

Dakota State University Beadle Scholar

Masters Theses & Doctoral Dissertations

Spring 5-1-2017

Information Security Awareness: Antecedents and User Satisfaction Perspective

Yazan Alshboul
Dakota State University

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

Recommended Citation

Alshboul, Yazan, "Information Security Awareness: Antecedents and User Satisfaction Perspective" (2017). *Masters Theses & Doctoral Dissertations*. 307.
<https://scholar.dsu.edu/theses/307>

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.



**INFORMATION SECURITY AWARENESS:
ANTECEDENTS AND USER SATISFACTION
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, 2017

By

Yazan Alshboul

Dissertation Committee:

Dr. Kevin Streff

Dr. Wayne Pauli

Dr. Gabe Mydland

Dr. Shuyuan (Lance) Deng



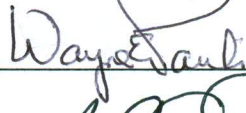
DISSERTATION APPROVAL FORM

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: Yazan Alshboul

Doctorate's Dissertation Title: Information Security Awareness: Antecedents and User Satisfaction Perspective

Dissertation Chair: Dr. Kevin Streff  Date: 2/28/17

Committee member: Dr. Wayne Pauli  Date: 3/20/17

Committee member: Dr. Gabe Mydland  Date: 3/20/17

Committee member: Dr. Shuyuan (Lance) Deng  Date: 3/20/2017

ACKNOWLEDGMENT

I would like to express my sincere appreciation for the efforts of Dr. Kevin Streff, my dissertation committee chair professor, for his guidance, encouragement, and patience. His support for my work has been, from the beginning, an engine for my effort and progress. He continually motivates me in research since the first time I set foot in Madison, SD. Without his guidance and persistent support, this study would not have come into existence.

Besides my advisor, I am profoundly grateful for the support of my committee members, Dr. Wayne Pauli, Dr. Gabe Mydland, and Dr. Shuyuan (Lance) Deng. They are incredibly generous with their help and time and provide me with insightful comments and encouragement. I would also like to thank Kacie Fodness, Jay Kahl, Dr. Bilal Sayaheen, and Omar Darwish who helped me in my data collection.

Not to forget to send a special thank you to my family for their continuous support. Words cannot express my profound gratitude, respect, and love for my mother for her passion, my father who inspire me in this life and support me emotionally and financially, and brothers. I stand speechless recalling the love, support, patience, and kindness of my wife, Reem. I am very blessed to have such an amazing woman as you. I will never forget your standing beside me in this period of life. Last but not least, I would like to thank my beautiful little daughter, Dareen. She came to this life while her father is busy with his Ph.D. Truly, I will not forget the fun I had with my little girl who brings happiness and joyful moments to my life, especially when she used to stand behind me and start singing “Jump Jump”.

ABSTRACT

In the fast-changing business world of today, organizations heavily rely on information systems to efficiently perform various business tasks. Using information systems involves some risks, particularly risks related to cybersecurity. Most organizations develop technical and procedural measures to protect their information systems. However, relying only on technical based security solutions is not enough. Organizations must consider technical security solutions along with social, human, and organizational factors (employees). The human element represents the employees (insiders) who use the information systems and other technology resources in their day-to-day operations. Employees' information security awareness, specifically information security policy (ISP) awareness, is essential to protect organizational information systems. This study adapts the Innovation Diffusion Theory along with other theoretical foundations to examine the antecedents of ISP awareness and its impact on the satisfaction with ISP and security practices.

Information security behavior and ISP compliance have been investigated heavily in the last two decades. However, there are still some gaps in this area, and more research is needed as cybersecurity risks are likely to continue in the future. One of the gaps is the lack of empirical investigations of the antecedents of ISP awareness. Another gap is that the literature addresses the impact of ISP awareness on several behavioral aspects, such as attitude toward ISP compliance, intention to comply with ISP, actual compliance behavior, and perception beliefs, but none of the prior studies examine the ISP awareness effects on the satisfaction with ISPs. Therefore, the current study aims to address these gaps by identifying the antecedents of ISP awareness and investigating the relationships between ISP awareness and satisfaction. In particular, the researcher categorizes the antecedents into two categories: organizational and individual enablers. The proposed research model posits that along with individuals' factors (self-efficacy and technology awareness), employees' ISP awareness is impacted by organizational factors (ISP fairness and ISP quality). The study further posits that ISP awareness has a direct impact on the satisfaction with ISP and security practices.

