gain compliance with rules and regulations, such as monitoring email traffic and Internet use, as well as other network activities (Panko & Beh, 2002; Urbaczewski & Jessup, 2002). Accordingly, in this study, it is argued that the use of monitoring practices from a policing perspective will increase the difficulty and complexity of compliance with the ISPs, and will affect employees' perceived usefulness of protection since they have no immediate benefits for them in terms of job performance and satisfaction Therefore, we hypothesized:

*Hypothesis H15: An employee's awareness of monitoring practices negatively affects PUOP to comply with the requirements of ISPs.*

*Hypothesis H16: An employee's awareness of monitoring practices positively affects PC to comply with the requirements of ISPs.*

## **CHAPTER FOUR**

### **RESEARCH METHODOLOGY**

This chapter addresses the methodology of the study, and begins by discussing the research design, followed by the presentation of the instrument design and a validation of the survey instrument. The chapter concludes with a discussion of the sampling and data collection procedure.

#### **Research Design**

The current study model, the Security Acceptance Model (SAM), is based on the Theory of Planned Behavior (TPB) and the Technology Acceptance Model (TAM). The basic premise of these theories is that behavioral intention is a function of perception, attitude, and perceived behavioral control. Such constructs are hard to observe and measure directly as they represent an internal state, and therefore are “measured through indirect indicators, such as verbal expressions or overt behavior” (Zikmund, 2003, p. 308). Considering it “is difficult to get accurate information about internal states, such as attitudes or emotions, with anything other than self-reports” (Spector, 2006, p. 229), and since “self-reports of participants via surveys, questionnaires, and interviews are a very common way to gather data in almost all of the social sciences” (Kline, Sulsky, & Rever-Moriyama, 2000), self-reports were utilized to measure all study constructs. People are expected to be able to report many internal states, including attitudes, emotions, perceptions, and values (Spector, 2006).

A field study approach was used to test the research model over a controlled experimental design since it was argued that experimental and case researchers were less likely to validate their instruments than field study researchers (Straub, 1989). Field studies according to Kerlinger (1973) are described as strong in realism, significant, and encompassing heuristic quality. Field study can be defined as "any scientific studies, large or small, that

systematically pursue relations and test hypotheses, that are ex post facto, and that are done in life situations like communities, schools, factories, organizations, and institutions" (Kerlinger, 1973, p. 405). Unlike controlled designs where experimental treatment and manipulation of the independent variables can happen, field studies are "non-experimental inquires occurring in natural systems where researchers cannot manipulate independent variables or control the influence of confounding variables" (Boudreau, Gefen, & Straub, 2001, p. 3).

For data collection techniques in field studies, a questionnaire is the most common method used (Boudreau et al., 2001), as it provides a "quick, inexpensive, efficient, and accurate means of assessing information about the population" (Zikmund, 2003, p. 175), and findings can be generalized to the population studied (Pinsonneault & Kraemer, 1993). However, different shortcomings are associated with this method, such as a weak questionnaire design, and potential issues with sampling procedures and sampling size, survey administration, and pretest of the questionnaires (Boudreau et al., 2001). To overcome these pitfalls, an extensive survey of literature regarding ISPs and compliance behavior was reviewed. In addition, having clearly defined independent and dependent variables, and a specific model of the expected relationships among these variables (Pinsonneault & Kraemer, 1993), are important requirements to help enhance the research design. Finally, well-researched, known, and used theories [the Theory of Planned Behavior (TPB) and the Technology Acceptance Model (TAM)], have been utilized as a theoretical framework for this study. The research model depicted in Figure 4 contains strong a priori theoretical relationships as specified by these theories, and supported, when needed, with other theoretical frameworks. Constructs of the study were developed from previously validated instruments, which have been standardized and adapted to the context of this study. To ensure greater reliability and validity, the survey instrument was refined based on feedback obtained from information security faculty members in the United States and Jordan, as well as from a number of employees working at a variety of banks in Jordan. Based on the feedback, several items were reviewed and modified. A pretest of the refined questionnaire was conducted to evaluate the reliability and validity, using a confirmatory factor analysis (Al-Omari, El-Gayar, & Deokar, 2012).

The study design can be classified as a non-experimental, cross-sectional survey design in which all data were collected at once. Using Campell and Stanley (1963), the research design is diagrammed as follows:

X                      O

Where X is the “treatment” and O is an observation. In the context of the current study, the treatment is having an information security policy at the organization.

### Survey Instrument Design

An initial survey instrument was developed by identifying and creating appropriate measurements based on a comprehensive literature review. The survey instrument is based on constructs validated and tested in prior research (Bulgurcu et al., 2010a; D'Arcy et al., 2009; Davis, 1989; Dinev & Hu, 2007; Herath & Rao, 2009a, 2009b; Rhee et al., 2009; Siponen et al., 2010), standardized and adapted to the context of this study. According Straub (1989) using validated and tested items will improve the reliability of results. The constructs include intention to comply, PUOP, PC, users’ awareness of general information security, technology awareness, subjective norm and users’ awareness of ISPs, SETA programs, and computer monitoring. The instrument also collected key demographic information. All constructs were measured reflectivity with multiple items on seven-point Likert scales. A pretest and pilot test were conducted to ensure the conceptual precision and face validity of the constructs. Table 4.1 presents all of the study constructs along with the types, source, and number of their measurement items. A complete version of the questionnaire is provided in Appendix B.

Table 4.1: Sources of Measurement Items

Construct	Type	Source	Items
Intention to Comply	Reflective	Bulgurcu et al. (2010a) and Siponen et al. (2010)	7
Perceived Usefulness of Protection	Reflective	Davis (1989)	13
Perceived Complexity	Reflective	Davis (1989)	12
Self-Efficacy	Reflective	Bulgurcu et al. (2010a) and Herath and Rao (2009b)	6
Controllability	Reflective	Dinev and Hu (2007) and Rhee et al. (2009)	4
User Awareness of General Information Security	Reflective	Bulgurcu et al. (2010a) and Dinev and Hu (2007)	3
General Information Security Awareness	Reflective		4
Technology Awareness			
User Awareness of Information Security Policies	Reflective	D'Arcy (2005); D'Arcy et al. (2009) and Bulgurcu et al. (2010a)	9
User Awareness of SETA Program	Reflective	D'Arcy (2005), and D'Arcy et al. (2009)	9
User Awareness of Computer Monitoring	Reflective	D'Arcy (2005) and D'Arcy et al. (2009)	7
Subjective Norm	Reflective	Herath and Rao (2009b)	5

**Demographics:** To identify and describe the characteristics of the participants, some demographic variables were collected, including gender, age, educational level, total years of experience, and years of experience in the current bank. Other demographic variables related to the work were collected as well, including the number of hours of using the computer at work, the organizational hierarchical level, and the type of software or databases used in the work site. Although some previous studies investigated the effect of demographic variables (control variables) on policy compliance or system abuse, no hypotheses were developed in this study regarding this; demographic information was merely used to describe the study sample.

**Intention to comply:** Intention to comply is measured with seven items, five of which were adopted from Bulgurcu et al. (2010a) and two from Siponen et al. (2010). The items assess employees' behavioral intention to comply with the requirements of the ISPs of their bank, and the employees' intention to carry out their responsibilities as described in the bank's ISP to protect information and technology resources. It also assesses their intention to recommend and assist others in complying with ISPs. Bulgurcu et al. (2010a) reported a reliability higher than .88 for the three items, and Siponen et al. (2010) reported values exceeding the suggested threshold of 0.60 for three items. Participants were asked to indicate the degree of their behavioral intention to compliance on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7), with higher scores indicating higher behavioral intention.

**Perceived usefulness of protection:** Perceived usefulness of protection is measured with a thirteen-item scale adapted from Davis (1989). The items measure three main things pertaining to usefulness of compliance to enhance protection; compliance effectiveness, productivity and time savings, and importance of compliance to one's job. Perceived usefulness was investigated by three researchers in the security domain. Dinev and Hu (2007) reported a reliability of 0.81 for the three items, Xue et al. (2010) reported a reliability of .84, and finally, Jones (2009) reported a reliability of 0.95. In the IS field, this construct has been used extensively and validated, and it has been found to be a rigorous and reliable construct (Lee et al., 2003). Participants were asked to indicate their behavioral intention to compliance degree on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7), with higher scores indicating higher perceptions of usefulness of protection.

**Perceived complexity:** Perceived complexity is measured with a twelve-item scale adapted from Davis (1989). The items measure three main complexities; physical effort, mental effort, and perceptions of how complex compliance is to learn and do. The majority of the studies in the information systems domain investigated the perception of ease of use, and the results always revealed a high reliability coefficient (Lee et al., 2003). In the security domain Dinev and Hu (2007) reported a reliability of 0.81 for the three items, Xue et al. (2010) reported a reliability of .90, and finally, Jones (2009) reported a reliability of 0.92. Participants were asked to indicate their behavioral intention to compliance degree on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7), with higher scores indicating higher perceptions of complexity to comply with ISP.

**Self-efficacy:** Self-efficacy is measured using six items adapted from Bulgurcu et al. (2010a) and Herath and Rao (2009b). The first three items assessed employees' confidence in their personal skills, knowledge, or competency about fulfilling the requirements of ISPs, whereas the other three items assessed their confidence in their ability to comply with the requirements of the ISPs on their own. This construct has been investigated in the IS field and is found to be a significant predictor of behavioral intention (Lee et al., 2003) Likewise, this construct was found to be a significant predictor of behavioral intention in the information security domain as well (e.g. Anderson & Agarwal, 2010; Bulgurcu et al., 2010a; Herath & Rao, 2009b; Siponen et al., 2007). Respondents were asked to indicate their level of agreement on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7).

**Controllability:** Controllability is measured using four items, three of which were adapted from Dinev and Hu (2007), and the fourth from Rhee et al. (2009). Items assess respondents' judgment about the availability and capability of resources, and opportunities to comply with the requirements of ISPs. Dinev and Hu (2007) reported a reliability of .92 for a three-item scale. Response options for the items are measured on a seven-point Likert scale, ranging from (1) strongly disagrees to (7) strongly agree.

**General information security awareness:** General information security awareness is measured using three items adapted from Bulgurcu et al. (2010a). The items assess respondents' overall knowledge and understanding of all probable matters related to information security and their consequences and complications. Bulgurcu et al. (2008) and

Bulgurcu et al. (2010a) reported a reliability higher than 0.90 for the three item scale. Respondents were asked to indicate their level of agreement on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7).

***Technology awareness:*** Four items were used to measure technology awareness adapted from Dinev and Hu (2007). The construct items measure respondents' perception of and interest in knowing about technological issues and strategies that help them comply with the requirements of the ISP, so they can help protect the organization's information assets. Dinev and Hu (2007) reported a reliability of .93 for this four-item scale. In another study, Dinev et al. (2009) investigated the effect of technology awareness on intentional behavior in different countries and reported a high reliability value of .86 in South Korea. Respondents were asked to indicate their level of agreement on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7).

***User awareness of information security policies:*** User awareness of information security policies is measured with nine items, seven of which were adapted from D'Arcy (2005), and the other from Bulgurcu et al. (2010a). The items measure respondents' knowledge and understanding of the requirements established in the bank's ISP and the aim of those requirements. Researchers reported a high reliability score for this construct; for example, D'Arcy (2005) reported a reliability of .89 for a seven-item scale. Respondents were asked to rate their level of agreement or disagreement with each of the items on a seven-point scale, ranging from (1) strongly disagree to (7) strongly agree.

***User awareness of SETA program:*** The security, education, training, and awareness program is measured with nine items, eight of those adapted from D'Arcy (2005) and D'Arcy et al. (2009), with the ninth being developed for this study. These items measure respondents' awareness of education and training programs at their organization that help improve their compliance behavior and enhance their awareness of information security issues. D'Arcy (2005) reported a reliability of .88 for the eight-item scale. Respondents were asked to indicate their level of agreement on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7).

***User awareness of computer monitoring:*** User awareness of monitoring practices is measured with seven items adapted from D'Arcy (2005) and D'Arcy et al. (2009). These items



assess the respondents' awareness of monitoring practices that include, but are not limited to, tracking users' internet usage and recording network activities. D'Arcy (2005) reported a reliability of .87 for the seven-item scale. Respondents were asked to indicate their level of agreement on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7).

**Subjective norm:** Five items were used to measure the subjective norm adapted from Herath and Rao (2009b). These items assess respondents' perceptions of social pressure about compliance with the requirements of the bank's ISP, which is a result of their beliefs about how important people would like them to behave in this regard. High reliability scores were recorded in the IS field and in information security; Herath and Rao (2009b) reported a reliability score higher than .88 for the five-item scale. Respondents were asked to indicate their level of agreement on a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7).

## **Survey Instrument Validation**

### **Face and Content Validity**

Boudreau et al. (2001) argued that each instrument must be pretested as a primary step to eliminate any unexpected future difficulties. Therefore, a pretest of the study instrument was conducted with a group of specialists from the United States and Jordan. The questionnaire was sent to a carefully selected group of information security researchers and faculty members in the United States and Jordan (Five MIS faculty members and researchers in the US and five MIS faculty members in Jordan), and to a number of employees working at variety of banks in Jordan (Five individuals), to see whether the items seemed like a good translation of the construct. Each one of these individuals received an electronic copy of the drafted questionnaire along with an explanation of the purpose of the study, study questions, and construct definitions. They were asked to respond to the survey by indicating the appropriateness of the item in measuring the construct, and if the item was not appropriate, they were asked to recommend changing or deleting it, or recommending other items. They were also asked to comment on the content and structure of the instrument as a whole. Employees were asked to focus and comment more on the understandability of the

questionnaire items, language issues, level of difficulty, and implication issues related to ISPs, than were the faculty and researchers.

Unfortunately, only seven out of ten questionnaires were returned to the researcher from the faculty, and two from banks employees. The feedback focused primarily on language issues and suggested revising the wording of some of the questions to eliminate ambiguity. The survey instrument was refined based on the feedback obtained and several items were reviewed and modified. To make sure that all recommended feedback was taken into account, the questionnaire was sent to one MIS faculty member in the US and one faculty and one bank's employee in Jordan to confirm that the changes enhanced the readability and understandability of the instrument, in addition to confirming if the items measured the target constructs. The result of the pretest suggested that the instrument possesses both types of translation validity; face and content.

### **Construct and Discriminant Validity**

After the pretest, a pilot study was conducted on a convenience sample of 205 employees from four different banks in Jordan. The pilot test served several purposes. First, it helped ensure that the time needed for filling out the survey was reasonable. Second, the data collected from this pilot group were analyzed and used in calculating different validity measures.

In order to assess the measurement quality of the eleven reflective scales, convergent validity, reliability, and discriminant validity were calculated. The distribution of all variables was analyzed, and it was found that all variables included in the model were normally distributed. Later, Exploratory Factor Analysis (EFA) was conducted to calculate measurement quality of the constructs. The number of factors was left to be defined by the Eigenvalue, which produced 11 factors (all their Eigenvalues are greater than 1.00) which are the number of constructs included in the model. All 11 factors accounted for 63.2% of the total variance.

To provide an adequate basis for proceeding to an empirical examination of adequacy for factor analysis at the overall level, as well as for each variable, an inspection of the correlation matrix was done. This revealed that most of the correlations are significant at 0.01 level. Bartlett's test was used to assess the overall significance of the correlation matrix and found to be significant at the 0.0001 level. To assess the patterns between variables, the measure of

sampling adequacy (MSA) was computed. The overall MSA value was 0.788, which is higher than the acceptable range (above 0.50) (Hair, Black, Babin, Anderson, & Tatham, 2009). As for each variable, MSA values were also found to be higher than the acceptable threshold of 0.50 (Hair et al., 2009).

To measure convergent validity, factor analysis was performed using the principal component extraction method, followed by orthogonal varimax rotation. Convergent validity captures how well the measurement items relate to the construct, and it is acceptable if factor loadings of each measurement item with the one construct it is related to is at 0.70 or higher, and each item loads significantly on its latent construct (Gefen & Straub, 2005). The unrotated component analysis factor matrix revealed that some of the items did not load highly on their hypothesized factor or on any other factors. Varimax rotation was performed based on this observation, and most of the items loaded well on their latent constructs. Items that had low factor loadings or those that cross loaded on other factors were removed from the analysis. Results from the final rotated factor pattern matrix indicate that all items loaded with significant t-values on their respective latent constructs and have loading values above 0.70. Therefore, all these reflective scales exhibit sound convergent validity (Gefen & Straub, 2005; Gefen, Straub, & Boudreau, 2000).

To confirm the scale reliability and internal consistency, composite reliability (CR) and average variance extracted (AVE) for the pilot study was examined. A scale is deemed to be reliable if it has CR above 0.70 and an AVE of more than 0.50 (Gefen et al., 2000). Results show that all the reflective scales were reliable. To establish discriminant validity, both the loading and cross loading matrix and the correlation matrix were examined (see Al-Omari et al., 2012). All measurement items found to load more strongly on their respective construct than on other constructs, which were found to be less than 0.50 for all items in the study (Gefen et al., 2000). Second, Table 4.2 shows that the square root of AVE of each construct is higher than the correlations between that construct and any other construct (inter-correlations) (Fornell & Larcker, 1981). As shown in the table, all constructs in the model satisfy these criteria for discriminant validity. Consequently, the measurement tool demonstrates adequate reliability and validity required for further data collection for testing the hypotheses.

Table 4.2: Composite Reliability, AVE, and Latent Variable Correlations

	CR	AVE	MPA	Cont.	GISA	IC	ISPA	PC	PUOP	SE	SETA	SN	TA
MPA	0.876	0.780	<b>0.883</b>										
Cont.	0.865	0.783	0.123	<b>0.885</b>									
GISA	0.841	0.838	0.134	0.333	<b>0.916</b>								
IC	0.823	0.787	0.123	0.150	0.394	<b>0.887</b>							
ISPA	0.826	0.796	0.201	0.276	0.415	0.266	<b>0.892</b>						
PC	0.832	0.775	0.168	0.242	0.443	0.260	0.374	<b>0.880</b>					
PU	0.892	0.683	0.124	0.253	0.358	0.253	0.368	0.376	<b>0.826</b>				
SE	0.905	0.767	0.136	0.268	0.325	0.352	0.294	0.259	0.161	<b>0.876</b>			
SETA	0.837	0.880	0.246	0.058	0.122	0.217	0.225	0.170	0.117	0.133	<b>0.938</b>		
SN	0.837	0.769	0.030	0.043	0.009	0.041	0.075	0.036	0.098	0.050	0.035	<b>0.877</b>	
TA	0.865	0.798	0.202	0.254	0.269	0.301	0.379	0.474	0.310	0.339	0.083	0.051	<b>0.893</b>

CR = Composite reliability; AVE = Average Variance Extracted; MP = Monitoring Practices; Cont. = Controllability; GISA = General Information Security Awareness; IC = Intention to Comply; ISPA = Information Security Awareness; PC = Perceived Complexity; PU = Perceived Usefulness of Protection; SE = Self-Efficacy to Comply; SETA = Security, Education, Training and Awareness; SN = Subjective Norms; TA = Security Awareness.