The researcher used a survey to collect data that captures beliefs and perceptions regarding ISP awareness. A sample of 236 employees in universities in the United States is collected to evaluate the research model. Results indicated that ISP quality, self-efficacy, and

technology security awareness significantly impact ISP awareness. ISP awareness is found to have a significant direct effect on the satisfaction with ISP and security practices and an indirect effect through perceived usefulness of ISP. However, ISP fairness is found to have a non-significant impact on the ISP awareness.

Overall, the current study presents significant contributions toward understanding the antecedents of ISP awareness and its role in impacting the perceptions of information security policies. This study provides a starting point toward including satisfaction aspect in information security behavioral domain.

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,



Yazan Alshboul

TABLE OF CONTENTS

DISSERTATION APPROVAL FORM.....	II
ACKNOWLEDGMENT	III
ABSTRACT.....	IV
DECLARATION.....	VI
TABLE OF CONTENTS	VII
LIST OF TABLES	X
LIST OF FIGURES	XI
CHAPTER ONE: INTRODUCTION.....	1
BACKGROUND AND MOTIVATION	1
PROBLEM OF STUDY	3
RESEARCH QUESTIONS	4
SIGNIFICANCE AND CONTRIBUTIONS	4
ORGANIZATION OF THE DISSERTATION.....	5
CHAPTER TWO: LITERATURE REVIEW.....	6
INFORMATION SECURITY OVERVIEW.....	6
<i>Information Security Approaches.....</i>	<i>7</i>
<i>Information Security Policy Awareness</i>	<i>8</i>
INFORMATION SECURITY BEHAVIORAL APPROACHES	13
<i>Theory Based Literature Review.....</i>	<i>14</i>
Theory of Reasoned Action/ Theory of Planned Behavior (TRA/TPB).....	14
General Deterrence Theory	19
Protection Motivation Theory	23
Technology Acceptance Model.....	27
Theory Integration of the Main Theories: TRA/TPB, GDT, PMT, and TAM.....	28
User Satisfaction.....	31
<i>Literature Gaps and Limitations</i>	<i>33</i>
CHAPTER THREE: RESEARCH MODEL AND HYPOTHESES.....	35
THEORETICAL FRAMEWORK	36
<i>Information Security Awareness</i>	<i>36</i>
<i>Innovation Diffusion Theory</i>	<i>42</i>
<i>Equity Theory vs. Information Security Awareness</i>	<i>44</i>

RESEARCH MODEL AND HYPOTHESES	45
<i>Perceived usefulness and employee satisfaction with security practices</i>	48
<i>ISP Awareness and perceived usefulness of ISP</i>	50
<i>ISP Awareness and user satisfaction with security practices</i>	51
<i>ISP Awareness Antecedents</i>	53
<i>Organizational Factors</i>	53
<i>Individual Factors</i>	56
CHAPTER FOUR: RESEARCH METHODOLOGY	58
RESEARCH DESIGN	58
SURVEY INSTRUMENT DESIGN.....	60
SURVEY INSTRUMENT VALIDATION.....	64
<i>Face and Content Validity</i>	64
<i>Construct and Measurement Model Evaluation</i>	65
POPULATION SAMPLING AND DATA COLLECTION	68
<i>Sample Size</i>	68
<i>Data Collection</i>	69
CHAPTER FIVE: DATA ANALYSIS AND RESULTS.....	71
SAMPLE DATA DESCRIPTION AND STATISTICS	71
RESEARCH MODEL EVALUATION OVERVIEW	73
MEASUREMENT MODEL EVALUATION.....	75
<i>Reflective Measurement Model Evaluation</i>	75
Internal Consistency	76
Convergent Validity	77
Discriminant Validity	79
<i>Formative Measurement Model Evaluation</i>	81
Convergent Validity of Formative Construct	81
Collinearity Assessment	83
Assessing the Significance and Relevance of the Formative Indicators	84
STRUCTURAL MODEL EVALUATION	86
<i>Path Significance and Coefficient Assessment</i>	86
<i>Coefficient of Determination (R²) and Total Effects</i>	87
CHAPTER SIX: DISCUSSION AND IMPLICATIONS.....	90
OVERVIEW OF THE STUDY AND FINDINGS	90
STUDY FINDINGS DISCUSSION	92
THEORETICAL CONTRIBUTION.....	96
PRACTICAL CONTRIBUTION	97

LIMITATIONS..... 99

CONCLUSION AND FUTURE WORK..... 100

REFERENCES..... 101

APPENDIX A: COVER LETTER..... 115

APPENDIX B: SURVEY INSTRUMENT 116

LIST OF TABLES

Table 1: Empirical studies of ISA.....	12
Table 2: Empirical studies based on TRA/TPB.....	17
Table 3: General Deterrence Theory studies.....	22
Table 4: Protection Motivation Theory studies.....	25
Table 5: Technology acceptance model studies.....	28
Table 6: Integration of different theories.....	30
Table 7: ISPAM constructs name, description, and resources.....	47
Table 8: Constructs items number and source.....	61
Table 9: Constructs and measurement model evaluation.....	67
Table 10: Sample data description statistics.....	72
Table 11: PLS-SEM systematic evaluation.....	74
Table 12: Cronbach's alpha, CR, AVE.....	77
Table 13: Measurement items loadings and reflective construct's AVE.....	78
Table 14: Cross loadings analysis.....	79
Table 15: Fornell-Larcker evaluation.....	80
Table 16: Formatively developed constructs and global item.....	82
Table 17: Path coefficient for formative convergent validity.....	83
Table 18: Collinearity analysis.....	84
Table 19: Outer weight and outer loadings values for formative indicators.....	85
Table 20: Path significance and coefficient.....	87
Table 21: Coefficient of determination.....	88
Table 22: Total effects.....	88

LIST OF FIGURES

Figure 1: Taxonomy of information security research approaches.....	40
Figure 2: Theory of Reasoned Action/Theory Planned Behavior (TRA/TPB).....	41
Figure 3: First three constructs of causal chain model.....	43
Figure 4: Research model- ISP Awareness (ISPAM).....	47
Figure 5: Significance and relevance assessment of formative indicators.....	85
Figure 6: Structural model evaluation.....	89

CHAPTER 1

CHAPTER ONE: INTRODUCTION

Background and Motivation

With the global proliferation of computerized information systems, organizations, akin to large organizations, use information systems as an essential tool to automate their tasks and distribute their products and services. The Adoption information systems enhances the ability of organizations to compete with their rivals, improve productivity, and in effort and time saving. This movement toward the interconnected information world, which includes a vast amount of knowledge sharing and online transactions between individuals and organization, highlights the importance of cybersecurity as a serious issue to keep organizational systems safe from cyber-attacks (Cavusoglu, Mishra, & Raghunathan, 2004b). It is crucial for organizations to protect their customers' sensitive data like healthcare information, credit card data, annual strategic plans information, and financial information (Beachboard et al., 2008; Brancheau, Janz, and Wetherbe, 1996; Gurkok, 2014; Ransbotham and Mitra, 2009).

To protect information systems, organizations are considering the implementation of several technical solutions, such as anti-virus setups, penetration testing, prevention and detection tools, and firewall management. However, relying on technical solutions only is not enough to mitigate information security risks, as there is an increasing need to non-technical users to perform the security related behavior (M. T. Siponen, 2005). Therefore, organizations are required to invest in both technical solutions along with the human factor (employees) that plays a significant role in any information security program (Gurpreet Dhillon & Backhouse, 2001; M. T. Siponen, 2005; D W Straub, 1990). The human factor represents the employees (insiders) who use the information systems and other technology resources in their day-to-day operations. Employees are expected to have certain levels of information security skills and awareness to prevent potential security breaches and mitigate cybersecurity threats associated with information systems. In this context, Warkentin and Willison (2009) correlate the lack of security skills and information security awareness with cybersecurity risks that threaten the confidentiality, integrity, or availability of information systems. They argue that the greatest

threat to information security are insiders(who are they employees working inside the organizations) not external hackers.