Diagonal elements in bold display the square root of AVE.

Finally, a paper presenting the pilot test results was published (Al-Omari et al., 2012). Results revealed that all constructs in the model satisfy the criteria for discriminant validity, and that all the reflective scales were reliable.

## Sampling and Data Collection

### Sample Size

Representativeness of the sample and correctly choosing the appropriate sample size is very critical as it can significantly weaken the generality of the findings (Boudreau et al., 2001) and influence the detection power of the significant relationships and interactions. Statistical tests with larger sample sizes are more likely to be overly sensitive, whereas for a small sample size, statistical tests will be insensitive and fail to detect even large effects (Hair et al., 2009; Straub, 1989). However, the smaller the sample size the less its precision (Boudreau et al., 2001), and the harder to determine whether findings are generalizable or peculiar to the case (Poole & DeSanctis, 2004). Since statistical significance reflects sample size and effect size, two studies might have different results and conclusions using the same model, as a result of having two different sample sizes (Biddle & Marlin, 1987; Fornell & Larcker, 1981). Therefore, an appropriate sample size should be selected; not so small that only large effects are detectable, nor so large that it is overly sensitive and detects small effects of little scientific importance.

Inferences in cross-sectional self-report survey studies are made from a sample which is believed to be representative of the population. The precision of the inference is highly dependent on the degree to which the information available in a sample reflects population information. The general rule is that the larger the sample size the “more information is available and, therefore, more confidence can be expressed for the model as a reflection of the population process” (Tanaka, 1987, p. 134). The question is how large of a sample is required to be representative, or more specifically, to deduce research findings back to a population? Unfortunately, there is no precise answer for this question as recommendations vary drastically. Gorsuch (1983) proposed a ratio of 5 participants per measured variable and that the sample size should be higher than 100. Hair et al. (2009) suggested that sample size should be a minimum of 200 participants and recommended that researchers should always try to obtain the highest cases-per-variable ratio. Everitt (1975) suggested a ratio of 10 participants per measured variable. Bentler and Chou (1987) provide a rule of thumb that under normal distribution the ratio of sample size to number of variables should be 10:1 to obtain significant tests.

Obviously there is no consensus between researchers and methodologists on a “rule of thumb” that can be relied upon to determine the best sample size. Hair et al. (2009) argued that these “previous guidelines ... are no longer appropriate” (p. 635); they suggested model complexity and basic measurement model characteristics should determine the sample size. Partial Least Square (PLS) was used to analyze the data. One guideline for setting sample size in PLS according to Gefen et al. (2000) requires a sample size of ten times the most complex construct in the model. Accordingly, if the most complex relationship involved a construct with six formative indicators, the required minimum sample size would be 60. Based on the previous discussion, and with a fairly complex model with ten or more constructs, most with seven or more observable items, and following Hair et al. (2009) recommendation, a minimum sample of 800 was needed to test the study model.

### **Data Collection**

Most of the previous IS literature on ISP compliance or misuse has focused solely on IS employees (Bulgurcu et al., 2010a; D'Arcy et al., 2009; Herath & Rao, 2009a; Li, Zhang, et al., 2010; e.g. Siponen et al., 2007; e.g. Straub, 1990). This study reflects a large number of

bank employees who are required to comply with their bank's ISPs. The population for the current study is all employees, who speak and understand English, and who are working at any bank in Jordan that already has a developed ISP that they are currently using. The target sample was a large mix of employees from different banks working in different departments (i.e., tellers, research and design, marketing and sales, and information technology) at different hierarchical levels (i.e., non-managerial, line management, senior, and CEOs), with various years of experiences at a bank.

The study participants were bank employees for several reasons. First, banks are a prime target for hackers, given that they maintain important information about customers, and have access to large amounts of monetary assets. Second, banks employ individuals with a diverse range of ages, education levels, and job titles, which allows for a representative sample. Finally, banks are heavy users of information technology, networks, and the Internet.

The data were gathered from Jordan for a few reasons. First, Jordan is the home country of the researcher, giving him access to different sectors such as banking and education. Second, Jordan is considered one of the largest computer user countries in the Middle East after UAE. Third, Jordan has a strong banking system that started to employ technology quite a while ago. Finally, Jordan is now starting to be a prime target for hackers because of the current absence of detailed regulations and laws in place to protect information resources in banks.

A list of all banks in Jordan that have ISPs in action were developed based on the researcher's personal contact, and through various contacts obtained from Dr. Aleassa, at Yarmouk University in Jordan, who also administered the questionnaire distribution. An email was sent to about twenty large bank administrators (either CEO or chief information officer or human resource department), which described the benefits and costs involved in participating in this research. Approximately one week after the email, each executive/manager was contacted by the researcher or by the survey administrator, and their willingness to participate in the research was determined. Thirteen large banks agreed to participate, but the rest declined for various reasons, such as time constraints and security concerns. Of the thirteen banks, nine were found to have a written and clear ISP under action, with most of their employees being fluent in English. The executive/manager from the nine banks was asked to provide a name of the contact person who would serve as a liaison with the researcher and the survey administrator, and facilitate the survey administration. Each designated contact person was

given an abstract description of the purpose of the study and the questionnaire, along with instructions for survey distribution. Specifically, the contact persons were instructed on the concept of random sampling and asked to randomly select a sample of employees from different departments, at different hierarchical levels, and with different years of experience and educational levels. They were also asked to equally survey both males and females.

Although a paper-based survey is expensive, and slow and difficult to deliver to respondents at different geographical locations, it was still selected as a method for collecting data because banks do not have business emails for their employees for security reasons, most communication with employees is done on paper or by phone, and most importantly, the researcher was told by some banks' CEOs that they do not have a list of personal emails for their employees, also for security reasons. In July – October of 2010, the researcher provided the instrument to the survey administrator who made copies with a "cover letter" attached to each copy. The survey administrator delivered about 150 copies for each contacted person at the nine banks, who then personally distributed the questionnaire to the randomly selected employees in the different bank branches. The cover letter emphasized the anonymous nature and confidentiality of the survey, and explained that participation was voluntary and withdrawing from the study was possible at any time without any consequences. The survey administrator contacted the liaison person within each bank approximately every week and collected the completed questionnaires and provided him with more copies when needed. As a primary screening process, participants were asked about their awareness of the existence of the ISPs and about their fluency in the English language. Only those participants that indicated some awareness with ISPs and those that were fluent in English were included in the survey study.

Two thousand one hundred and seventeen (2117) employees received the questionnaire, and nine hundred and thirty seven (937) filled it out, for an initial response rate of 44 percent. The researcher went over every questionnaire and deleted incomplete or unusable entries from the dataset. Every questionnaire that was less than 90 percent completed (Meaning that it was missing at least one question from each construct) was discarded. Of the questionnaires that were completed, a check question was used to see if the respondents fully read and understood the questionnaire. If the answers were contradictory, the questionnaire was discarded. A total of 878 questionnaires were found to be usable, for a response rate of 41 percent.

A random sample of employees at different job levels and in different departments at nine banks was taken. Usually a sample size of 10 to 20 percent of all employees is used with this type of sampling technique. According to Hair et al. (2009), a general rule is to have at least five times as many observations as the number of variables to be analyzed, and a more acceptable sample size would have a 10:1 ratio. Structural Equation Modeling (SEM) requires a larger sample relative to other multivariate approaches; Hair et al. (2009) stated “when the number of factors are larger than six, some of which use fewer than three measured items as indicators, and multiple low communalities are present, sample size requirements may exceed 500” (p. 742).



## **CHAPTER FIVE**

### **DATA ANALYSIS AND RESULTS**

This chapter presents the data analysis and results of the hypotheses tests. The chapter begins with a description of the study sample, along with the initial instrument validation. The Partial Least Square (PLS) is used to test the validity and reliability of the instrument, and a description of the hypothesized relationships in the research model is presented. Finally, results of the PLS analysis is presented for the structural model.

#### **Sample Characteristics and Descriptive Statistics**

Employees at banks in Jordan which have developed ISPs in action represented the study population. A random sample was collected from employees working in nine different banks. Table 5.1 contains the demographic profile of the survey participants.

As shown in table 5.1, of the 878 respondents in the final sample, 44% were female, 68.9% were in the 20-29 age range, 62.8% held a bachelor's degree, and more than 16% held advanced degrees. The majority of the sample (54.6%) had 1 to 5 total years of experience. The table also shows a diverse distribution of jobs in various departments at different organizational levels; 25.9% were in middle management and 3.4% were CEO/president. The average length of computer usage was 9.93 years, the average use of the computer at work was 6.29 hours per days, and the average period of speaking English was 10.44 years. Participants reported using different computer software such as spreadsheets, word processing packages, e-mail, programming languages, database applications, and their bank's special tailored software. The sample was quite evenly distributed in terms of the responsibilities of the respondents and in terms of the managerial level. The data collected represents a diverse employee population since it includes employees from local as well as international banks in Jordan.

Table 5.1: Sample Characteristics

Variable	Category	Frequency	Percentage
Sex	Male	492	56.0%
	Female	386	44.0%
Age	20-29 years	605	68.9%
	30-39 years	175	19.9%
	40-49 years	66	7.5%
	≥ 50 years	32	3.6%
Educational level	High School	61	6.9%
	Collage	122	13.9%
	Bachelor's Degree	551	62.8%
	Master's Degree	119	13.6%
	Doctoral Degree	25	2.8%
Experience	1-5 years	479	54.6%
	6-10 years	181	20.6%
	11-15 years	72	8.2%
	16-20 years	95	10.8%
	More than 20 years	51	5.8%
Years of experience with the current bank	Less than 6 months	142	16.2%
	6 months to 1 year	62	7.1%
	1 to 2 years	146	16.6%
	2 to 4 years	128	14.6%
	4 to 6 years	147	16.7%
	6 to 10 years	141	16.1%
	10 to 15 years	60	6.8%
	More than 15 years	52	5.9%
Functional area of work	Teller	160	18.2%
	Administration/Clerical	171	19.5%
	Information Technology	257	29.3%
	Audit	76	8.7%
	Marketing and Sales	132	15.0%
	Credit Department	82	9.3%
Organizational level	Non-management	238	27.1%
	Line Management (supervising non-management personnel)	188	21.4%
	Middle Management	227	25.9%
	Senior Management	142	16.2%
	Executive/Senior Vice President	53	6.0%
	CEO/President	30	3.4%
Computer software used for job-related work	Spreadsheets (e.g., Microsoft Excel)	564	64.2%
	Word processing (e.g., Microsoft Word)	589	67.1%
	E-mail	638	72.7%
	Programming languages (e.g., C++, Java, Visual Basic)	244	27.8%
	Application packages (e.g., accounting or payroll software)	201	22.9%
	Database applications	236	26.9%
	Bank's special tailored software	398	45.3%
Computer use at work (hrs./day)	Mean	6.29	
	Std. Deviation	2.67	
For how long you have been using the computer	Mean	9.93	
	Std. Deviation	5.73	
For how long you have been speaking English	Mean	10.44	
	Std. Deviation	7.53	

## **Initial Assessment of Validity and Reliability**

As a first step in the analysis, and before proceeding with testing the research model and hypotheses, the validity and reliability of the constructs were assessed. A construct will be considered valid if both convergent and discriminant validity are achieved (Straub, Boudreau, & Gefen, 2004; Trochim & Donnelly, 2006). Convergent validity means that “each measurement item correlates strongly with the one construct it is related to, while correlating weakly or not significantly with all other constructs, while discriminant validity is shown when each measurement item correlates weakly with all other constructs except for the one to which it is theoretically associated” (Gefen & Straub, 2005, p. 92). Reliability is concerned with measurement accuracy, and is “the extent to which the respondent can answer the same questions or close approximations the same way each time” (Straub, 1989, p. 151). To assess convergent validity, both item loading on constructs and Average Variance Extracted (AVE) need to be calculated. AVE measures the variance captured by the latent construct. As a rule of thumb, AVE should be more than 0.50 (Fornell & Larcker, 1981; Gefen & Straub, 2005).

## **Exploratory Factor Analysis**

As recommended by Heck (1998), EFA was conducted as an essential first step in data analysis when relationships among observed indicators and underlying factors are not tested or investigated beforehand. EFA basically classifies the essential latent variables that explain the pattern of correlations within a set of measurement items (Gefen & Straub, 2005). This study adopted different factors from different studies and built relationships between those variables that have never been tested or examined. Although most of the items for measuring the constructs were developed and tested in different studies in the information security policy compliance or misuse domain, some of these items adopted from the literature are being studied for the first time in the security domain. The most important reason for us to conduct this analysis is the fact that these items and relationships will be tested for the first time in Jordan. According to the SPSS manual, EFA objectives are “to establish that the measurement items converge into the appropriate number of theoretical factors, and that each item loads with a high coefficient on only one factor” (Gefen & Straub, 2005, p. 92).

To provide an adequate basis for proceeding to an empirical examination of adequacy for factor analysis at the overall level as well as for each variable, an inspection of the correlation

matrix as recommended by Hair et al. (2009) was done, and results revealed no substantial number of correlations higher than 0.30 inspected between items of different constructs, in other words, correlations between items of the same factor found to be high, and low correlations, were recorded with other factors items. This initially could give an indication that they are not explained to any great extent by the other variables, but do explain each other. Bartlett's test was used to assess the overall significance of the correlation matrix and found to be significant at the 0.0001 level. To assess the patterns between variables, the measure of sampling adequacy (MSA) was computed. The overall MSA value was 0.937; categorized as "meritorious", it is higher than the acceptable range (above 0.50) (Hair et al., 2009). As for each variable, MSA values were also found to be higher than the acceptable threshold of 0.50 (Hair et al., 2009).

Using SPSS version 17, an EFA with principle components analysis and varimax rotation method was conducted. The setup option regarding selecting the number of factors was left to be determined by the eigenvalue which is supposed to exceed 1.0. According to Hair et al. (2009) the choice of the rotation method, either orthogonal or oblique, should be based on the assumption and study needs of a given research problem. Since the goals of this study are to identify the underlying latent variables, and to signify that these factors are independent of each other, and to improve the interpretation by reducing some of the ambiguities that often accompany the preliminary analysis, varimax orthogonal rotational method was used. The result produced theoretically meaningful factors and the simplest factor structure (Hair et al., 2009).

For the factor loading acceptable level, guidelines from Hair et al. (2009) were adopted to assess the factor loadings. According to Hair et al. (2009) and Chin (1998) a .30 loading accounts for nearly 10 percent of the variance, while a .50 loading indicates that 25 percent of the variance is accounted for by the factor, and in order to account for 50 percent of the variance, a variable loading must exceed .70 . Based on these guidelines any item loaded less than .70 on an assigned factor, or loaded high on two factors (cross-loading), was deleted. As shown in table 5.2, EFA produced eleven factors with eigenvalues greater than 2.0, which is exactly the same number of factors investigated in the study. The eleven factors accounted for 76.71 percent of the total variance, which is higher than the generally accepted level of 60 percent (Hair et al., 2009).

Table 5.2: Measurement Items and Item Loadings

Items	Dimensions/Questions	Mean	STD	Loading
IC	<b>Intention to Comply</b>			
	I intend to comply with the requirements of the ISP of my organization	5.450	1.645	.863
	I intend to protect information resources according to the requirements of the ISP of my organization.	5.539	1.528	.859
	I intend to protect technology resources according to the requirements of the ISP of my organization.	5.527	1.607	.845
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information resources.	5.579	1.545	.830
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use technology resources.	5.569	1.505	.825
	I intend to recommend that others comply with ISP.	5.591	1.470	.785
	I intend to assist others in complying with ISP.	5.541	1.463	.740
	Eigenvalue = 9.579	Variance Explained = 12.773		
PUOP	<b>Perceived Usefulness of Protection</b>			
	My job would be easier to perform without complying with my organization's ISP	5.330	1.653	.747
	Complying with my organization's ISP gives me greater control over my work.	5.460	1.612	.799
	Complying with my organization's ISP does not hinder my job performance.	5.385	1.590	.784
	Complying with my organization's ISP addresses my job-related security needs.	5.375	1.688	.821
	Complying with my organization's ISP saves me time.	5.382	1.646	.833
	Complying with my organization's ISP enables me to accomplish tasks more securely.	5.443	1.590	.789
	Complying with my organization's ISP supports critical security aspects of my job	5.351	1.614	.812
	Complying with my organization's ISP reduces unproductive activities.	5.432	1.640	.782
	Complying with my organization's ISP enhances my effectiveness on the job.	5.375	1.591	.806
	Complying with my organization's ISP improves the quality of the work I do.	5.470	1.575	.796
	Complying with my organization's ISP improves my productivity.	5.409	1.571	.804
	Complying with my organization's ISP makes it easier to do my job.	5.396	1.585	.772
	Overall, I find complying with my organization's ISP useful in my job.	5.423	1.603	.770
Eigenvalue = 7.370	Variance Explained = 9.827			
PC	<b>Perceived Complexity</b>			
	I often become confused when complying with the requirements of my organization's ISP.	2.456	1.417	.946
	I make errors frequently when complying with the requirements of my organization's ISP.	2.483	1.445	.839
	Complying with the requirements of my organization's ISP is often frustrating.	2.634	1.592	.887
	Learning to comply with the requirements of my organization's ISP is hard for me	2.665	1.605	.872
	Compliance with the requirements of my organization's ISP requires a lot of mental effort.	2.498	1.503	.718
	I find it easy to comply with my organization's ISP.	2.270	1.266	.846
	It is easy for me to remember how to perform tasks while complying with my organization's ISP.	2.531	1.484	.935
	My organization's ISP provides helpful guidance in performing tasks.	2.605	1.559	.718
Eigenvalue = 7.152	Variance Explained = 9.536			
SE	<b>Self-Efficacy</b>			
	I have the necessary skills to fulfill the requirements of the ISP.	5.117	1.735	.774
	I have the necessary knowledge to fulfill the requirements of the ISP.	5.163	1.781	.807
	I have the necessary competencies to fulfill the requirements of the ISP.	5.052	1.741	.805
	I would feel comfortable following my organization's ISP on my own.	5.136	1.723	.806
	If I wanted to, I could easily comply with my organization's ISP on my own.	5.028	1.741	.781
	I would be able to follow most of ISP even if there was no one around to help me.	5.077	1.767	.746
Eigenvalue = 6.373	Variance Explained = 8.497			

Table 5.2 Measurement Items and Item Loadings (Continued)