In order for organizations to discipline the usage of their employees to information systems, they have to develop information security policies along with acceptable use policies that meet their information security objectives (Höne & Eloff, 2002; NIST SP 800-100, 2006; Peltier, 2002). Employees have to use information systems in terms of information security practices and regulations to effectively use information systems (Goel and Chengalur-Smith, 2010). Developing information security policy is one of the essential measures that any cybersecurity programs should consider. Nevertheless, having well-developed information security policy is worthless if employees are not become aware of it and do not comply with its instructions. Thus, organizations need to consider employees' awareness of their information security policy that helps to reduce ISP violations and result in cutting the cost of information security (Chen, Shaw, & Yang, 2006; D'Arcy, Hovav, & Galletta, 2009). Several empirical research studies have investigated the role of information security awareness and ISP awareness on the attitude toward ISP compliance, intention to comply, and actual compliance with ISP (Bulgurcu, Cavusoglu, & Benbasat, 2008, 2010a; D'Arcy et al., 2009; T Dinev & Hu, 2007; Tamara Dinev, Goo, Hu, & Nam, 2009; Pahnla et al., 2007).

There are two motivational approaches of human behavior; the command-and-control approach and the self-regulatory approach (Tyler & Blader, 2005). The command-and-control approach represents the extrinsic motivational models where external effects influence individuals' behavior. The self-regulatory approach represents the intrinsic motivational models where the connatural drivers affect the behavior of individuals (Tyler & Blader, 2005). In comparing both approaches, intrinsic motivational models has better effects on individuals' behavior than the extrinsic motivational model (Son, 2011). Most of the prior studies have relied only on one approach; the command-and-control approach or the self-regulatory approach. Using only one of the approaches highlights the point of involving both approaches in one model. To address this gap, the researcher combines both approaches to investigate the antecedents of the information security policy awareness.

The literature analysis highlights the significant role of information security awareness and specifically ISP awareness in influencing ISP compliance (Al-Omari, El-Gayar, & Deokar, 2012; Bulgurcu et al., 2010a; D'Arcy et al., 2009). Improving ISP awareness leads to improve

employees' compliance with information security policies, mitigate systems mistakes, and enhance systems use (Bulgurcu et al., 2010a; Kirsch & Boss, 2007; M. Siponen, Pahlila, & Mahmood, 2007). Since ISP awareness is critical in any cybersecurity program, understanding the factors that affect the awareness is necessary to improve the ISP awareness in organizations which impact the overall security. Drawing on ISP awareness definition from Bulgurcu et al. (2010a), the researcher of the current study defines ISP awareness as the overall knowledge and understanding of the information security policy requirements prescribed in organization's ISP.

Problem of Study

An extensive literature review has shown a lack of empirical investigations of the drivers of information security awareness, particularly ISP awareness. Most of the previous research efforts rely on a conceptual analysis as a research method to discuss the role of information security awareness and the factors impacting it. Therefore, a next step is required to conduct more empirical studies to highlight the role of information security and to understand the factors affecting ISP awareness. Furthermore, prior studies focus more on the impact of ISP awareness on information security behavior. However, there are no empirical studies address the antecedents of ISP awareness. Therefore, the current study will be the first to address this gap, which will be the starting point toward a comprehensive understanding of the antecedents of ISP awareness.

Finally, the literature addresses the impact of ISP awareness on different behavioral aspects including; attitude toward ISP compliance (Bulgurcu et al. 2010a), intention to comply with ISP or systems abuses intention (D'Arcy & Hovav, 2009; D'Arcy et al., 2009; Hovav & D'Arcy, 2012), actual behavior (computer abuse or actual compliance) (Humaidi, 2016; S. M. Lee, Lee, & Yoo, 2004), perceptions and beliefs (Al-Omari et al. 2012), and ISA (Bulgurcu et al., 2010a; Haeussinger & Kranz, 2013), but none of the previous studies addressed the influence of ISP awareness on employees satisfaction with ISPs. Therefore, the current study aims to address this gap by investigating the relationship between ISP awareness and satisfaction. Addressing the relationship between ISP awareness and satisfaction provides a starting point toward including satisfaction aspect in information security behavioral domain. In this regard, Herath and Rao (2009b) argue that employees are less likely to comply with their organization's ISP if they think that ISP compliance will create difficulties for their day to day

job activities. Thus, it is important to consider the satisfaction aspect of information security behavior, which results in viewing ISP compliance as a beneficial factor instead of obstacles to work in the eyes of employees.