Items	Dimensions/Questions	Mean	STD	Loading
Cont.	<b>Controllability</b>			
	I have the resources (like antivirus, firewall, brochures) to help me comply with the requirements of my organization's ISP.	5.588	1.509	.837
	I have the resources to protect my organization's information and technology assets from potential threats.	5.557	1.458	.785
	Threats to information security in my work are under control.	5.645	1.455	.793
	In general, technology used at my organization is advanced enough to prevent information security threats.	5.581	1.546	.747
	Eigenvalue = 5.478	Variance Explained = 7.304		
GISA	<b>General Information Security Awareness</b>			
	Overall, I am aware of the potential security threats and their negative consequences	5.489	1.502	.804
	I have sufficient knowledge about the cost of potential security problems.	5.335	1.655	.765
	I understand the concerns regarding information security and the risks they pose in general.	5.564	1.551	.882
	Eigenvalue = 5.355	Variance Explained = 7.140		
TA	<b>Technology Awareness</b>			
	I follow news and developments about the security related technologies.	5.390	1.603	.746
	I discuss Internet security issues or anecdotes with friends and people around me	5.440	1.553	.785
	I read about the problems of malicious threats attacking users' computers.	5.387	1.505	.775
	I seek advice about security issues through online discussion forums, magazines, and other media sources	5.397	1.591	.727
	Eigenvalue = 4.474	Variance Explained = 5.965		
ISPA	<b>User Awareness of Information Security Policies</b>			
	I am aware of my organization's rules of behavior for use of computer resources.	2.869	1.764	.791
	I am aware of my organization's specific guidelines that describe acceptable use of information systems.	2.875	1.815	.818
	I am aware that my organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use.	2.916	1.755	.836
	I am aware that my organization has a formal policy that forbids employees from installing their own software on work computers.	2.818	1.793	.822
	I am aware that my organization has specific guidelines that govern what tasks employees are allowed to perform on their work computers.	2.836	1.718	.808
	I am aware of my organization's specific guidelines that describe acceptable use of computer passwords.	2.790	1.733	.796
	I am aware that my organization has a formal policy that forbids employees from modifying computerized data in an unauthorized way.	2.874	1.721	.823
	I understand the rules and regulations prescribed by my organization's ISP.	2.821	1.748	.809
	I understand my responsibilities toward enhancing my organization's information system security as prescribed in the organization's ISP.	2.825	1.657	.778
	Eigenvalue = 3.798	Variance Explained = 5.064		
SETA	<b>User Awareness of SETA Program</b>			
	I am aware that my organization provides training to help employees comply with the organization's ISP.	5.248	1.696	.801
	I am aware that my organization provides training to help employees improve their awareness of computer and information security issues.	5.313	1.709	.816
	I am aware that my organization provides employees with education on computer software copyright laws.	5.236	1.707	.837
	I am aware that employees in my organization are briefed on the consequences of modifying computerized data in an unauthorized way.	5.315	1.714	.841
	I am aware that my organization educates employees on their computer security responsibilities.	5.238	1.712	.833

Table 5.2 Measurement Items and Item Loadings (Continued)

Items	Dimensions/Questions	Mean	STD	Loading
	I am aware that employees in my organization are briefed on the consequences of accessing computer systems that they are not authorized to use.	5.318	1.642	.836
	I am aware that employees in my organization are instructed in the appropriate usage of information technologies.	5.175	1.630	.829
	I am aware that my organization educates employees on their responsibilities for managing computer passwords.	5.297	1.620	.816
	I am aware that my organization educates employees on appropriate use of information technology resources (e.g. email).	5.265	1.683	.803
Eigenvalue = 2.945		Variance Explained = 3.926		
MPA	<b>User Awareness of Monitoring Practices</b>			
	I am aware that my organization monitors any modification or altering of computerized data by employees.	5.173	1.691	.790
	I am aware that employees' computing activities are monitored by my organization	5.352	1.630	.773
	I am aware that my organization monitors computing activities to ensure that employees are performing only explicitly authorized tasks.	5.286	1.687	.769
	I am aware that my organization reviews logs of employees' computing activities on a regular basis.	5.196	1.812	.835
	I am aware that my organization conducts periodic audits to detect the use of unauthorized software on its computers.	5.161	1.709	.830
	I am aware that my organization regularly monitors employee access to sensitive computerized information.	5.255	1.641	.803
	I am aware that my organization actively monitors the content of employees' work e-mail messages.	5.253	1.714	.809
Eigenvalue = 2.741		Variance Explained = 3.654		
SN	<b>Subjective Norm</b>			
	Upper level management thinks I should comply with the requirements of my organization's ISPs.	5.263	1.682	.803
	My boss thinks that I should comply with the requirements of my organization's ISPs.	5.292	1.706	.808
	My colleagues think that I should comply with the requirements of my organization's ISPs.	5.259	1.683	.814
	The information security/technology department in my organization thinks that I should comply with the requirements of my organization's ISPs.	5.240	1.644	.803
	Other computer technical specialists in the organization think that I should comply with the requirements of my organization's ISPs.	5.213	1.655	.779
Eigenvalue = 2.267		Variance Explained = 3.022		

First, we conducted EFA run on all items with the same procedures described before. Results showed that all items loaded high only on the target factor, and no cross loading were found. Only four items from perceived complexity (PC) were found not to satisfy the 0.70 loading requirements. Although confirmatory factor analysis (discussed later in the chapter) showed that maintaining these items was not problematic from a loading perspective, we still chose to stick to the 0.70 loading rule, hoping to concentrate the variance effect of the variable in the structural model. Furthermore, we found that the deletion of these items (PC6, PC7, PC9, and PC12) had no effect on the content validity since the PC construct consisted originally from 12 items, leaving it with 8 highly loading items.

After the deletion of the low loading items, we conducted a second EFA on the remaining items. Results from the final rotated factor pattern matrix indicated that all items loaded high only on their respective latent constructs, and had loading values above 0.70. Therefore, all these reflective scales exhibited sound convergent and discriminant validity at this stage of the analysis.

### **Assessment of Reliability**

Following the EFA analysis, refinement, and deletion of low loaded items, revised items reliability was calculated. The philosophical foundations of reliability according to Straub et al. (2004) submit that the researcher is endeavoring to find contiguous measures of the “true scores” that perfectly describe the phenomenon. An internal consistency measure was used to assess each construct inter-item correlations. Table 5.3 shows the Cronbach’s alpha values for each construct based on the results of the last EFA results. In order for the construct to demonstrate acceptable reliability, Cronbach’s alpha values should be 0.7 or greater (Gefen et al., 2000; Hair et al., 2009). As reported in Table 5.3 the Cronbach’s alpha values for all of the constructs in the research model were greater than 0.89, demonstrating that all constructs had adequate reliability assessment scores.

Table 5.3: Reliability of Construct

Construct	Number of Items	Cronbach’s Alpha
Intention to Comply	7	0.948
Perceived Usefulness of Protection	13	0.962
Perceived Complexity	8	0.958
Self-Efficacy	6	0.939
Controllability	4	0.896
General Information Security Awareness	3	0.908
Technology Awareness	4	0.915
User Awareness of Information Security Policies	9	0.963
User Awareness of SETA Program	9	0.962
User Awareness of Monitoring Practices	7	0.946
Subjective Norm	5	0.936

### **Common Methods Bias**

Common methods variance is one of the most prevalent problems in behavioral research (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003) which happens when most of the variables cross-load across regular phases (Straub et al., 2004), as a result of using a single instrument that is obtained from one source, and not measured in a different context (Straub et al., 2004),



as in the case of TAM ( Gefen et al. (2000) ). Since this study falls under the category of behavioral studies that adopted the TAM, common methods variance could be a problem. Several procedural steps were implemented in the instrument design phase to minimize the potential sources of common methods bias described by Podsakoff et al. (2003). Still these procedures are not enough to completely eliminate the potential of such an effect. Following Podsakoff et al. (2003) recommendations, we conducted Harmon's single factor test to examine the existence of this problem.

According to Podsakoff et al. (2003), Harmon test is the most widely used statistical technique to examine common methods variance. This technique involves subjecting all the study items to a single factor analysis and then analyzing the unrotated factor matrix. Common methods variance is assumed to exist if either (a) a single factor emerged from the factor analysis or (b) one factor accounted for the majority of the variance among variables. Results of this test as demonstrated in table 5.4 shows that multiple factors emerged from the factor analysis (11 factors) and no single factor accounted for the majority of the variance among the factors. These results indicate that common methods variance is not a significant problem in this study.

Table 5 4: Harmon's Single-factor Results

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	16.620	17.367	17.367	14.326	14.995	14.995
2	8.829	11.945	29.313	8.559	12.035	27.030
3	6.722	9.279	38.591	6.425	9.333	36.363
4	4.652	6.658	45.249	4.395	6.763	43.126
5	4.321	6.239	51.489	4.061	6.340	49.467
6	3.521	5.227	56.716	3.257	5.322	54.789
7	3.001	4.568	61.283	2.732	4.658	59.447
8	2.813	4.330	65.614	2.547	4.424	63.870
9	1.739	2.970	68.584	1.505	3.105	66.975
10	1.428	2.577	71.161	1.158	2.666	69.641
11	1.203	2.292	73.453	0.975	2.434	72.075
12	.951	1.973	75.425			
13	.752	1.721	77.146			

## Data Analysis and Results

Following the recommendations of Barclay, Higgins, and Thompson (1995) , the model reliability and validity is assessed to ensure that the construct measures are valid and reliable

before assessing the correlations between the constructs in the structural model. the structural model is assessed. The measurement and the structural models were examined using structural equation modeling.

### **Assessment of Measurement Model**

The component-based partial least squares (PLS) approach, a structural modeling technique, was used to test and evaluate the psychometric properties of the constructs and to test the study hypotheses. Currently, PLS is superior to traditional first generation statistical methods such as regression, LOGIT, ANOVA, and MANOVA as it tests the measurement model (relationships between constructs and measures) and the structural model (theoretical relationships among constructs) simultaneously. Initially, PLS estimates the items loading on constructs and then estimates casual relationships among construct iteratively (Gefen et al., 2000).

PLS is the most widely used statistical package in information system research (Rouse & Corbitt, 2008). PLS, as a component-based approach, is the most used as it allows the analysis of non-normal data, is less sensitive to sample size, is supportive of exploratory research (Gefen et al., 2000), does high quality theory testing, (Rouse & Corbitt, 2008), and processes each indicator separately, allowing each item to differ in the amount of influence on the construct estimate (Chin, Marcolin, & L., 2003). PLSs is the most appropriate for this study because of its focus on prediction of data, and it is best suited for exploratory research and theory building. The Smart-PLS software package (version 2.0.M3) (Ringle, Wende, & Will, 2005) was used to assess the measurement model fit indices and to evaluate the validity and reliability.

In order to assess the measurement quality of the eleven reflective scales, factorial validity (convergent validity and discriminant validity), individual item reliability, and composite reliability were calculated (Barclay et al., 1995; Gefen & Straub, 2005). A confirmatory factor analysis was produced using PLS to assess the quality of the measurement model. All of the items that resulted from the exploratory factor analysis, explained previously, were included in the model. Gefen et al. (2000) stated that PLS and EFA might produce different factor loadings; for example, an item loading of .50 in PLS could be below .40 in EFA. Therefore, we could have claimed higher loading of these items in PLS, but actually they created

different problems, some of which were related to the directions of the correlations, so we chose to eliminate them.

Table 5.5 summarizes the items constituting the research model. The table shows the questionnaire items, as well as weight, factor loading, and t-value of each item. Even though PLS does not require the items to be normally distributed, the distribution of all variables were still analyzed, and it was found that all variables included in the model were normally distributed. The number of factors was set to 11, which are the number of constructs included in the model. All 11 factors accounted for 88.5% of the total variance.

Table 5 5: Measurement Items and Item Loadings

Constructs	Item	Weight	Loading	T-value
Intention to Comply	IC1	0.161	0.890	100.721
	IC2	0.161	0.890	81.519
	IC3	0.162	0.891	99.004
	IC4	0.168	0.880	77.272
	IC5	0.165	0.880	81.326
	IC6	0.161	0.853	60.444
	IC7	0.167	0.830	55.355
Perceived Usefulness of Protection	PUOP1	0.083	0.768	38.277
	PUOP2	0.100	0.850	71.378
	PUOP3	0.094	0.823	53.145
	PUOP4	0.092	0.850	68.214
	PUOP5	0.088	0.846	66.364
	PUOP6	0.095	0.831	48.694
	PUOP7	0.095	0.850	67.495
	PUOP8	0.100	0.838	57.763
	PUOP9	0.089	0.831	57.299
	PUOP10	0.094	0.836	63.735
	PUOP11	0.089	0.827	56.202
	PUOP12	0.094	0.814	46.697
	PUOP13	0.093	0.810	41.500
Perceived Complexity	PC1	0.127	0.937	111.186
	PC2	0.145	0.872	47.703
	PC3	0.165	0.941	169.689
	PC4	0.173	0.938	168.319
	PC5	0.134	0.785	41.033
	PC8	0.103	0.803	34.703
	PC10	0.139	0.950	176.761
Self-Efficacy	SE1	0.186	0.862	69.703
	SE2	0.191	0.887	95.984
	SE3	0.181	0.881	75.753
	SE4	0.193	0.891	98.389
	SE5	0.197	0.872	80.163
	SE6	0.195	0.860	74.461
Controllability	CONT1	0.250	0.895	75.716
	CONT2	0.334	0.886	73.887

Table 5.5 Measurement Items and Item Loadings (Continued)

Constructs	Item	Weight	Loading	T-value
	CONT3	0.281	0.874	63.720
	CONT4	0.282	0.837	50.886
General Information Security Awareness	GISA1	0.348	0.885	71.593
	GISA2	0.371	0.916	91.949
	GISA3	0.369	0.955	205.336
Technology Awareness	TA1	0.275	0.893	82.578
	TA2	0.301	0.902	88.558
	TA3	0.258	0.888	65.075
	TA4	0.286	0.889	77.342
User Awareness of Information Security Policies	ISPA1	0.133	0.874	89.664
	ISPA2	0.121	0.887	105.782
	ISPA3	0.130	0.901	120.514
	ISPA4	0.131	0.906	121.848
	ISPA5	0.124	0.883	85.926
	ISPA6	0.121	0.868	73.585
	ISPA7	0.123	0.869	80.327
	ISPA8	0.122	0.858	75.911
	ISPA9	0.133	0.862	81.183
User Awareness of SETA Program	SETA1	0.133	0.865	79.371
	SETA2	0.126	0.875	87.401
	SETA3	0.130	0.881	93.488
	SETA4	0.120	0.887	94.152
	SETA5	0.133	0.880	91.381
	SETA6	0.138	0.889	96.799
	SETA7	0.116	0.873	78.226
	SETA8	0.115	0.865	74.858
	SETA9	0.130	0.867	83.409
User Awareness of Monitoring Practices	MPA1	0.149	0.863	79.691
	MPA2	0.163	0.864	68.932
	MPA3	0.167	0.853	66.398
	MPA4	0.160	0.876	91.917
	MPA5	0.161	0.878	87.151
	MPA6	0.175	0.875	75.389
	MPA7	0.176	0.876	84.233
Subjective Norm	SN1	0.226	0.893	90.175
	SN2	0.223	0.894	90.098
	SN3	0.221	0.896	95.866
	SN4	0.233	0.900	119.214
	SN5	0.217	0.875	87.589
	IC1	0.161	0.890	100.721

First, to ensure convergent validity and reliability of every item, factor loading of each individual item on its underlying construct was examined, as well as the Average Variance Extracted (AVE). As shown in table 5.5, all item loadings exceeded the recommended minimum value of 0.70, indicating that at least 50 percent of the variance was accounted for by the construct (Chin, 1998; Hair et al., 2009). Results also showed that all items loaded significantly ( $p < 0.000$ ) on their underlying constructs as evident from the t-values, which are

higher than 1.96 for all items. As shown in Table 5.6, the AVE was higher than the minimum recommended value of 0.5 for each construct, indicating that the items satisfied the convergent validity.

To establish the discriminant validity of the constructs in the study model, the square root of the average variance extracted for each construct, with the correlation scores of that construct with other constructs, was compared. For each scale, the square root of the AVE of each construct, reported in the diagonal of the correlation matrix in Table 5.6, was higher than the correlations between that construct and any other construct (inter-correlations). The cross loading matrix from confirmatory factor analysis was also utilized as another requirement to assess discriminant validity of the constructs (see Table C1 in Appendix C). From the cross loading matrix it was found that, as recommended, all measurement items loaded higher than 0.768 on their underlying construct, and loaded very low, less than 0.40, on other constructs (Gefen et al., 2000). As shown in Table 5.6 and Table C1 (Appendix C), all constructs in the model satisfied these criteria for discriminant validity.

Table 5 6: Composite Reliability, AVE, and Latent Variable Correlations

	CR	AVE	MPA	Cont.	GISA	IC	ISPA	PC	PUOP	SE	SETA	SN	TA
MPA	0.956	0.756	<b>0.869</b>										
Cont.	0.928	0.762	0.314	<b>0.873</b>									
GISA	0.942	0.845	0.359	0.266	<b>0.919</b>								
IC	0.958	0.763	0.320	0.221	0.040	<b>0.874</b>							
ISPA	0.968	0.772	0.419	0.381	0.343	0.309	<b>0.879</b>						
PC	0.965	0.777	0.240	-0.154	-0.215	-0.203	-0.099	<b>0.881</b>					
PU	0.966	0.687	0.327	0.221	0.350	0.310	0.311	-0.254	<b>0.829</b>				
SE	0.952	0.766	0.408	0.396	0.253	0.284	0.359	-0.285	0.384	<b>0.875</b>			
SETA	0.967	0.767	0.343	0.329	0.227	0.360	0.359	-0.231	0.326	0.421	<b>0.876</b>		
SN	0.951	0.795	0.311	0.070	0.252	0.368	0.356	-0.251	0.365	0.354	0.315	<b>0.892</b>	
TA	0.940	0.797	0.322	0.243	0.210	0.302	0.447	-0.218	-0.093	0.297	0.319	0.288	<b>0.893</b>

CR = Composite reliability; AVE = Average Variance Extracted; MP = Monitoring Practices; Cont. = Controllability; GISA = General Information Security Awareness; IC = Intention to Comply; ISPA = Information Security Awareness; PC = Perceived Complexity; PU = Perceived Usefulness of Protection; SE = Self-Efficacy to Comply; SETA = Security, Education, Training and Awareness; SN = Subjective Norms; TA = Security Awareness.  
Diagonal elements in bold display the square root of AVE.

To confirm the scale reliability and internal consistency, the composite reliability (CR) and Cronbach's alpha was calculated. A scale is deemed to be reliable if it has CR and Cronbach's alpha above 0.70 (Gefen et al., 2000). Table 5.6 shows that all composite reliability values are more than 0.982, and Cronbach's alpha, as shown in Table 5.3, are higher than 0.896, demonstrating that all constructs had adequate reliability assessment scores and all construct

measures were considered to be reflective as all indicators satisfy the recommended criteria specified by Petter, Straub, and Rai (2007). These items will be used in future studies for testing the proposed theoretical research model.

Consequently, the results of the measurement model demonstrated adequate convergent validity, discriminant validity, and reliability required for further testing of our research hypotheses.

### **Structural Model Testing**

Having established that the model demonstrated adequate factorial validity and reliability, a test of the structural model was conducted. As stated in the research methodology, PLS approach to structural equation modeling was used to estimate the measurement model. The PLS algorithm and the bootstrapping re-sampling method with 878 cases and 1756 re-samples were used to estimate the structural model. Figure 5 shows the results of the model estimation, path coefficients, paths significant level based on a two-tailed t-test, and the variance explained by the independent variables ( $R^2$ ). Together, path coefficients (loadings and significant) and  $R^2$  are indicators of the model performance, with  $R^2$  indicating the predictive power of the model, which is equivalent to the  $R^2$  in a regression model (Gefen et al., 2000). Path coefficients are significant and directionally consistent with the assumptions of the study.

As shown in figure 5, the structural model could explain 17.8 percent of the variance for the intention to comply, where 26.6 percent of the variance could be explained for perceived complexity, and 44.1 percent of the variance for perceived usefulness of protection. In the variance explained by the original TAM constructs (PC and PUOP), and SN, perceived complexity accounts for 12.2 percent of the variance explained in intention to comply, perceived usefulness of protection accounts for 18.7 percent, and subjective norm accounts for 31.6 percent of the variance. All of these figures are greater than the minimum value of a 10 percent criterion that was suggested by Falk and Miller (1992) as an indicator of substantive explanatory power.

Consistent with hypotheses 1 through 4 (H1 – H4), perceived usefulness of protection was found to have a significant impact on intention to comply ( $\beta = 0.188$ ,  $P < 0.001$ ); therefore H1 is supported. Perceived complexity was found to have significant impact on intention to

comply directly ( $\beta = -0.085$ ,  $p < 0.01$ ) and a significant impact on perceived usefulness of protection ( $\beta = -0.197$ ,  $p < 0.001$ ); therefore, both H2a and H2b are supported. Subjective norm was found to have a significant impact on intention to comply ( $\beta = 0.278$ ,  $P < 0.001$ ) and a significant impact on perceived usefulness of protection ( $\beta = 0.201$ ,  $P < 0.001$ ); therefore, H3 and H4 are supported.

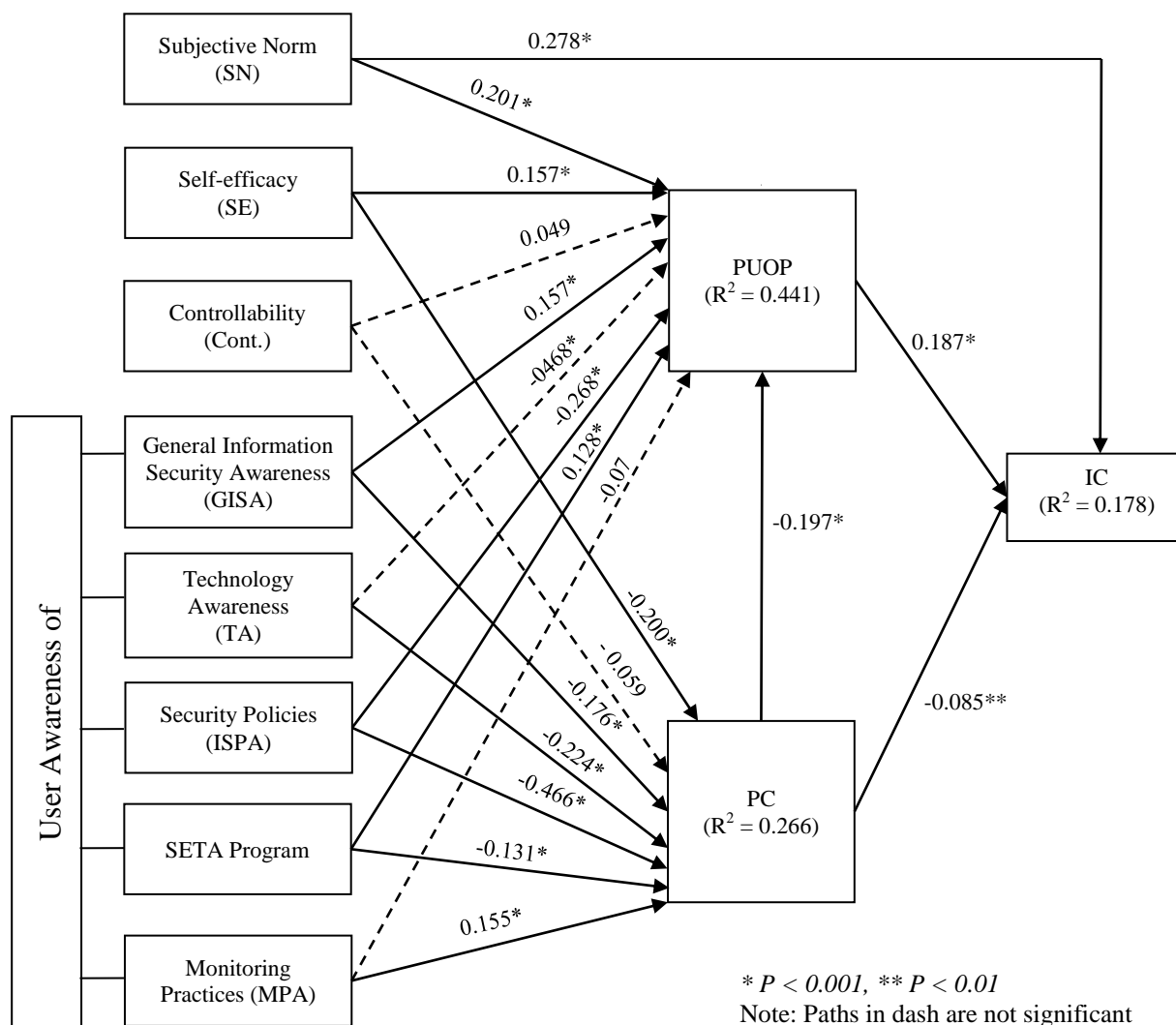


Figure 5: The Results of the Structural Model Testing

Consistent with H5 – H8, self-efficacy has a significant impact on perceived usefulness of protection ( $\beta = 0.57$ ,  $P < 0.001$ ) and on perceived complexity ( $\beta = -0.200$ ,  $P < 0.001$ ); therefore, H5 and H6 are supported. However, controllability was not found to have a significant impact on either perceived usefulness of protection or perceived complexity: therefore, H7 and H8 are not supported. For H9a – H10b, general information security

awareness was found to have a significant effect on perceived usefulness of protection ( $\beta = 0.157, P < 0.001$ ) and on perceived complexity ( $\beta = 0.176, P < 0.001$ ); therefore, H9a and H9b are supported. Regarding technology awareness, it was found to have significant effect on perceived usefulness of protection ( $\beta = -0.468, P < 0.001$ ) and on perceived complexity ( $\beta = -0.224, P < 0.001$ ), however, the direction of the relationship with perceived usefulness was opposite to that hypothesized; therefore, H10a is not supported while H10b is supported.

Consistent with H11 – H16, users' awareness of security policy was found to have a significant impact on perceived usefulness of protection ( $\beta = -0.260, P < 0.001$ ) and on perceived complexity ( $\beta = -0.466, P < 0.001$ ), however, the direction of the relationship with perceived usefulness was opposite to that hypothesized; therefore, H11 is not supported while H12 is supported. SETA program was found to have a significant effect on perceived usefulness of protection and on perceived complexity ( $\beta = 0.128, -0.131, P < 0.001$ , respectively); therefore, H13 and H14 are supported. Monitoring practices was not found to have a significant impact on perceived usefulness of protection ( $\beta = 0.079, P < 0.10$ ), and therefore H15 is not supported. On the other hand, it was found to have a significant impact on perceived complexity ( $\beta = 0.155, P < 0.001$ ), and therefore H16 is supported. Table 5.7 summarizes the results of the hypotheses testing.

Table 5 7: Main Effect Path Coefficient (Structural Model Results)

H#	Hypothesis (Direction)	Path Coefficient	t-value	Significance	Supported?
H1	PUOP → IC (+)	0.187	4.414	P < 0.001	Yes
H2a	PC → IC (-)	-0.085	2.270	P < 0.01	Yes
H2b	PC → PUOP (-)	-0.197	5.487	P < 0.001	Yes
H3	SN → IC (+)	0.278	6.223	P < 0.001	Yes
H4	SN → PUOP (+)	0.201	4.811	P < 0.001	Yes
H5	SE → PUOP (+)	0.157	3.718	P < 0.001	Yes
H6	SE → PC (-)	-0.200	5.145	P < 0.001	Yes
H7	Cont. → PUOP (+)	0.049	1.188	NS	No
H8	Cont. → PC (-)	-0.059	1.670	NS	No
H9a	GISA → PUOP (+)	0.157	3.815	P < 0.001	Yes
H9b	GISA → PC (-)	-0.176	4.751	P < 0.001	Yes
H10a	TA → PUOP (+)	-0.468	14.313	P < 0.001	No
H10b	TA → PC (-)	-0.224	7.007	P < 0.001	Yes
H11	ISPA → PUOP (+)	-0.260	5.561	P < 0.001	No
H12	ISPA → PC (-)	-0.466	13.792	P < 0.001	Yes
H13	SETA → PUOP (+)	0.128	3.158	P < 0.001	Yes
H14	SETA → PC (-)	-0.131	3.848	P < 0.001	Yes
H15	MPA → PUOP (-)	-0.079	1.872	NS	No
H16	MPA → PC (+)	0.155	3.952	P < 0.001	Yes



## **CHAPTER SIX**

### **DISCUSSION AND IMPLICATIONS**

#### **Overview of the Study and Findings**

Compliance with information security policies became a main concern for organizations since ISP violations have significantly increased information security threats and vulnerabilities, and contribute significantly to information security breaches. Employees who are aware of the information security policies of their institutions and deliberately violating the policy, are considered a big problem and a hidden threat, since awareness and training programs will have little impact on their behavior. Information security policy violation varies from behaviors that are unethical (such as inappropriate use of e-mail, and shopping or selling using the company's network), to ones that are criminal or illegal (such as sabotage, data theft, and data destruction), to ones that are unintentional or accidental (forgetting to change a password or the careless discarding of sensitive information rather than shredding it). Such acts are often known as information security non-compliance behavior. This study focused on all types of policy violation by employees or users; intentional or unintentional, inappropriate or illegal, and considers any act of violating the ISPs as a noncompliance problem.

Employees can impose excessive damage to the confidentiality, integrity, or availability of the IS through deliberate activities (espionage), or they may present a potential threat through passive noncompliance with security policies (laziness, poor training, or lack of motivation to adequately ensure information security) (Warkentin & Willison, 2009). In order to foster employees' rule adherence, different approaches have been adopted to investigate and explain employees' rule following behavior (Tyler & Blader, 2005). Some studies adopted the command-and-control approach, which is linked to extrinsic motivational models of human behavior, such as the external contingencies of reward (e.g. Siponen et al., 2010) and

punishment (e.g. D'Arcy et al., 2009; Straub, 1990), and breaking the rules (Hu et al., 2010; Posey et al., 2010). Other studies have employed a self-regulatory approach, which is linked to intrinsic motivational models, emphasizing individuals follow the rules as connatural drivers of behavior. Intrinsic motivational models of human behavior were found to explain employees' rule-following behavior better than extrinsic motivational models which have been built on GDT, RCT, PMT, and other extrinsic behavioral theories (Son, 2011).

From the extensive review of systems abuse literature, it was obvious that the command-and-control model symbolizes a conventional approach to animate rule-following; it is based on the idea that people abide by the rules as a function of the costs and benefits they associate with doing so. This approach is well represented in different theories such as GDT (e.g. D'Arcy & Hovav, 2009; Siponen & Vance, 2010; Straub, 1990), RCT (e.g. Bulgurcu et al., 2010a; Hu et al., 2010; Li, Zhang, et al., 2010), and PMT (e.g. Herath & Rao, 2009b; Johnston & Warkentin, 2010; Siponen et al., 2007). The approach contends that employees are materialistically motivated, and are basically interested in the resources and outcomes they obtain from their organizations. Therefore, in order to enforce policies, rules, and procedures, organizations must take an active role by providing incentives (to encourage desired behavior) and sanctions (to discourage undesirable behavior) (Tyler et al., 2007).

The question to ask at this point is "do such techniques work?" The analysis of the literature and the results of this study indicate that these strategies often help shape employees' behavior. But such strategies also come with significant cost because in order for sanctions and deterrence systems to work, organizations must be able to dedicate substantial resources to the surveillance needed to make the detection of systems misuse or abuse likely enough that people are deterred.

This study focused on the self-regularity approach, which represents an alternate approach to encouraging rule following behavior, since it is concentrated on employees' intrinsic motivations. This method identifies rule following as initiated with an individual's innate desire to follow organizational rules, and not with external contingencies in the environment that are linked to rule following, such as rewards, penalty, fear, outcomes, or social pressure (Tyler & Blader, 2005). Therefore, the technology acceptance model (TAM) was found appropriately fit to investigate employees' innate behavior toward complying with

organizations' ISPs since it concentrates on employees' desire and willingness to follow rules as described in the ISPs, for the sake of protecting the organization information systems, and not to maximize any outcomes for themselves. Utilizing TAM and TBP, this study developed a Security Acceptance Model (SAM), analogous to the TAM, to explain compliance intention behavior among bank employees. The model explained users' compliance behavior with ISPs in terms of perceived complexity of ISPs, perceived usefulness of protection afforded by ISPs, and user awareness of information security issues and countermeasures. It was posited that among different factors, information security awareness likely plays a major role in shaping user compliance behavior with ISPs.

The model was tested in Jordan for several reasons. First, Jordan became a target for hackers due to the absence of governmental legislation and a delayed interest by institutions in security and data protection. As well as the absence of security policies to these banks, beside the novelty of the concept of security awareness among employees and their belief that they are immune from security threats. Second, Jordan is the researcher's home country, giving him access to information there. Third, Jordan is considered one of the largest users of computers in the Middle East after the UAE. Finally, Jordan has a strong banking system that has been using technology for some time.

Data was collected via a self-reported questionnaire from a sample of 878 bank employees. The resulting data was analyzed by two main statistical techniques; exploratory factor analysis and component-based partial least square approach. The validity and reliability tests indicated that the designed model SAM fit the data well. Perceived complexity (PC) and perceived usefulness of protection (PUOP) were significantly related to employees' intention to comply with ISPs. These findings provided strong statistical support that SAM is a useful theoretical framework for predicting users' intention behavior with ISPs. The downstream effect of the SAM is evident not only in the significance of the paths linking perceived complexity and perceived usefulness of protection with compliance behavioral intention, but also in the significant relationships between employees' awareness of security countermeasures (structured and unstructured) with PC and PUOP.

## Discussion of Findings

This study presented a Security Awareness Model (SAM) that underscores the user dimension in addressing ISP compliance issues. This user focus, along with consideration of ISPs as a system, is a novel approach as compared to extant theoretical frameworks such as GDT, PMT, TRA, and TPB, among others. The model tries to explain user compliance behavior with ISPs in terms of perceived complexity of ISPs, perceived usefulness of protection afforded by ISPs, and the user awareness of information security issues and countermeasures. It is posited that among different factors, information security awareness likely plays a major role in shaping user compliance behavior with ISPs. The results of this study supported the validity of the SAM as a useful theoretical framework to predict employees' behavioral compliance intention with ISPs. The model explained about 18 percent of the total variance in the dependent variable, and the casual structural paths of the main predictors (PC and PUOP) were statistically significant ( $\beta = -0.085$ ,  $t = 2.270$ , and  $\beta = 0.187$ ,  $t = 4.414$ , respectively). These results refute the assumptions of some researchers (e.g. Johnston & Warkentin, 2010) that technology adoption theories do not have the ability to explain the acceptance and use of security policies because they do not include the concept of threat as productivity-based applications.

Consistent with the predictions of SAM, perceived complexity (PC) and perceived usefulness of protection (PUOP) both had a significant impact of behavioral intention to comply with ISPs. These results are consistent with TAM literature (e.g. Davis & Venkatesh, 1996; Venkatesh & Bala, 2008; Venkatesh & Davis, 2000). Perceived complexity was found to have a significant negative effect on behavioral intention to comply and on perceived usefulness of protection. The importance of perceived complexity was further explained by its indirect impact on intention to comply through perceived usefulness of protection. This suggests that if employees perceive ISPs to be easy to use and not complex, they will perceive their security compliance behavior to have a favorable impact on their performance to protect an organization's information assets, and they are more likely to use it. Further, compared to productivity-based software tools such as spreadsheets, emails, and word processors, which can improve job performance and productivity, compliance with ISPs to secure the working environment impede performance (Johnston & Warkentin, 2010). These findings are

consistent with the recommendations of Whitman and Mattord (2008) that when designing ISPs, they should be easy to use. Moreover, these results are consistent with a number of studies which used perceived complexity instead of perceived ease of use, and found that perceived complexity negatively affected behavioral intention (Chang & Cheung, 2001; Igbaria et al., 1996; Thompson et al., 1991). In the security domain, these results were different than the results of Dinev and Hu (2007) and Xue et al. (2010), which found that PU and PEOU had no significant impact on behavioral intention.

As compliance with ISPs is mandatory, subjective norm is a significant factor that predicts behavioral intention. Under this assumption, if a superior suggests that a particular system is useful, a person might believe it is actually useful and then form an intention to use it. Venkatesh and Davis (2000) refer to the casual mechanism underlying the impact of subjective norm on behavioral intention as compliance. Consistent with TAM results in mandatory environments (Hartwick & Barki, 1994; Venkatesh & Bala, 2008; Venkatesh & Davis, 2000; Venkatesh et al., 2003), subjective norm was found to have a significant effect on intention to comply with ISP, which is also consistent with the results of studies in the same field of security compliance (e.g. Anderson & Agarwal, 2010; Bulgurcu et al., 2010a; Herath & Rao, 2009a; Siponen et al., 2010; Zhang et al., 2009). Subjective norm accounts for the highest percent (31.6%) of the variance explained in intention to comply. This suggests that employees will form favorable perceptions toward compliance through the social influence of superiors, managers, or colleagues, more than any other reason. The implication of this highest effect on intention to comply could be due to cultural issues since the study sample was from Jordan, where it is very unorthodox and shameful for an employee's peers and superiors to discover that s/he did not comply with ISPs. What confirms this assumption is the effect of subjective norm on PUOP, where it was found to have the highest percent (20%) of the variance explained in PUOP; meaning if peers and superiors perceive it as useful, and then an employee will perceive it to be too.