Research Questions

In this study, the researcher aims to fill the research gaps discussed in the previous section. The proposed research model addresses the first and second gaps by identifying the drivers of ISP awareness involving both approaches; the command-and-control approach and the self-regulatory approach. The researcher addresses the third gap by investigating the direct influence of information security awareness on employees' satisfaction with ISP and security practices and ISP and the indirect influence through the perceived usefulness of protection. Drawing on the innovation diffusion theory (IDT) (Everett M. Rogers, 2003; Everette M Rogers, 1995), ISP awareness model (ISPAM) is proposed. ISPAM will help explain employees' awareness level about their organization's ISP in two directions: the antecedents of ISP awareness and how it will impact their satisfaction of ISPs. In particular, the researcher examines the antecedent factors in two folds: organizational and individual enablers. Organizational enablers consist of ISP fairness and ISP quality. Individual enablers comprise of self-efficacy, and technology awareness. The research mainly aims to answer the following research questions:

1. What are the enablers that drive employees' awareness of ISP?
2. What is the role of ISP awareness in shaping the perceived usefulness of ISP and how it influences the satisfaction with ISP and security practices?
3. Does ISP awareness have a direct influence on the satisfaction with ISP and security practices?

Significance and Contributions

In the organizational environment, information systems play an essential role in achieving organizations' goals and performing its tasks. The current study aims to highlight the employee's ISP awareness and the influence on his/her satisfaction with security practices in terms of ISP compliance. The findings of this study will assist the senior management to

understand the factors that affect employees' ISP awareness, which in turn impact their information security behavior and reduce ISP violations. Reducing ISP violations and encouraging proper security behavior, lead to reduce the security cost. The results will be very helpful in developing high-quality ISPs in terms of clarity, completeness, and consistency. The study findings recommend to consider employees' self-efficacy in cybersecurity programs and encourage them to learn more about information security which impacts their ISP understanding and leads to proper cybersecurity behavior. The study provides an empirical evidence of the practical effectiveness of ISP quality, self-efficacy, technology awareness, and ISP awareness. Extracting such information is helpful for practitioners since empirical evidences provide more credible results than unempirical evidences.

With regards to theoretical foundations, the findings of current study contribute to the theoretical knowledge in information security awareness domain, and will also point out the role of ISP awareness as an influential factor in information security behavior. This study will create a new model, information security policy awareness model (ISPAM), that explains the antecedents of ISP awareness and the impact of ISP awareness on satisfaction with ISP and other security practices. The field of information security awareness lacks studies that address information security awareness and ISP awareness and their role in human behavior. This study will contribute to the theoretical knowledge using the innovation diffusion theory as a new theoretical foundation to be used in information security behavioral domain. Furthermore, this study will be the starting point toward applying different theories to understand the ISP awareness antecedents.

Organization of the Dissertation

This dissertation is structured as follows. Chapter two presents a thorough analysis of relevant literature and points out the contributions of the current study. Chapter three explains the theoretical foundations of the study and discusses the proposed research model and the research hypotheses. Chapter fourth presents the research methodology used to evaluate the research model. Chapter five discusses the analysis results of the empirical analysis including measurement model and structural model evaluations. Finally, chapter six discusses the findings of the study and concludes the dissertation.

CHAPTER 2

CHAPTER TWO: LITERATURE REVIEW

This chapter presents a systematic literature review of the information security behavior and awareness domain with relevance to the proposed research. Chapter two starts with an overview of the general approaches to information systems security. ISP awareness is discussed as an essential part of information security programs and how it affects different behavioral aspects. Then, the chapter discusses the theoretical premises and the various approaches related to information security behavior and awareness research. Finally, gaps in the literature are highlighted to support the current study.

Information Security Overview

The National Institute of Standards and Technology (NIST) refers to information security as the procedures and techniques that are used to protect organizational information assets to provide confidentiality, integrity, and availability of information systems (IS). NIST explains that information security mission is to prevent unauthorized access to organization's data, data leakage, data modifications, and data destruction (NIST SP 800-53 rev4, 2013). Anderson (2003) discusses different definitions of information security that address confidentiality, integrity, and availability (CIA). He concludes that information security is "a well-informed sense of assurance that information risks and controls are in the balance". Peltier (2010) points out that information security covers physical and logical data access controls to protect organizational data from unauthorized access and prohibit accidental or intentional data destruction, damage, modification, leakage, or loss.