To overcome situations where behavior is nonvolitional, Ajzen (1991) introduced the concept of perceived behavioral control (PBC) that consists of two components; self-efficacy and controllability. The results of this study found that self-efficacy has a significant effect on PUOP and PC ( $\beta = 0.157$ ,  $p < 0.001$ , and  $\beta = -0.200$ ,  $p < 0.001$ , respectively), while controllability was not significant. Self-efficacy was found to have a positive impact on

PUOP, which is consistent with TAM studies in both voluntarily and mandatory environments (e.g. Ong et al., 2004; Ong & Lai, 2006; Venkatesh et al., 2003), and also with the results of security compliance studies which have investigated its impact on intention to comply (e.g. Boss et al., 2009; Bulgurcu et al., 2010a; Johnston & Warkentin, 2010; Siponen et al., 2010). This result suggests that if employees perceive ISPs as relevant to their work and important for protecting information assets, they will comply with the policies. Inconsistent policies and procedures can lead to frustration, confusion, and potential non-compliance. The results also showed that self-efficacy had a negative significant impact on PC. This result was consistent with TAM studies in both voluntarily and mandatory settings (e.g. Ong et al., 2004; Venkatesh & Bala, 2008; Venkatesh & Davis, 1996; Venkatesh et al., 2003; Wu, Chen, & Lin, 2007), as well as with the results of security compliance studies which investigated its impact on intention to comply (e.g. Bulgurcu et al., 2010a; Johnston & Warkentin, 2010; Liang & Xue, 2010; Ng et al., 2009; Siponen et al., 2010). According to self-efficacy theory, this suggests that in order for employees to comply with ISPs, they must understand these policies. This also confirms the recommendations of different studies on the importance of designing clear and easy to understand policies (Hone & Eloff, 2002; Whitman et al., 2001). As for controllability, the non-significant impact was inconsistent with the previous literature (Dinev & Hu, 2007; Kim et al., 2008), while it was consistent with (Dinev et al., 2009). A plausible explanation is that the adoption and use of the technology and resources to protect information assets to a large extent is mandated by the bank.

In terms of the research model, findings demonstrated that perceived complexity and perceived usefulness of protection are key prevailing variables linking information security awareness to compliance behavior with ISPs.

General information security awareness was found to have a positive significant impact on perceived usefulness of protection ( $\beta = 0.157$ ,  $p < 0.001$ ). The result suggests that an employee's perceived usefulness of the ISP toward compliance can be enhanced by his/her general security awareness. This result was consistent with the findings of Bulgurcu et al. (2010a) and Bulgurcu et al. (2009). The results also showed that general information security awareness has a negative significant impact on perceived complexity ( $\beta = -0.176$ ,  $p < 0.001$ ). This result suggests that higher general security awareness increases employees' confidence in overcoming the complexities and hurdles toward compliance with the requirements of the

ISPs. This result is also very consistent with the findings of Bulgurcu et al. (2010a) that employees' perception that compliance impedes job-related functions can be reduced by information security awareness. As for employees' knowledge and understanding of security related technologies, it was found that it has a negative significant impact on perceived usefulness of protection. The negative direction suggests that employees think they are savvy, encompass enough knowledge, and have enough resources (e.g., magazines, discussion forums, and online help) about security issues which make ISPs obsolete to their work compared to the size of knowledge they possess. This result was inconsistent with the findings of Dinev and Hu (2007) which showed that technology awareness has a positive impact on employees' attitude toward intention to use protective technologies. On the other hand, the negative impact of technology awareness on employees' perceptions of complexity of ISPs was consistent with the theoretical base. The result suggests that an employee's perception of the complexity of the ISP toward compliance can be enhanced by the knowledge s/he generates about security issues from different resources, such as magazines, online help, and discussion forums. This result is consistent with previous studies that investigated the effect of ISA on intention to comply (Bulgurcu et al., 2009, 2010a; Dinev & Hu, 2007).

Users' awareness of information security policies had a negative impact on their perception of the usefulness of ISPs in protecting information resources. This suggests that information security policies at these banks are not defined clearly and lack the processes that will help to ensure system security. This is confirmed by Whitman et al. (2001, p. 13) where he stated that "if security procedures unnecessarily inhibit employees' use of the information system, they will be less productive or will bypass the procedure". Moreover, Straub (1990) emphasized the necessity to develop detailed policies defining proper and improper use of information systems. This result was not consistent with the prior research that found clearly defined security policies will reduce the behavioral intention of system misuse (D'Arcy, 2005; D'Arcy & Hovav, 2007, 2009; D'Arcy et al., 2009). Another suggestion for the negative effect that comes with (Finch, Furnell, and Dowland (2003) line of thinking, is that employees might not be fully aware of the existence of security policy within their banks. On the contrary, users' awareness of information security policies had a negative impact on their perception of the complexity of complying with ISPs. This suggests that high awareness of information security

policies will reduce employees' complexity perception in complying with ISPs. This result is consistent with (Lee et al., 2004) and with the results of studies adopted from GDT (D'Arcy, 2005; D'Arcy et al., 2009; Lee et al., 2004) which found that awareness of information security policies enhances users' perception and understanding of punishment for systems misuse, which will decrease misuse behavioral intention. In general, these two results suggest that when designing ISPs, banks should emphasize the ease of understanding the policy more than its usefulness in protecting the bank's information systems and resources.

Users' awareness of SETA programs had a significant positive impact on perceived usefulness of protection, while it was found to have significant negative impact on perceived complexity. This suggests that proper cognitive education, and awareness and training for employees on security issues, such as threats, technologies, and compliance, are effective in enhancing their perceptions of the usefulness of ISPs for protecting information and technology resources, which eventually will increase compliance behavioral intention with the rules and requirements of the ISPs. These programs will also decrease employees' perceptions about the complexity of compliance with the ISPs. Previous literature emphasized the importance and benefits of SETA programs in altering users' behavior in a positive direction (e.g. Puhakainen & Siponen, 2010; Schultz, 2004; Straub & Welke, 1998; von Solms & von Solms, 2005), but little empirical work has been put into practice (D'Arcy et al., 2009; Kankanhalli et al., 2003; Posey et al., 2010; Straub, 1990). This study provides empirical evidence that SETA programs are effective mechanisms for enlightening employees about the importance of complying with ISPs by improving their perceptions about the usefulness of ISPs in protecting information and technological resources, and by reducing perceived complexity of compliance. Puhakainen and Siponen (2010) emphasized the quality of training programs by utilizing methods and learning tasks that stimulate learners to complete organized cognitive processing of information.

Users' awareness of monitoring practices had an insignificant negative impact on perceived usefulness of protection, while it had a positive significant impact on perceived complexity. This suggests making employees aware that they are electronically monitored increases their perceived complexity in compliance with ISPs, and although not significant, decreases their satisfaction with usefulness of protection. These results are consistent with Urbaczewski and Jessup (2002) findings that reported when employees were aware of electronic monitoring



“policing”, their focus was more on task and they were less satisfied. These findings are applicable to this study, because when employees are aware of monitoring “policing” practices, they concentrate literally on compliance more than on work, and that impacts their perception about the usefulness of compliance negatively, since they see it as an impediment of their performance, making it more complex to comply since they will be very cautious not to make mistakes. This result was also consistent with prior research which found monitoring to lower employee satisfaction and increase turnover in some cases (Alder et al., 2008; Chalykoff & Kochan, 1989; George, 1996). However, it is still important to note that monitoring can play a key role in protecting an organization from employee abuse (e.g. Ariss, 2002; D'Arcy et al., 2009; Kankanhalli et al., 2003; Straub, 1990; Straub & Welke, 1998).

In conclusion, the results of this study suggest that each of the information security awareness countermeasures plays an important role in enhancing users' perception about the usefulness of protecting information and technology resources and lowering the degree of complexity of compliance, which in turn increases intention to comply with ISPs. Awareness of information security policy seems to have the highest impact on intention to comply, followed by technology awareness, with monitoring practices having the least impact.

### **Theoretical Contribution**

Different behavioral theories have been adopted in the information security domain to investigate either compliance intention or to deter misuse behavior, and others have been adopted to deploy preventive and protective technologies. Theories such as TRA, TPB, RCT, PMT, GDT, SCT, RCT, TAM, and others were adopted as the theoretical foundation for their studies, since each of them has the potential to predict behavioral intention. Much of the previous literature concentrated on the deterrent effect of sanctions or incentives to encourage employees' desirable behavior, but none of the studies addressed this problem as a system that employees must accept first. Accordingly, this study is the first to develop a model, the Security Acceptance Model (SAM), to investigate the users' perceptions about complying with ISPs, motivated only by intrinsic desire, and a willingness to follow rules as described in the ISPs for the sake of protecting the organization's information systems, and not to maximize any outcomes for themselves.

Another important contribution this study makes to the behavioral aspects of the information security body of knowledge is being the first study to present empirical support that technology adoption theories have the ability to explain the acceptance and use of security policies as they were found to include the concept of threat as productivity-based applications. This study demonstrated that employees' intrinsic desire and willingness to follow rules as described in the ISPs can be traced back to normative beliefs, and perceived behavioral control.

Third, the field of security awareness is lacking research which views this concept from a behavioral perspective and that employs behavioral theories, such as TRA, TPB, TAM, and others, to help understand its effect on shaping compliance intention or deterring misuse intention. Thus, this study is the first to assess the impact of structured and unstructured information security awareness on compliance intention. The findings showed that information security awareness (ISA) exerts a significant impact on users' perceived usefulness of protection and perceived complexity, which shapes users' intentional behavior to comply with ISPs. Accordingly, this study will contribute to the library of security awareness research.

Finally, this study is the first to investigate the complexity of complying with ISPs. Most of the previous studies adopted TAM, and investigated the role of PEOU, which has not been found to be an appropriate or significant predictor of intention to comply. Due to the nature of ISPs which involve compliance rather than using, and are mostly described as difficult, it is more appropriate to utilize this factor than the PEOU.

### **Practical Contribution**

The results of this study will help senior management to understand the factors that encourage behavior toward the adoption of security countermeasures, which will help to elicit positive behaviors from employees, leading to a decrease in human errors and reducing the cost of security. The subjective norm had the highest impact on employees' intention to comply with ISPs. This means that employees' intention to comply with the ISPs is greatly affected by opinions and by significant others. Thus, when developing security awareness programs, management and practitioners need to be aware that perceived social pressure is an important factor that helps enhance compliance with ISPs by concentrating on social and organizational

matters. Puhakainen (2006) proposed a framework for analyzing employees' motivation to comply with ISPs and noted that the subjective norm is one of the main factors that helps us to understand the reasons for compliance and non-compliance with the instructions. Most of the literature on ISP compliance or misuse investigated the impact of subjective norm (e.g. Anderson & Agarwal, 2010; Dinev & Hu, 2007; Siponen et al., 2010; Zhang et al., 2009), and showed the importance of significant others and opinions in the compliance process. Accordingly, management should take compliance with ISPs seriously and emphasize to employees firmly that they should comply. Management can do that through day-to-day activities such as brochures, emails, and posters, or by other means, such as training or during meetings.

The results of this study provide significant evidence that users' awareness of the existence of security policies, SETA programs, and monitoring practices are each a significant factor in improving users' intention to comply with the ISPs. Therefore, each of these countermeasures should be an essential component of a bank's security management program. Some previous studies found that managers did not believe that the role of these countermeasures is significant in changing users' behavior toward compliance or in deterring systems misuse (Hoffer & Straub, 1989; Straub & Welke, 1998). The results of this study prove otherwise, and suggest that organizations can help improve compliance behavior by (1) developing comprehensive detailed policies that define appropriate and inappropriate use of the resources; (2) conducting special educational, training, and awareness programs that instruct employees in different security issues, such as why security policies are important, security technology, security threats and controls, cost of compliance and non-compliance, legitimate and illegitimate use of IS resources, consequences of non-compliance, and how to enforce information security policies; and (3) building an effective monitoring program designed to control and provide feedback at the same time, and conducting periodical audits on all employee activities.

In designing security policies, management should develop clear, concise, detailed, direct, and easy to understand security procedures that do not obstruct employees' use of the information system. The policy should be available for all employees on paper or electronically. Acceptable and unacceptable, and legal and illegal use of information resources must be clearly defined in the policy and instructed to all users. Management should also try to make

use of international security standards as guidelines when developing ISPs, and periodically assess security policies, procedures, and guidelines.

In designing SETA programs, a training program targeting top management about the necessity of security awareness programs must be developed and presented first. Then a security awareness committee can be established that will be responsible for reviewing and recommending training needs and tools. Next, evaluations regarding employees' training and awareness needs must be conducted, and based on this assessment, development of educational and awareness programs. Overall, SETA programs must be designed based on the roles and responsibilities defined in an employee's job description since some educational programs are not suitable for certain jobs and some users may have more knowledge on certain issues than the designed program itself. Ethical ideology is an important factor in security, and especially in compliance with ISPs; therefore, a special ethical program should be delivered to all employees aimed at influencing their morals toward compliance with ISPs.

Monitoring employees' practices to ensure compliance with rules and requirements as described in the ISPs is important. Studies found that users believe that monitoring their practices is a kind of violation of their privacy, and it can lower their job satisfaction, and in some cases, increase the turnover rate (e.g. Alder et al., 2008; Chalykoff & Kochan, 1989; Urbaczewski & Jessup, 2002). Therefore, when designing monitoring systems it is important to educate all employees about the program, and explain to them its purpose, which must be control and providing feedback. Policing the users' activities must be removed from their minds through training and awareness programs, and by empirically providing them with feedback when necessary, such as when violation is unintentional. Interestingly, monitoring practices were found to have no significant impact on perceived usefulness of protection. This has a practical implication; a training program about the importance and usefulness of monitoring in protecting information resources and its role in confirming compliance with ISPs could be given to all employees.

As the results show, employees' personal education and knowledge about security issues (unstructured awareness) was found to have a significant effect on compliance behavior. Therefore, management must provide employees with training sessions about the different resources and their reliabilities for solving security issues. Further, management can leverage

this by having a special room with PCs to be used for self-education purposes, which define and specify certain websites and forums for employees to help them solve specific security issues.

Perceived behavioral control was partially (self-efficacy) found to have a significant impact on intention to comply with ISPs. This suggests that employees perceive that they are capable of complying with the rules and requirements of ISPs . Therefore, management should enhance and strengthen this perception by giving limited controlled privilege for employees that will increase their confidence in their abilities to handle security issues and to comply with ISPs.

## **Limitations**

As with any other study, this study had some limitations. The first limitation is related to the self-reported measure and cross-sectional design. A common method bias and social desirability bias were important problems to this study. In the common method bias, several procedures were adopted to contain and minimize its effect, and these procedures were effective in showing that this bias was not a threat for this study. With the social desirability bias threat, anonymity of respondents was confirmed to respondents, there were not any signs or indicators of who the respondents were, and a pilot study was conducted to ensure no significant differences between the respondents.

A second limitation is also related to the measurement tool (the questionnaire). This tool was developed in English and distributed in an Arabic speaking country. Some interpretation and translation problems occurred with some respondents, who had some difficulty understanding some questions. The researcher considered translating the questionnaire into Arabic, but by doing so, many of the questions would lose their intended meanings. To overcome these limitations, a question was added about the number of years the respondent had been speaking English. Those who spoke no English at all were excluded from the sample, and those whose English was not proficient enough to answer the questionnaire, did not participate in the survey.

The third limitation is also related to the measurement tool. Items and factors were validated and tested in the United States and other countries, but to the best of the researcher's knowledge, they had never been tested in an Arabic speaking country. Thus a pilot study was

conducted to validate the instrument before collecting the final study sample. Results of the pilot study showed valid and reliable results of the instrument.

The fourth limitation is related to the administration of the data collection. A friend of the researcher administered the distribution of the questionnaire, working with a designated contact person from each bank. To make sure that the sample collected was representative, the researcher informed the friend and the designated contact people about the purpose of the study, explained the questionnaire, and gave instructions for survey distribution and sample representation. Regarding the sample representation, these individuals were specifically instructed on the concept of random sampling and asked to randomly select a sample which took into consideration demographic variables to ensure a representative sample. Related to the data collection limitations, a paper-based survey was used since it was impossible to conduct an electronic survey for the various reasons explained in Chapter Four. This created a problem of cost and time. To make sure that data was collected in a short timeframe, the researcher and data collection administrator kept following up with the designated contact person at each bank and collected completed questionnaires on weekly basis. In the data entry process, initially professional people were used to enter the data; however, later the researcher entered the data to ensure data accuracy and integrity. Future Research

The aforementioned limitations can establish a base for future studies. First, to lower the threat of social desirability biases, Siponen and Vance (2010) proposed using scenarios with a full description of a hypothetical situation, and indirectly asking the study participants about their perception of the situation. Scenarios also help capture detailed explanations about specific policies, rules, and guidelines. Therefore, we recommend future research develop hypothetical scenarios to measure users' perceptions about the usefulness and complexity of compliance with ISPs.

This study focused on the self-regularity approach, concentrating on employees' intrinsic motivations, and as Myyry et al. (2009) argued, moral and ethical values play an important role in shaping users' compliance behavior. Knowing that ethical ideology in the security domain is rarely investigated, this stream of research will be very fruitful and promising.

This study was the first to investigate users' perceptions of the complexity of compliance with ISPs. No study was found to investigate the impact of compliance complexity except maybe

Bulgurcu et al. (2008) who investigated the perceived burden of compliance as time consuming and hindering work progress and personal productivity. This factor is totally disregarded in spite of its importance, and therefore, there is an urgent need for studies in this fruitful and important research stream.

An in-depth investigation of subjective norm and perceived behavioral control is recommended, since they show significant impact on compliance behavior. These factors should be investigated in the context of ethical ideology and perceived complexity respectively, as the theoretical base of these factors shows that they are correlated to the proposed research domain.

Finally, this study focused on information security awareness (ISA) as a container or motivator for the compliance behavioral intention, but future research might investigate the impact of other factors such as rewards, cost of compliance and non-compliance, or deterrence, on employees' perceptions of complexity and usefulness of protection toward compliance.

## **Conclusion**

This study presented a Security Awareness Model (SAM) that underscores the user dimension in addressing ISP compliance issues. This user focus, along with consideration of ISPs as a system, is a novel approach as compared to extant theoretical frameworks such as GDT, PMT, TRA, and TPB, among others. The model explained user compliance behavior with ISPs in terms of perceived complexity of ISPs, perceived usefulness of protection afforded by ISPs, and user awareness of information security issues and countermeasures. It is posited that among different factors, information security awareness likely plays a major role in shaping user compliance behavior with ISPs. The findings were consistent with previous studies which utilized TAM and TBP to explain information security policy compliance behavior or to deter system misuse. Results of this study revealed astonishing findings regarding subjective norm which was found to account for the highest percentage (31.6%) of the variance explained in intention to comply.

Of the security countermeasures, the results also show that information security policies had the highest path coefficient impact, which suggests that developing clear and comprehensive information security policies is the most effective and important factor in changing users'

behavior toward compliance with ISPs. Unstructured information security awareness (general information security awareness and technology awareness) was also found to be an essential factor in shaping behavioral intention to comply. This suggests that organizations should motivate their employees to educate themselves with different security issues.

Overall this study presents a significant contribution by explaining the impact and relationships between information security awareness and intention to comply with ISPs. Most importantly, the study confirms the applicability of technology adoption theories in the security compliance domain, and highlights the concept of perceived complexity as a better predictor of compliance behavior than perceived ease of use.