Pfleeger and Pfleeger (2006) argue that information security is all about ensuring the three top security basics: confidentiality, integrity, and availability. There are several research articles, conferences, and books that adopt the definition of information security where they center around addressing the main principles of information security, which include:

confidentiality, integrity, and availability (McCumber, 2005, 2007; Stewart, Chapple, & Gibson, 2012). According to McCumber (2007), confidentiality of information means that information should be accessible only to people who have access privileges to organizational data at the time they need. He also defines integrity as information being complete, accurate, robust, and not illegally modified, while he states that availability means that the information is available for people at the time when they need it (McCumber, 2007). Other perspectives of information security focus on information security behavior. In the context of behavior, information security addresses the human actions (behavior) and their impact on the confidentiality, integrity, and availability of information systems (Abraham, 2011; Stanton, Stam, Guzman, & Caledra, 2003). The study at hands focuses on information security behavior.

Information Security Approaches

There are several studies of IS security that address different topics, such as security planning and risk management (Detmar W Straub & Welke, 1998) and information security policy design and development (Doherty & Fulford, 2006; M. Siponen & Iivari, 2006). Organizations use to adopt several strategies to ensure systems security at different phases, including deterrence, prevention, detection, and recovery (D'Arcy et al., 2009; Detmar W Straub & Welke, 1998). Straub and Welke (1998) call these security phases as security action cycle. Within this cycle, security professionals aim to increase the number of deterred and prevented illegal actions and reduce those related to detection and recovery (Theoharidou, Kokolakis, & Karyda, 2005). In other words, security professionals need to deter and prevent cybersecurity accidents before they occur.

Siponen (2005) discusses the traditional security methods used to secure organizational information assets. The conventional methods include: IS security checklists, IS security standards, IS security maturity criteria, and risk management. IS security checklist creates a list of information security controls and solutions that security practitioners can utilize as a security solution (Baskerville, 1993). IS security standards represent the best security practices, activities, actions, rules, or regulations designed to support the information security goals (Peltier, 2002). IS security maturity criteria represents the scales of information security maturity (M. T. Siponen, 2005). Risk management represents the management process and assessments of the security risks and security controls (M. T. Siponen, 2005).

Information security consists of two components: technology-based solutions and human beings. It is important for people to use information systems properly (Aytes & Connolly, 2004). In this regard, several research studies discuss the human perspective and their behaviors of information security. Neumann (1999) referred to the human beings as the employees (insiders) who have access privileges on computer systems. Some studies discuss the challenges in the organizational environment result from their employees' mistakes, abuses, ignorance, or any deliberate illegal use (Durgin, 2007; J. Lee & Lee, 2002; S. M. Lee et al., 2004).

With regards to insiders' behavior, a classification study investigates different approaches to information security behavior (Siponen, 2000b). Siponen (2000b) classifies the approaches into two types. The first category includes the approaches that use motivation perspectives (Non-punishment) to affect users' security behavior in order to reduce their misuses. Motivation perspectives include different means to influence users' behavior such as increasing the users' motivation to use information systems correctly and instruct users about security rules and guidelines to protect information systems. The second type includes those approaches that introduce punishment strategies as an external deterrence to reduce IS misuses (Siponen, 2000b). Information security awareness, the main focus of this dissertation, belongs to the non-punishment approach (Siponen, 2000b).