## References

- Adams, D. A., Nelson, R. R., & Todd, P. A. (1992). Perceived usefulness, ease of use, and usage of information technology: a replication. *MIS Quarterly*, *16*(2), 227-247.
- Agarwal, R., & Prasad, J. (1997). The role of innovation characteristics and perceived voluntariness in the acceptance of information technologies. *Decision Sciences*, *28*(3), 557-582.
- Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). Research Report: The Evolving Relationship Between General and Specific Computer Self-Efficacy--An Empirical Assessment. *Information Systems Research*, *11*(4), 418-430.
- Agnew, R. (1985). Social control theory and delinquency: A longitudinal test. *Criminology*, *23*(1), 47-61.
- Agnew, R. (1991). A longitudinal test of social control theory and delinquency. *Journal of Research in Crime and Delinquency*, *28*(2), 126-156.
- Agnew, R. (1993). Why do they do it? An examination of the intervening mechanisms between "social control" variables and delinquency. *Journal of Research in Crime and Delinquency*, *30*(3), 245-266.
- Ajzen, I. (1988). *Attitudes, Personality, and Behavior*. Chicago, IL: The Dorsey Press.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.
- Ajzen, I. (2002a). Constructing a TpB questionnaire: Conceptual and methodological considerations. Retrieved 4/20/2011 from: <http://www.iwar.org.uk/comsec/resources/satools/Motivation-for-Information-Security.pdf>
- Ajzen, I. (2002b). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1. *Journal of Applied Social Psychology*, *32*(4), 665-683. doi: 10.1111/j.1559-1816.2002.tb00236.x
- Ajzen, I. (2005). *Attitudes, personality, and behavior*: Maidenhead, Berkshire, England; New York: Open University Press.
- Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). *Security Policy Compliance: User Acceptance Perspective*. Paper presented at the 2012 45th Hawaii International Conference on System Sciences, Maui, Hawaii.
- Alavi, M., & Weiss, I. R. (1985). Managing the Risks Associated with End-User Computing. *Journal of Management Information Systems*, *2*(3), 5-20.

- Alder, G., Schminke, M., Noel, T., & Kuenzi, M. (2008). Employee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation. *Journal of Business Ethics*, 80(3), 481-498.
- Allen, B. (1968). Danger ahead! Safeguard your computer. *Harvard Business Review*, 46(6), 97-101.
- Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing Special Issue Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, 34(3), 613-643.
- Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, 22(4), 308-313.
- Ariss, S. S. (2002). Computer monitoring: benefits and pitfalls facing management. *Information & Management*, 39(7), 553-558.
- Armitage, C. J., & Conner, M. (2001). Efficacy of the Theory of Planned Behaviour: A meta analytic review. *British Journal of Social Psychology*, 40(4), 471-499.
- Aytes, K., & Conolly, T. (2003). *A research model for investigating human behavior related to computer security*. Paper presented at the AMCIS 2003 Proceedings. Paper 260.
- Ball, L., & Harris, R. (1982). SMIS Members: A Membership Analysis. *MIS Quarterly*, 6(1), 19-38.
- 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), 285-309.
- Benson, D. H. (1983). A Field Study of End User Computing: Findings and Issues. *Mis Quarterly*, 7(4), 35-45.
- Bentler, P. M., & Chou, C. P. (1987). Practical issues in structural modeling. *Sociological Methods & Research*, 16(1), 78-117.
- Bernard, R. (2007). Information Lifecycle Security Risk Assessment: A tool for closing security gaps. *Computers & Security*, 26(1), 26-30.
- Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, 23(3), 253-264.
- Beznosov, K., & Beznosova, O. (2007). On the imbalance of the security problem space and its expected consequences. *Information Management & Computer Security*, 15(5), 420-431.

- Bhattacharjee, A., & Premkumar, G. (2004). Understanding Changes in Belief and Attitude Toward Information Technology Usage: A Theoretical Model and Longitudinal Test. *MIS Quarterly*, 28(2), 229-254.
- Biddle, B. J., & Marlin, M. M. (1987). Causality, Confirmation, Credulity, and Structural Equation Modeling. *Child Development*, 58(1), 4-17.
- Blair, M. M., & Stout, L. A. (2001). Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law. *University of Pennsylvania Law Review*, 149(6), 1735-1810.
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151-164.
- Boudreau, M. C., Gefen, D., & Straub, D. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 25(1), 1-16.
- Brancheau, J. C., & Wetherbe, J. C. (1987). Key Issues in Information Systems Management. *MIS Quarterly*, 11(1), 23-45.
- Bray, T. J. (2002). Security actions during reduction in workforce efforts: What to do when downsizing. [Article]. *Information Systems Management*, 19(3), 85.
- Bresz, F. (2004). People—Often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, 6(4), 57-60.
- Brown, S. A., Massey, A. P., Montoya-Weiss, M. M., & Burkman, J. R. (2002). Do I really have to? User acceptance of mandated technology. *European Journal of Information Systems*, 11(4), 283-295.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2008). *Analysis of Perceived Burden of Compliance : The Role of Fairness , Awareness , and Conditions*. Paper presented at the Association of Information Systems SIGSEC Workshop on Information Security & Privacy (WISP 2008). Paris, France.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). *Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance*. Paper presented at the AMCIS 2009 Proceedings. Paper 419.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010a). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010b). *Quality and Fairness of an Information Security Policy As Antecedents of Employees' Security Engagement in the Workplace: An Empirical Investigation*. Paper presented at the HICSS 43, Koloa, Kauai, Hawaii.

- Campbell, D. T., & Stanley, J. C. (1963). *Experimental and Quasi-Experimental Designs for Research*. Chicago: Rand McNally. In D. R. Cooper & P.S. Schindler, (2006), *Business Research Methods*, 9th Ed., McGraw-Hill/Irwin.
- CAPEC. (2011). The Common Attack Pattern Enumeration and Classification Retrieved Feb. 9, 2011, from [www.capec.mitre.org](http://www.capec.mitre.org)
- Chalykoff, J., & Kochan, T. A. (1989). Computer-Aided Monitoring: Its Influence on Employee Job Satisfaction and Turnover. *Personnel Psychology*, 42(4), 807-834.
- Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy & Security*, 1(3), 18-41.
- Chang, M. K., & Cheung, W. (2001). Determinants of the Intention to Use Internet/WWW at Work: a Confirmatory Study. *Information & Management*, 39(1), 1-14.
- Chau, P. Y. K. (2001). Influence of computer attitude and self-efficacy on IT usage behavior. *Journal Of End User Computing*, 13(1), 26-33.
- Chen, C. C., Shaw, R., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: a case study of an information security awareness system. *Information Technology, Learning, and Performance Journal*, 24(1), 1-15.
- Chenoweth, T., Minch, R., & Gattiker, T. (2009). *Application of Protection Motivation Theory to Adoption of Protective Technologies*. Paper presented at the Proceedings of the 42nd Hawaii International Conference on System Sciences.
- Chin, W., Marcolin, B., & L., N., P., R. (2003). A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Information Systems Research*, 14(2), 189-229.
- Chin, W. W. (1998). Issues and Opinion on Structural Equation Modeling. [Editorial]. *MIS Quarterly*, 22(1), vii - xvi.
- Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security*, 16(5), 484-501.
- Cohen, E., & Cornwell, L. (1989). A question of ethics: Developing information system ethics. *Journal of Business Ethics*, 8(6), 431-437.
- Colwill, C. (2009). Human factors in information security: The insider threat-Who can you trust these days? *Information Security Technical Report*, 14(4), 186-196.
- D'Arcy, J. (2005). *Security countermeasures and their impact on information systems misuse: A deterrence perspective*. (Ph.D. Dissertation), Temple University, United States --

Pennsylvania. Retrieved from Dissertations & Theses: Full Text.(Publication No. AAT 3203001)

- D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM*, 50(10), 113-117.
- D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, 89(S1), 59-71.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1), 79-98.
- Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: theory and results*. Massachusetts Institute of Technology, Cambridge, MA. (Ph.D. Dissertation)
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Mis Quarterly*, 13(3), 319-340.
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science*, 35(8), 982-1003.
- Davis, F. D., & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal of Human-Computer Studies*, 45(1), 19-45.
- Dhillon, G. (1997). *Managing information system security*: Macmillan Press, Hampshire.
- Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, 7(4), 171-175.
- Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, 43(7), 125-128.
- Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio organizational perspectives. *Information Systems Journal*, 11(2), 127-153.
- Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, 19(4), 391-412.
- Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), 23.

- Dugo, T. M. (2007). *The insider threat to organizational information security: A structural model and empirical test*. (Ph.D), Auburn University, Auburn, Alabama. (Dissertation)
- Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, 45(1), 67-87.
- Ernst, & Young. (2010). Borderless Security - 2010 Global Information Security Survey, from [http://www.ey.com/Publication/vwLUAssets/Global\\_information\\_security\\_survey\\_2010\\_advisory/\\$FILE/GISS%20report\\_final.pdf](http://www.ey.com/Publication/vwLUAssets/Global_information_security_survey_2010_advisory/$FILE/GISS%20report_final.pdf)
- Everitt, B. (1975). Multivariate analysis: The need for data, and other problems. *The British Journal of Psychiatry*, 126(3), 237-240.
- Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling*. Akron, Ohio: University of Akron Press.
- Finch, J., Furnell, S., & Dowland, P. (2003). *Assessing IT security culture: system administrator and end-user perspectives*. Paper presented at the Proceedings of the ISOneWorld Conference 2003, April 23-25, Las Vegas, NV.
- Fishbein, M. (2008). A reasoned action approach to health promotion. *Medical Decision Making*, 28(6), 834.
- Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*: MA: Addison-Wesley.
- Fitzgerald, T. (2007). Building Management Commitment through Security Councils, or Security Council Critical Success Factors. In H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook* (Sixth ed., pp. 105-121). Boca Raton, New York: Auerbach Publications.
- Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18(1), 39-50.
- Forsyth, D. (1980). A taxonomy of ethical ideologies. *Journal of Personality and Social Psychology*, 39(1), 175-184.
- Furnell, S., Gennatou, M., & Dowland, P. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, 15(5/6), 352-357.
- Gefen, D., & Straub, D. (2000). The relative importance of perceived ease of use in IS adoption: A study of e-commerce adoption. *Journal of the Association for Information Systems*, 1(1), 8.

- 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*(1), 5.
- Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(1), 7.
- George, J. F. (1996). Computer-Based Monitoring: Common Perceptions and Empirical Results. *MIS Quarterly, 20*(4), 459-480.
- Goodhue, D. L., & Straub, D. (1991). Security concerns of system users : A study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27.
- Gorsuch, R. L. (1983). *Factor analysis* (Second ed.). Hillsdale, NJ: Erlbaum: Psychology Press.
- Greene, G., & D'Arcy, J. (2010). *Assessing the Impact of Security Culture and the Employee-Organization Relationship in IS Security Compliance*. Paper presented at the Proceedings of the 5th Annual Symposium on Information Assurance, New York, USA.
- Gupta, A., & Zhdanov, D. (2006). *Trust and Fairness as Incentives for Compliance with Information Security Policies*. Paper presented at the Proceedings of the 16th Workshop on Information Technologies and Systems,.
- Hackathorn, R. D. (1987). End-user computing by top executives. *ACM SIGMIS Database, 19*(1), 1-9.
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2009). *Multivariate Data Analysis* (Seventh Edition ed.). Upper Saddle River, NJ: Pearson Prentic Hall.
- Hansche, S. (2001). Designing a security awareness program: Part 1. *Information Security Journal: A Global Perspective, 9*(6), 1-9.
- Hansche, S., Berti, J., & Hare, C. (2004). *Official (ISC) 2 Guide to the CISSP Exam*. Boca aton, Florida: Auerbach Publication.
- Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security, 24*(1), 31-43.
- Harrington, S. J. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly, 20*(3), 257-278.
- Hartwick, J., & Barki, H. (1994). Explaining the role of user participation in information system use. *Management science, 40*(4), 440-465.

- Hawkins, S., Yen, D. C., & Chou, D. C. (2000). Awareness and challenges of Internet security. *Information Management & Computer Security*, 8(3), 131-143.
- Heck, R. H. (1998). Factor Analysis: Exploratory and Confirmatory Approaches. In G. A. Marcoulides (Ed.), *Modern Methods for Business Research* (pp. 177-216). Mahwah, New Jersey: Lawrence Erlbaum Associates.
- Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.
- Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18, 106-125.
- Hill, B., & Pemberton, J. M. (1995). Information security: an overview and resource guide for information managers. *Records Management Quarterly*, 29(1), 14-25.
- Hoffer, J. A., & Straub, D. (1989). The 9 to 5 underground: are you policing computer crimes? *Sloan Management Review*, 30(4), 35-43.
- Hone, K., & Eloff, J. (2002). What makes an effective information security policy? *Network Security*, 2002(6), 14-16.
- Hovav, A., & D'Arcy, J. (2003). The Impact of Denial of Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, 6(2), 97-121.
- Hu, Q., & Dinev, T. (2005). Is spyware an internet nuisance or public menace? *Communications of the ACM*, 48(8), 61-66.
- Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2010). *Why Individuals Commit Computer Offences in Organizations: Investigating the Roles of Rational Choice, Self-Control, and Deterrence*. Paper presented at the Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Paper 132.
- Hubona, G. S., & Cheney, P. H. (1994). *System effectiveness of knowledge-based technology: the relationship of user performance and attitudinal measures*. Paper presented at the Proceedings of the Twenty-Seventh Hawaii International Conference on System Sciences, Wailea, HI.
- Hurd, B. E. (2001). *The digital economy and the evolution of information assurance*. Paper presented at the Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY.
- Igbaria, M., Parasuraman, S., & Baroudi, J. J. (1996). A Motivational Model of Microcomputer Usage. *Journal of Management Information Systems*, 13(1), 127-143.



- Im, G. P., & Baskerville, R. L. (2005). A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error. *The DATA BASE for Advances in Information Systems*, 36(4), 68-79.
- ISO/IEC17799. (2005). Information Technology – Security Techniques – Code of Practice for Information Security Management: ISO.
- Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *Management Information Systems Quarterly*, 34(3), 549-566.
- Jones, C. (2009). *Utilizing the technology acceptance model to assess employee adoption of information systems security measures*. (D.B.A. dissertation), Nova Southeastern University, United States -- Florida. Retrieved from Dissertations & Theses: Full Text.(Publication No. AAT 3372768)
- Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139-154.
- Karahanna, E., Straub, D., & Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *Mis Quarterly*, 23(2), 183-213.
- Karjalainen, M., & Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems*, 12(8), 518-555.
- Kerlinger, F. N. (1973). *Foundations of behavioral research: 2nd ed.* New York: Holt Rinehart et Winston.
- Kim, G. S., Park, S. B., & Oh, J. (2008). An examination of factors influencing consumer adoption of short message service (SMS). *Psychology and Marketing*, 25(8), 769-786.
- Kline, T. J. B., Sulsky, L. M., & Rever-Moriyama, S. D. (2000). Common Method Variance and Specification Errors: A Practical Approach to Detection. [Article]. *Journal of Psychology*, 134(4), 401-421.
- Kolkowska, E., Hedström, K., & Karlsson, F. (2009). *Information Security Goals in a Swedish Hospital*. Paper presented at the Proceedings of the 8th Annual Security Conference Discourses in Security Assurance & Privacy, Las Vegas, NV, USA.
- Koufaris, M. (2003). Applying the technology acceptance model and flow theory to online consumer behavior. *Information Systems Research*, 13(2), 205-223.
- Kraemer, S., & Carayon, P. (2005). *Computer and Information Security Culture: Findings from Two Studies*. Paper presented at the Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting.

- Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7), 509-520.
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289-296.
- Kwok, L.-f., & Longley, D. (1999). Information Security Management and Modelling. *Information Management & Computer Security*, 7(1), 30-39.
- Lai, J. Y. (2009). How reward, computer self-efficacy, and perceived power security affect knowledge management systems success: An empirical investigation in high - tech companies. *Journal of the American Society for Information Science and Technology*, 60(2), 332-347.
- Layton, T. P. (2005). *Information security awareness: the psychology behind the technology*. Bloomington, Indiana: AuthorHouse.
- Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6), 707-718.
- Lee, Y., Kozar, K. A., & Larsen, K. R. T. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems*, 12(1), 50.
- Leitheiser, R. L., & Wetherbe, J. C. (1986). Service Support Levels: An Organized Approach to End-User Computing. *MIS Quarterly*, 10(4), 337-349.
- Li, H., Sarathy, R., & Zhang, J. (2010). *Understanding Compliance with Internet Use Policy: An Integrative Model Based on Command-and-Control and Self-Regulatory Approaches*. Paper presented at the ICIS 2010 Proceedings. Paper 181.
- Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4), 635-645.
- Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), 71-90.
- Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.
- Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, 16(2), 173-186.

- Luftman, J., & Ben-Zvi, T. (2010). Key Issues for IT executives 2009: Difficult economy's Impact on IT. *MIS Quarterly Executive*, 9(1), 49-59.
- Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin*, 18(1), 3.
- Mahmood, M. A., Burn, J. M., Gemoets, L. A., & Jacquez, C. (2000). Variables affecting information technology end-user satisfaction: a meta-analysis of the empirical literature. *International Journal of Human-Computer Studies*, 52(4), 751-771. doi: 10.1006/ijhc.1999.0353
- Markus, M. L. (2000). Toward an Integrated Theory of IT-Related Risk Control. In R. Baskerville, J. Stage & J. I. DeGrossTake (Eds.), *Organizational and social perspectives on information technology* (pp. 167-178). Norwell, Massachusetts, USA: Kluwer Academic Publishers.
- Mármol, F. G., & Pérez, G. M. (2009). Security threats scenarios in trust and reputation models for distributed systems. *Computers & Security*, 28(7), 545-556.
- Mason, R. O. (1986). Four Ethical Issues of the Information Age. *Mis Quarterly*, 10(1), 5-12.
- McCarthy, B. (2002). New Economics of Sociological Criminology. *Annual Review of Sociology*, 28(1), 417-443.
- McCoy, C., & Fowler, R. (2004). "You are the key to security": establishing a successful security awareness program. Paper presented at the Proceedings of the SIGUCCS'04, Baltimore, Maryland.
- McCumber, J. (2005). *Assessing and managing security risk in IT systems: A structured methodology*. Boca Raton, Florida: Auerbach Publications.
- Molok, N. N. A., Chang, S., & Ahmad, A. (2010). *Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats*. Paper presented at the 8th Australian Information Security Management Conference, Perth, Western Australia.
- Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures. In S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith & S. Sinclair (Eds.), (Vol. 39, pp. 17-52).
- 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), 192-222.
- Myyry, L., Siponen, M., Pahlila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules An empirical study. *European Journal of Information Systems*, 18(2), 126-139.

- Nadkarni, S., & Gupta, R. (2007). A Task-Based Model of Perceived Website Complexity. [Article]. *MIS Quarterly*, 31(3), 501-524.
- Ng, B. Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815-825.
- Ng, B. Y., & Xu, Y. (2007). *Studying Users' Computer Security Behavior Using the Health Belief Model*. Paper presented at the 11th Pacific-Asia Conference on Information Systems
- NIST. (2009). Recommended Security Controls for Federal Information Systems and Organizations *NIST Special Publication 800-53 Revision 3*. National Institute of Standards and Technology.
- Ong, C.-S., Lai, J.-Y., & Wang, Y.-S. (2004). Factors affecting engineers' acceptance of asynchronous e-learning systems in high-tech companies. *Information & Management*, 41(6), 795-804.
- Ong, C. S., & Lai, J. Y. (2006). Gender differences in perceptions and relationships among dominants of e-learning acceptance. *Computers in Human Behavior*, 22(5), 816-829.
- Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' Behavior towards IS Security Policy Compliance*. Paper presented at the 40th Annual Hawaii International Conference on System Sciences, HICSS 2007. .
- Panko, R. R., & Beh, H. G. (2002). Monitoring for pornography and sexual harassment. *Communications of the ACM*, 45(1), 84-87.
- Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. New York: John Wiley & Sons, Inc.
- Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review*, 30(3), 549-583.
- Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *Management Information Systems Quarterly*, 30(1), 8.
- Peguero, A. A., Popp, A. M., Latimore, T. L., Shekarkhar, Z., & Koo, D. J. (2011). Social Control Theory and School Misbehavior: Examining the Role of Race and Ethnicity. *Youth Violence and Juvenile Justice*, 9(3), 259-275.
- Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security*, 14(2), 37-49.
- Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *Management Information Systems Quarterly*, 31(4), 623-656.

- Pinsonneault, A., & Kraemer, K. L. (1993). Survey Research Methodology in Management Information Systems: An Assessment. [Article]. *Journal of Management Information Systems*, 10(2), 75-105.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of applied psychology*, 88(5), 879-903.
- Ponemon, I. (2010). 2009 Annual Study: Cost of a Data Breach: The Ponemon Institute.
- Poole, M. S., & DeSanctis, G. (2004). Structuration theory in information systems research: Methods and controversies. In M. E. Whitman & A. B. Woszczynski (Eds.), *The handbook of information systems research* (pp. 206-249). Hershey, PA: IDEA Group Publishing.
- Posey, C., Roberts, T. L., Lowry, P. B., & Bennett, B. (2010). *How Explanation Adequacy of Security Policy Changes Decreases Organizational Computer Abuse*. Paper presented at the Proceedings of the Ninth Annual Workshop on HCI Research in MIS (SIGHCI), Paper 14, Saint Louis, Missouri.
- Puhakainen, P. (2006). *A design theory for information security awareness*. (Ph.D. Dissertation), University of Oulu, Finland. Retrieved from Dissertations & Theses: Full Text.(Publication No. AAT C827011).
- Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4), 757-778.
- Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8), 816-826.
- Richardson, R. (2008). 2008 CSI Computer Crime & Security Survey, Retrieved Feb. 2,, 2010, from <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2008.pdf>
- Richardson, R. (2009). 2009 CSI Computer Crime and Security Survey. *Computer Security Institute* Retrieved Dec. 10, 2010, from <http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf>
- Richardson, R. (2011). 2010 / 2011 CSI Computer Crime and Security Survey: Computer Security Institute.
- Ringle, C. M., Wende, S., & Will, S. (2005). SmartPLS Release 2.0 (M3) Beta. University of Hamburg, Hamburg, Germany: <http://www.smartpls.de>.
- Rogers, E. M. (1995). *Diffusion of innovations* (Fourth ed.). New York: The Free Press.

- Rouse, A., & Corbitt, B. (2008). There's SEM and" SEM": A Critique of the Use of PLS Regression in Information Systems Research. *ACIS 2008 Proceedings*, 81.
- Sambamurthy, V., & Chin, W. W. (1994). The Effects of Group Attitudes Toward Alternative GDSS Designs on the Decision making Performance of Computer Supported Groups\*. *Decision Sciences*, 25(2), 215-241.
- Schlienger, T., & Teufel, S. (2003). *Analyzing information security culture: increased trust by an appropriate information security culture*. Paper presented at the Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03).
- Schou, C., & Shoemaker, D. (2007). *Information Assurance for the Enterprise: A Roadmap to Information Security*. New York: McGraw-Hill Irwin.
- Schultz, E. (2004). Security training and awareness-fitting a square peg in a round hole. *Computers & Security*, 23(1), 1-2.
- Schweitzer, J. A. (1990). *Managing Information Security*: Elsevier Science & Technology Books.
- Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92-100.
- Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *The Journal of Consumer Research*, 15(3), 325-343.
- Shimazu, H. (2007). Business Content Security: Present Issues and Future Outlook for Its Employment. *NEC Technical Journal*, 2(1), 30-34.
- Shumarova, E. V., & Swatman, P. A. (2006). *The New Economy, eValue and the Impact on User Acceptance of Pervasive IT*. Paper presented at the 19th Bled eConference eValues, Bled, Slovenia.
- Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 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), 303-315.
- Siponen, M., Pahnla, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In H. Venter, Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. (Ed.), *IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 133-144): Boston: Springer.

- Siponen, M., Pahlila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, 43(2), 64-71.
- Siponen, M., & Vance, A. O. (2010). Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations. *MIS Quarterly*, 34(3), 487-502.
- Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48(7), 296-302.
- Spector, P. E. (2006). Method Variance in Organizational Research : Truth or Urban Legend? *Organizational Research Methods*, 6(2), 221-232.
- Stanton, J., Caldera, C., Isaac, A., Stam, K., & Marcinkowski, S. (2003). Behavioral Information Security: Defining the Criterion Space In P. M. Mastrangelo & W. J. Everton (Eds.), *The Internet at work or not: Preventing computer deviance. Symposium presentation at the 2003 meeting of the Society for Industrial and Organizational Psychology*. Orlando, FL.
- Stanton, J., Stam, K., Guzman, I., & Caldera, C. (2003, 5-8 Oct. 2003). *Examining the linkage between organizational commitment and information security*. Paper presented at the IEEE International Conference on Systems, Man and Cybernetics, 2003.
- Straub, D. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 147-169.
- Straub, D. (1990). Effective IS security. *Information Systems Research*, 1(3), 255-276.
- Straub, D. (1994). The Effect of Culture on IT Diffusion: E-Mail and FAX in Japan and the US. *Information Systems Research*, 5(1), 23.
- Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13(1), 24.
- Straub, D., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *Mis Quarterly*, 14(1), 45-60.
- Straub, D., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 22(4), 441-469.
- Swanson, M., Hash, J., & Bowen, P. (2006). Guide for developing security plans for federal information systems: National Institute of Standards and Technology (NIST) Special Publication 800-18 Revision 1.
- Talib, Y. A., & Dhillon, G. (2010). *Invited Paper: Employee Emancipation and Protection of Information*. Paper presented at the Proceedings of the 5th Annual Symposium on Information Assurance, New York, USA.

- Tanaka, J. S. (1987). "How Big Is Big Enough?": Sample Size and Goodness of Fit in Structural Equation Models with Latent Variables. *Child Development*, 58(1), 134. doi: 10.1111/1467-8624.ep7264172
- Taylor, S., & Todd, P. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(2), 144-176.
- Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, 33(8), 544-557.
- Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal Computing: Toward a Conceptual Model of Utilization. *Mis Quarterly*, 15(1), 125-143.
- Thompson, R. L., Higgins, C. A., & Howell, J. M. (1994). Influence of Experience on Personal Computer Utilization: Testing a Conceptual Model. *Journal of Management Information Systems*, 11(1), 167-187.
- Thomson, K. L., & von Solms, R. (2005). Information security obedience: a definition. *Computers & Security*, 24(1), 69-75.
- Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security*, 6(4), 167-173.
- Tornatzky, L. G., & Klein, K. J. (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on engineering management*, 29(1), 28-45.
- Trafimow, D., Sheeran, P., Conner, M., & Finlay, K. A. (2002). Evidence that perceived behavioural control is a multidimensional construct: Perceived control and perceived difficulty. *British Journal of Social Psychology*, 41(1), 101-121.
- Trevino, L. K. (1986). Ethical Decision Making in Organizations: A Person-Situation Interactionist Model. *The Academy of Management Review*, 11(3), 601-617.
- Trochim, W. M., & Donnelly, J. P. (2006). *The Research Methods Knowledge Base* (Third ed.). Cincinnati, OH: Atomic Dog.
- Tyler, T. R., & Blader, S. L. (2005). Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings. *Academy of Management Journal*, 48(6), 1143-1158.
- Tyler, T. R., Callahan, P. E., & Frost, J. (2007). Armed, and Dangerous (?): Motivating Rule Adherence Among Agents of Social Control. *Law & Society Review*, 41(2), 457-492.
- Urbaczewski, A., & Jessup, L. M. (2002). Does electronic monitoring of employee internet usage work? *Communications of the ACM*, 45(1), 80-83.



- Valentine, J. A. (2006). Enhancing the employee security awareness model. *Computer Fraud & Security*, 2006(6), 17-19.
- Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research*, 11(4), 342-365.
- Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, 39(2), 273-315.
- Venkatesh, V., & Davis, F. D. (1996). A Model of the Antecedents of Perceived Ease of Use: Development and Test. *Decision Sciences*, 27(3), 451-481.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, 46(2), 186-204.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478.
- Verizon. (2009). Data Breach Investigations Report Retrieved Oct. 2, 2010, from <http://www.verizonbusiness.com/resources/security/reports/2009databreachrp.pdf;2009>
- von Solms, B., & von Solms, R. (2005). From information security to...business security? *Computers & Security*, 24(4), 271-273.
- von Solms, R. (1998). Information security management (3): the code of practice for information security management (BS 7799). *Information Management & Computer Security*, 6(5), 224-225.
- Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, 20(3), 267-284.
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), 101-105.
- Warkentin, M., Willison, R., & Johnston, A. C. (2011). *The Role of Perceptions of Organizational Injustice and Techniques of Neutralization in Forming Computer Abuse Intentions*. Paper presented at the AMCIS 2011 Proceedings - All Submissions. Paper 318.
- Wasserman, J. J. (1969). Plugging the leaks in computer security. *Harvard Business Review*, 47(5), 119-129.
- Werlinger, R., Hawkey, K., & Beznosov, K. (2008). *Human, organizational and technological challenges of implementing IT security in organizations*. Paper

presented at the Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008), Plymouth, UK.

- Wetzels, M., Odekerken-Schroder, G., & Van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration. *MIS Quarterly*, 33(1), 177-195.
- Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, 46(8), 91-95.
- Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, 24(1), 43-57.
- Whitman, M. E. (2008). Security Policy: From Design to Maintenance. In D. W. Straub, S. Goodman & R. Baskerville (Eds.), *Information Security: Policy, Processes, and Practices*. Armonk NY: M E Sharpe Inc.
- Whitman, M. E., & Mattord, H. J. (2008). *Management of Information Security* (Second ed.). Boston, USA: Thomson Course Technology.
- Whitman, M. E., & Mattord, H. J. (2009). *Principles of Information Security* (Third ed.). Boston, MA: Course Technology Press.
- Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information systems security and the need for policy. In G. Dhillon (Ed.), *Information Security Management: Global Challenges in the New Millennium*. Hershey, PA, USA: Idea Group Publishing.
- Wood, C. C., & Banks, W. W. (1993). Human error: an overlooked but significant information security problem. *Computers & Security*, 12(1), 51-60.
- Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Security Journal: A Global Perspective*, 16(6), 315-331.
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816.
- Wu, J. H., Chen, Y. C., & Lin, L. M. (2007). Empirical evaluation of the revised end user computing acceptance model. *Computers in Human Behavior*, 23(1), 162-174.
- Wybo, M. D., & Straub, D. (1989). Protecting organizational information resources. *Information Resources Management Journal (IRMJ)*, 2(4), 1-16.
- Xia, W., & Lee, G. (2000). *The influence of persuasion, training and experience on user perceptions and acceptance of IT innovation*. Paper presented at the Proceedings of the twenty first international conference on Information systems, Brisbane, Queensland, Australia.

- Xue, Y., Liang, H., & Wu, L. (2010). Punishment, Justice, and Compliance in Mandatory IT Settings. *Information Systems Research*, 22(2), 400-414.
- Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, 17(4), 330-340.
- Zikmund, W. G. (2003). *Business Research Methods*. Mason, Ohio: Thomson/South-Western.

## Appendix A

### Cover Letter

*Dear Banks' employees*

Thank you for participating in this survey. I am conducting a research project entitled "Information Security Policy Compliance: A user Acceptance Perspective" as part of a **dissertation at Dakota State University.**

The purpose of the study is to **examine users' behavioral intention to comply with Information Security Policies (ISPs).** You as an employee are invited to participate in the study by *completing the attached survey.* We realize that your time is valuable and have attempted to keep the requested information as brief and concise as possible. It will take you approximately 20 minutes of your time. Your participation will contribute significantly to the successful completion of this study. Your participation in this project is voluntary and anonymous. You may withdraw from the study at any time without consequence.

There are *no known risks* to you for participating in this study. Your responses are strictly confidential, you are not required to provide your name or what bank you are working at or other information that may reveal your identity. The collected data will not be used for any purposes other than research purposes. When the data and analysis are presented, you will not be linked to the data by your name, title, place of work or any other identifying item.

If you have any questions regarding this study, please feel free to contact us

Ahmad Al-Omari  
Dakota State University  
College of Business & Information Systems  
Dept of Management of Information Systems  
[aaal-omari8026@pluto.dsu.edu](mailto:aaal-omari8026@pluto.dsu.edu)  
+605-270-1215

Dr. Omar El-Gayar  
Dakota State University  
College of Business & Information Systems  
Dept of Management of Information Systems  
[Omar.El-gayar@dsu.edu](mailto:Omar.El-gayar@dsu.edu)  
+605-256-5799

Dr. Amit Deokar  
Dakota State University  
College of Business & Information Systems  
Dept of Management of Information  
[Amit.Deokar@dsu.edu](mailto:Amit.Deokar@dsu.edu)  
+605-256-516

## Appendix B

### Survey Instrument

1. Has your bank establish Information Security Policy
 

<input type="checkbox"/> Yes	<input type="checkbox"/> No
------------------------------	-----------------------------
  
2. Gender
 

<input type="checkbox"/> Male	<input type="checkbox"/> Female
-------------------------------	---------------------------------
  
3. Age
 

<input type="checkbox"/> 20-29 years	<input type="checkbox"/> 30-39 years
<input type="checkbox"/> 40-49 years	<input type="checkbox"/> $\geq$ 50 years
  
4. Education level
 

<input type="checkbox"/> High School	<input type="checkbox"/> Collage
<input type="checkbox"/> Bachelor's Degree	<input type="checkbox"/> Master's Degree
<input type="checkbox"/> Doctoral Degree	<input type="checkbox"/> Other (_____)
  
5. Experience
 

<input type="checkbox"/> 1-5 years	<input type="checkbox"/> 6-10 years
<input type="checkbox"/> 11-15 years	<input type="checkbox"/> 16-20 years
<input type="checkbox"/> > 20 years	
  
6. Years with the Bank
 

<input type="checkbox"/> Less than 6 months	<input type="checkbox"/> 6 months to 1 year
<input type="checkbox"/> 1 to 2 years	<input type="checkbox"/> 2 to 4 years
<input type="checkbox"/> 4 to 6 years	<input type="checkbox"/> 6 to 10 years
<input type="checkbox"/> 10 to 15 years	<input type="checkbox"/> More than 15 years
  
7. Functional area of work
 

<input type="checkbox"/> Teller	<input type="checkbox"/> Administration/Clerical
<input type="checkbox"/> Information Technology	<input type="checkbox"/> Audit
<input type="checkbox"/> Marketing and Sales	<input type="checkbox"/> Credit Department
<input type="checkbox"/> Treasury & investment	<input type="checkbox"/> Other (_____)
  
8. For how long you have been using the computer \_\_\_\_\_ years.
  
9. For how long you have been speaking English \_\_\_\_\_ years.
  
10. How many hours a day do you use the computer at work \_\_\_\_\_ hours?
  
11. Organizational level (managerial) put others
  - Non-management
  - Line management (supervising non-management personnel)
  - Middle management
  - Senior management
  - Executive/Senior Vice President
  - CEO/President
  
12. Please indicate whether you use, or have used in the past, any of the following computer software for job-related work: (check all that apply)
  - Spreadsheets (e.g., Microsoft Excel)
  - Word processing (e.g., Microsoft Word)
  - E-mail
  - Programming languages (e.g., C++, Java, Visual Basic)
  - Application packages (e.g., accounting or payroll software)
  - Database applications
  - Bank's special tailored software

		Strongly Disagree	Disagree	Somewhat Disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
<b>Intention to Comply</b>								
1	I intend to comply with the requirements of the ISP of my organization	1	2	3	4	5	6	7
2	I intend to protect information resources according to the requirements of the ISP of my organization.	1	2	3	4	5	6	7
3	I intend to protect technology resources according to the requirements of the ISP of my organization.	1	2	3	4	5	6	7
4	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information resources.	1	2	3	4	5	6	7
5	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use technology resources.	1	2	3	4	5	6	7
6	I intend to recommend that others comply with ISP.	1	2	3	4	5	6	7
7	I intend to assist others in complying with ISP.	1	2	3	4	5	6	7
<b>Perceived Usefulness of Protection</b>								
1	<i>My job would be easier to perform without complying with my organization's ISP.</i>	1	2	3	4	5	6	7
2	Complying with my organization's ISP gives me greater control over my work.	1	2	3	4	5	6	7
3	Complying with my organization's ISP does not hinder my job performance.	1	2	3	4	5	6	7
4	Complying with my organization's ISP addresses my job-related security needs.	1	2	3	4	5	6	7
5	Complying with my organization's ISP saves me time.	1	2	3	4	5	6	7
6	Complying with my organization's ISP enables me to accomplish tasks more securely.	1	2	3	4	5	6	7
7	Complying with my organization's ISP supports critical security aspects of my job.	1	2	3	4	5	6	7
8	Complying with my organization's ISP reduces unproductive activities.	1	2	3	4	5	6	7
9	Complying with my organization's ISP enhances my effectiveness on the job.	1	2	3	4	5	6	7
10	Complying with my organization's ISP improves the quality of the work I do.	1	2	3	4	5	6	7
11	Complying with my organization's ISP improves my productivity.	1	2	3	4	5	6	7
12	Complying with my organization's ISP makes it easier to do my job.	1	2	3	4	5	6	7
13	Overall, I find complying with my organization's ISP useful in my job.	1	2	3	4	5	6	7
<b>Perceived Complexity</b>								
1	I often become confused when complying with the requirements of my organization's ISP	1	2	3	4	5	6	7
2	I make errors frequently when complying with the requirements of my organization's ISP	1	2	3	4	5	6	7
3	Complying with the requirements of my organization's ISP is often frustrating.	1	2	3	4	5	6	7
4	Learning to comply with the requirements of my organization's ISP is hard for me.	1	2	3	4	5	6	7
5	Compliance with the requirements of my organization's ISP requires a lot of mental effort.	1	2	3	4	5	6	7
6	<i>I find it easy to recover from errors encountered when complying with my organization's ISP</i>	1	2	3	4	5	6	7
7	The compliance requirements of my organization's ISP are rigid and inflexible.	1	2	3	4	5	6	7
8	<i>I find it easy to comply with my organization's ISP.</i>	1	2	3	4	5	6	7
9	I find it hard to comply with the requirements of my organization's ISP.	1	2	3	4	5	6	7
10	<i>It is easy for me to remember how to perform tasks while complying with my organization's ISP.</i>	1	2	3	4	5	6	7
11	<i>My organization's ISP provides helpful guidance in performing tasks.</i>	1	2	3	4	5	6	7
12	<i>Overall, I find my organization's ISP easy to use.</i>	1	2	3	4	5	6	7
<b>Self-Efficacy</b>								
1	I have the necessary skills to fulfill the requirements of the ISP.	1	2	3	4	5	6	7
2	I have the necessary knowledge to fulfill the requirements of the ISP.	1	2	3	4	5	6	7
3	I have the necessary competencies to fulfill the requirements of the ISP.	1	2	3	4	5	6	7
4	I would feel comfortable following my organization's ISP on my own.	1	2	3	4	5	6	7
5	If I wanted to, I could easily comply with my organization's ISP on my own.	1	2	3	4	5	6	7
6	I would be able to follow most of the ISP even if there was no one around to help me	1	2	3	4	5	6	7

Items 6, 7, 9, and 12 load low on Perceived Complexity so they are removed from the final analysis.

Items in *Italic* are reversed coded.

		Strongly Disagree	Disagree	Somewhat Disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
<b>Controllability</b>								
1	I have the resources (like antivirus, firewall, brochures) to help me comply with the requirements of my organization's ISP.	1	2	3	4	5	6	7
2	I have the resources to protect my organization's information and technology assets from potential threats.	1	2	3	4	5	6	7
3	Threats to information security in my work are under control.	1	2	3	4	5	6	7
4	In general, technology used at my organization is advanced enough to prevent information security threats.	1	2	3	4	5	6	7
<b>User Awareness of General Information Security</b>								
<b>General Information Security Awareness</b>								
1	Overall, I am aware of the potential security threats and their negative consequences.	1	2	3	4	5	6	7
2	I have sufficient knowledge about the cost of potential security problems.	1	2	3	4	5	6	7
3	I understand the concerns regarding information security and the risks they pose in general.	1	2	3	4	5	6	7
<b>Technology Awareness</b>								
4	I follow news and developments about the security related technologies.							
5	I discuss Internet security issues or anecdotes with friends and people around me.	1	2	3	4	5	6	7
6	I read about the problems of malicious threats attacking users' computers.	1	2	3	4	5	6	7
7	I seek advice about security issues through online discussion forums, magazines, and other media sources	1	2	3	4	5	6	7
<b>User Awareness of Information Security Policies</b>								
1	I am aware of my organization's rules of behavior for use of computer resources.	1	2	3	4	5	6	7
2	I am aware of my organization's specific guidelines that describe acceptable use of information systems.	1	2	3	4	5	6	7
3	I am aware that my organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use.	1	2	3	4	5	6	7
4	I am aware that my organization has a formal policy that forbids employees from installing their own software on work computers.	1	2	3	4	5	6	7
5	I am aware that my organization has specific guidelines that govern what tasks employees are allowed to perform on their work computers.	1	2	3	4	5	6	7
6	I am aware of my organization's specific guidelines that describe acceptable use of computer passwords.	1	2	3	4	5	6	7
7	I am aware that my organization has a formal policy that forbids employees from modifying computerized data in an unauthorized way.	1	2	3	4	5	6	7
8	I understand the rules and regulations prescribed by my organization's ISP.	1	2	3	4	5	6	7
9	I understand my responsibilities toward enhancing my organization's information system security as prescribed in the organization's ISP.	1	2	3	4	5	6	7
<b>User Awareness of SETA Program</b>								
1	I am aware that my organization provides training to help employees comply with the organization's ISP.	1	2	3	4	5	6	7
2	I am aware that my organization provides training to help employees improve their awareness of computer and information security issues.	1	2	3	4	5	6	7
3	I am aware that my organization provides employees with education on computer software copyright laws.	1	2	3	4	5	6	7
4	I am aware that employees in my organization are briefed on the consequences of modifying computerized data in an unauthorized way.	1	2	3	4	5	6	7
5	I am aware that my organization educates employees on their computer security responsibilities.	1	2	3	4	5	6	7
6	I am aware that employees in my organization are briefed on the consequences of accessing computer systems that they are not authorized to use.	1	2	3	4	5	6	7
7	I am aware that employees in my organization are instructed in the appropriate usage of information technologies.	1	2	3	4	5	6	7

		Strongly Disagree	Disagree	Somewhat Disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
<b>User Awareness of SETA Program</b>								
8	I am aware that my organization educates employees on their responsibilities for managing computer passwords.	1	2	3	4	5	6	7
9	I am aware that my organization educates employees on appropriate use of information technology resources (e.g. email)	1	2	3	4	5	6	7
<b>User Awareness of Computer Monitoring</b>								
1	I am aware that my organization monitors any modification or altering of computerized data by employees.	1	2	3	4	5	6	7
2	I am aware that employees' computing activities are monitored by my organization.	1	2	3	4	5	6	7
3	I am aware that my organization monitors computing activities to ensure that employees are performing only explicitly authorized tasks.	1	2	3	4	5	6	7
4	I am aware that my organization reviews logs of employees' computing activities on a regular basis.	1	2	3	4	5	6	7
5	I am aware that my organization conducts periodic audits to detect the use of unauthorized software on its computers.	1	2	3	4	5	6	7
6	I am aware that my organization regularly monitors employee access to sensitive computerized information.	1	2	3	4	5	6	7
7	I am aware that my organization actively monitors the content of employees' work e-mail messages.	1	2	3	4	5	6	7
<b>Subjective Norm</b>								
1	Upper level management thinks I should comply with the requirements of my organization's ISPs.	1	2	3	4	5	6	7
2	My boss thinks that I should comply with the requirements of my organization's ISPs.	1	2	3	4	5	6	7
3	My colleagues think that I should comply with the requirements of my organization's ISPs.	1	2	3	4	5	6	7
4	The information security/technology department in my organization thinks that I should comply with the requirements of my organization's ISPs.	1	2	3	4	5	6	7
5	Other computer technical specialists in the organization think that I should comply with the requirements of my organization's ISPs.	1	2	3	4	5	6	7



## Appendix C

Table C1. Cross Loadings

	<b>CMA</b>	<b>Cont.</b>	<b>GISA</b>	<b>IC</b>	<b>ISPA</b>	<b>PC</b>	<b>PU</b>	<b>SE</b>	<b>SETA</b>	<b>SN</b>	<b>TA</b>
<b>CMA1</b>	<b>0.863</b>	0.267	0.309	0.291	-0.399	-0.168	0.272	0.371	0.326	0.259	0.303
<b>CMA2</b>	<b>0.864</b>	0.322	0.314	0.287	-0.409	-0.233	0.262	0.370	0.332	0.251	0.336
<b>CMA3</b>	<b>0.853</b>	0.278	0.308	0.312	-0.375	-0.191	0.303	0.355	0.313	0.242	0.313
<b>CMA4</b>	<b>0.876</b>	0.237	0.255	0.268	-0.330	-0.229	0.257	0.346	0.265	0.272	0.274
<b>CMA5</b>	<b>0.878</b>	0.255	0.284	0.276	-0.341	-0.196	0.283	0.348	0.283	0.265	0.224
<b>CMA6</b>	<b>0.875</b>	0.273	0.363	0.250	-0.350	-0.222	0.301	0.349	0.296	0.296	0.271
<b>CMA7</b>	<b>0.876</b>	0.274	0.347	0.267	-0.353	-0.219	0.306	0.344	0.279	0.304	0.246
<b>CONT1</b>	0.268	<b>0.895</b>	0.242	0.178	-0.331	-0.098	0.179	0.350	0.280	-0.081	0.204
<b>CONT2</b>	0.250	<b>0.886</b>	0.244	0.198	-0.337	-0.167	0.213	0.352	0.294	-0.042	0.215
<b>CONT3</b>	0.303	<b>0.874</b>	0.196	0.210	-0.356	-0.123	0.192	0.354	0.299	-0.048	0.222
<b>CONT4</b>	0.278	<b>0.837</b>	0.245	0.185	-0.306	-0.138	0.182	0.327	0.274	-0.079	0.206
<b>GISA1</b>	0.335	0.231	<b>0.885</b>	-0.025	-0.270	-0.224	0.288	0.211	0.178	0.207	0.193
<b>GISA2</b>	0.338	0.281	<b>0.916</b>	-0.069	-0.377	-0.171	0.348	0.243	0.230	0.263	0.230
<b>GISA3</b>	0.319	0.221	<b>0.955</b>	-0.018	-0.295	-0.200	0.328	0.243	0.215	0.223	0.157
<b>IC1</b>	0.261	0.149	-0.052	<b>0.890</b>	-0.257	-0.148	0.266	0.193	0.287	0.323	0.221
<b>IC2</b>	0.266	0.140	-0.037	<b>0.890</b>	-0.259	-0.140	0.284	0.202	0.285	0.315	0.238
<b>IC3</b>	0.296	0.209	-0.050	<b>0.891</b>	-0.285	-0.146	0.278	0.241	0.298	0.320	0.250
<b>IC4</b>	0.295	0.162	-0.028	<b>0.880</b>	-0.277	-0.184	0.257	0.240	0.308	0.343	0.261
<b>IC5</b>	0.267	0.206	-0.042	<b>0.880</b>	-0.277	-0.199	0.276	0.258	0.323	0.316	0.261
<b>IC6</b>	0.259	0.216	-0.029	<b>0.853</b>	-0.251	-0.226	0.258	0.272	0.333	0.305	0.327
<b>IC7</b>	0.311	0.268	-0.010	<b>0.830</b>	-0.282	-0.195	0.275	0.325	0.364	0.326	0.290
<b>ISPA1</b>	-0.394	-0.329	-0.340	-0.296	<b>0.874</b>	-0.078	-0.292	-0.317	-0.296	-0.325	-0.391
<b>ISPA2</b>	-0.379	-0.357	-0.298	-0.288	<b>0.887</b>	-0.112	-0.253	-0.309	-0.297	-0.282	-0.386
<b>ISPA3</b>	-0.361	-0.343	-0.297	-0.246	<b>0.901</b>	-0.120	-0.270	-0.313	-0.298	-0.301	-0.383
<b>ISPA4</b>	-0.388	-0.347	-0.319	-0.287	<b>0.906</b>	-0.090	-0.284	-0.334	-0.339	-0.334	-0.425
<b>ISPA5</b>	-0.387	-0.339	-0.315	-0.261	<b>0.883</b>	-0.085	-0.267	-0.320	-0.322	-0.332	-0.404
<b>ISPA6</b>	-0.360	-0.305	-0.321	-0.282	<b>0.868</b>	-0.061	-0.267	-0.345	-0.325	-0.355	-0.429
<b>ISPA7</b>	-0.343	-0.310	-0.266	-0.251	<b>0.869</b>	-0.077	-0.268	-0.287	-0.299	-0.307	-0.374
<b>ISPA8</b>	-0.330	-0.338	-0.256	-0.253	<b>0.858</b>	-0.066	-0.270	-0.334	-0.317	-0.287	-0.362
<b>ISPA9</b>	-0.371	-0.345	-0.293	-0.279	<b>0.862</b>	-0.092	-0.287	-0.285	-0.348	-0.295	-0.381
<b>PC1</b>	-0.185	-0.112	-0.202	-0.154	-0.070	<b>0.937</b>	-0.204	-0.202	-0.168	-0.192	-0.181
<b>PC10</b>	-0.217	-0.119	-0.193	-0.145	-0.095	<b>0.950</b>	-0.231	-0.227	-0.199	-0.224	-0.173
<b>PC11</b>	-0.227	-0.127	-0.188	-0.174	-0.105	<b>0.805</b>	-0.253	-0.214	-0.196	-0.222	-0.173
<b>PC2</b>	-0.205	-0.139	-0.136	-0.188	-0.069	<b>0.872</b>	-0.208	-0.290	-0.219	-0.189	-0.254
<b>PC3</b>	-0.224	-0.165	-0.192	-0.224	-0.124	<b>0.941</b>	-0.240	-0.301	-0.226	-0.265	-0.195
<b>PC4</b>	-0.243	-0.167	-0.197	-0.217	-0.134	<b>0.938</b>	-0.262	-0.325	-0.244	-0.277	-0.186
<b>PC5</b>	-0.196	-0.117	-0.208	-0.171	-0.069	<b>0.785</b>	-0.219	-0.209	-0.181	-0.208	-0.195
<b>PC8</b>	-0.180	-0.122	-0.211	-0.124	0.011	<b>0.803</b>	-0.144	-0.202	-0.180	-0.157	-0.182
<b>PU1</b>	0.252	0.108	0.249	0.220	-0.215	-0.200	<b>0.768</b>	0.244	0.223	0.240	-0.120
<b>PU10</b>	0.251	0.220	0.321	0.233	-0.264	-0.226	<b>0.836</b>	0.355	0.303	0.282	-0.071
<b>PU11</b>	0.239	0.203	0.315	0.202	-0.262	-0.227	<b>0.827</b>	0.303	0.251	0.302	-0.067
<b>PU12</b>	0.275	0.179	0.289	0.261	-0.255	-0.240	<b>0.814</b>	0.358	0.272	0.320	-0.052
<b>PU13</b>	0.294	0.187	0.266	0.279	-0.300	-0.228	<b>0.810</b>	0.325	0.250	0.314	-0.031
<b>PU2</b>	0.296	0.202	0.299	0.281	-0.309	-0.201	<b>0.850</b>	0.339	0.299	0.317	-0.081
<b>PU3</b>	0.256	0.177	0.305	0.261	-0.248	-0.228	<b>0.823</b>	0.314	0.275	0.307	-0.078
<b>PU4</b>	0.261	0.183	0.286	0.260	-0.221	-0.205	<b>0.850</b>	0.291	0.294	0.293	-0.096
<b>PU5</b>	0.260	0.160	0.282	0.263	-0.220	-0.206	<b>0.846</b>	0.278	0.255	0.284	-0.080
<b>PU6</b>	0.273	0.194	0.309	0.261	-0.281	-0.170	<b>0.831</b>	0.317	0.283	0.336	-0.077

Table C1. Cross Loadings (Continued)

	CMA	Cont	GISA	IC	ISPA	PC	PU	SE	SETA	SN	TA
<b>PU7</b>	0.295	0.197	0.260	0.294	-0.254	-0.176	<b>0.850</b>	0.347	0.281	0.303	-0.086
<b>PU8</b>	0.298	0.177	0.295	0.269	-0.274	-0.228	<b>0.838</b>	0.328	0.281	0.335	-0.097
<b>PU9</b>	0.266	0.188	0.299	0.248	-0.242	-0.207	<b>0.831</b>	0.325	0.238	0.291	-0.063
<b>SE1</b>	0.335	0.328	0.189	0.249	-0.319	-0.250	0.322	<b>0.862</b>	0.388	0.308	0.281
<b>SE2</b>	0.338	0.344	0.214	0.230	-0.335	-0.254	0.334	<b>0.887</b>	0.357	0.301	0.283
<b>SE3</b>	0.350	0.361	0.233	0.216	-0.310	-0.260	0.303	<b>0.881</b>	0.351	0.270	0.261
<b>SE4</b>	0.354	0.341	0.227	0.272	-0.321	-0.223	0.361	<b>0.891</b>	0.367	0.336	0.238
<b>SE5</b>	0.385	0.334	0.227	0.232	-0.296	-0.277	0.333	<b>0.872</b>	0.370	0.314	0.237
<b>SE6</b>	0.377	0.373	0.238	0.288	-0.306	-0.235	0.359	<b>0.860</b>	0.376	0.327	0.262
<b>SETA1</b>	0.311	0.294	0.196	0.335	-0.319	-0.214	0.298	0.363	<b>0.865</b>	0.285	0.279
<b>SETA2</b>	0.327	0.320	0.194	0.335	-0.311	-0.199	0.284	0.392	<b>0.875</b>	0.264	0.273
<b>SETA3</b>	0.284	0.272	0.161	0.321	-0.283	-0.197	0.298	0.355	<b>0.881</b>	0.258	0.231
<b>SETA4</b>	0.291	0.280	0.203	0.321	-0.313	-0.187	0.272	0.382	<b>0.887</b>	0.275	0.299
<b>SETA5</b>	0.263	0.272	0.188	0.306	-0.310	-0.227	0.287	0.364	<b>0.880</b>	0.279	0.270
<b>SETA6</b>	0.312	0.266	0.216	0.326	-0.286	-0.245	0.293	0.361	<b>0.889</b>	0.300	0.278
<b>SETA7</b>	0.274	0.275	0.211	0.280	-0.349	-0.191	0.256	0.357	<b>0.873</b>	0.283	0.308
<b>SETA8</b>	0.311	0.296	0.216	0.298	-0.345	-0.154	0.279	0.359	<b>0.865</b>	0.271	0.280
<b>SETA9</b>	0.332	0.323	0.206	0.311	-0.327	-0.198	0.299	0.385	<b>0.867</b>	0.268	0.303
<b>SN1</b>	0.302	-0.058	0.251	0.327	-0.314	-0.243	0.331	0.301	0.282	<b>0.893</b>	0.261
<b>SN2</b>	0.284	-0.053	0.266	0.299	-0.312	-0.217	0.352	0.320	0.298	<b>0.894</b>	0.239
<b>SN3</b>	0.260	-0.076	0.183	0.322	-0.298	-0.256	0.324	0.299	0.257	<b>0.896</b>	0.273
<b>SN4</b>	0.267	-0.063	0.213	0.349	-0.335	-0.209	0.332	0.337	0.264	<b>0.900</b>	0.241
<b>SN5</b>	0.275	-0.063	0.208	0.344	-0.329	-0.193	0.289	0.320	0.305	<b>0.875</b>	0.271
<b>TA1</b>	0.270	0.210	0.149	0.267	-0.403	-0.171	-0.128	0.238	0.284	0.267	<b>0.893</b>
<b>TA2</b>	0.296	0.216	0.226	0.231	-0.373	-0.215	-0.074	0.289	0.266	0.241	<b>0.902</b>
<b>TA3</b>	0.273	0.228	0.185	0.300	-0.401	-0.186	-0.059	0.259	0.291	0.264	<b>0.888</b>
<b>TA4</b>	0.310	0.216	0.189	0.288	-0.421	-0.205	-0.070	0.273	0.300	0.259	<b>0.889</b>