Information Security Policy Awareness

Nowadays, the increasing dependency on information systems highlights the importance of building effective cybersecurity programs. Effective cybersecurity programs should include the implementation of information security policy. ISP implementation is an essential component to secure informational assets by guiding employees toward proper security behavior. ISP represents a high level statement of guidelines, rules, principles, and protocols documented and used to assist organizations in instructing their employees of what to do and not to do regarding information systems (Bulgurcu et al., 2010a; D'Arcy et al., 2009; Peltier, 2002; Siponen, 2000a). According to NIST, ISP is "an aggregate of directives, rules, and practices that describe how an organization manages, protects, and distributes information" (NIST SP 800-100, 2006). Security people aim to motivate employees to comply with ISP and follow its security instructions (Siponen, 2000a). ISP compliance is becoming a more serious

issue as it instructs non-technical users to perform a proper security related behavior (Anderson & Agarwal, 2010; Bulgurcu et al., 2010a; Johnston & Warkentin, 2010). Information security awareness (ISA) is the integral component to ISPs to ensure the security of the informational assets by increasing the awareness of their security goals, rules, and guidelines as prescribed in the information security policy (H. H. Cavusoglu & Raghunathan, 2004; H. Cavusoglu, Mishra, & Raghunathan, 2004a).

The National Institute of Standards and Technology (NIST) defines ISA programs as a “blended solution of activities that promote security, establish accountability, and inform the workforce of security news and issues” (NIST SP 800-100, 2006). A research article describes ISA as the general knowledge about information security general matters that is built from life experiences and personal interests (Bulgurcu et al., 2010a). Siponen (2001) presents the five dimensions of information security awareness, namely “organizational, general-public, socio-political, computer ethical, and institutional education dimensions.” The organizational dimension asserts the significance role of information security awareness on organizations’ security levels.

Regarding ISP awareness, two approaches define ISP awareness. The first approach describes ISP awareness as the state where the employee is aware of the existence of ISPs in their organization or not (D’Arcy et al., 2009). This description does not consider the level of awareness employees have; it only assumes that the employee who has ISP awareness is aware of every aspect of the policy or not aware at all. However, an employee may be aware of some aspects of ISP but not others aspects which may lead to increase cybersecurity vulnerabilities. In other words, this definition of ISP awareness does not consider how much knowledge of ISP content an employee has. For instance, if employees are aware of changing passwords policy but not aware of anti-virus or using illegal software policies, he/she is considered to has a full awareness of ISP.

The second approach describes ISP awareness as the level of knowledge and understanding an employee has about his organization’s ISP and its requirements (Bulgurcu et al., 2010a; Siponen, 2000a). The study in hands indicates that employees vary widely in their ISP awareness levels based on their understanding of the ISP and the related threats of cybersecurity. Thus, there is a need to understand the factors impacting ISP awareness in order to improve employees’ ISP awareness (Siponen, 2000a). In this regard, Rezgui and Marks

(2008) conduct a case study to explore the factors that impact information security awareness of employees in higher education institutions. The study concludes that conscientiousness, cultural assumptions and beliefs, and social conditions influence employees' behavior, attitude, and awareness of information security. However, their study does not provide an evidence of the effectiveness of these factors.

ISP awareness investigations are necessary in information security domain and ISP compliance for several reasons. First, ISP awareness is found to have an essential impact on employees behavior when it comes to information security and ISP compliance (Bulgurcu et al., 2010a; D'Arcy et al., 2009; Siponen, 2000a). Second, without ISP awareness, information security policy will lose its real usefulness on information security toward preventing security breaches and increase ISP violations (Ceraolo, 1996; Goodhue & Straub, 1991; Hoffer & Straub, Jr., 1989; Detmar W Straub & Welke, 1998). Therefore, ISP awareness is recommended to explain the importance of ISP compliance and persuade individuals to comply with ISP rules and instructions (Maddux, James E.; Rogers, 1983; M. T. Siponen, 2000a).

In this regard, Furnell et al. (1996) found that information security awareness plays a significance role in promoting cybersecurity standards and guidelines. They assert that employees in organizations should be aware of the disciplinary actions (i.e. sanctions) of ISP violations. Denning (2000) discusses the importance of ISP awareness as a significant factor in defending IS security and motivating proper IS behavior. Barman (2001) states that information security officers should consider the awareness of ISPs when writing information security policy by involving employees in ISPs development. Murray (1991) states that ISP awareness is the solution to make employees accurately estimate the dangers and threats of ISP violations. Other research articles and security books confirm that organizations should focus on increasing their employees' ISP awareness by means, such as introducing security policy to employees to ensure that strong deterrents are in place (Banerjee, Cronan, & Jones, 1998; Kovacish & Halibozek, 2003; Martins & Eloff, 2002; Murray, 1991).

In summary, ISP development and ISP awareness play a significance role in cybersecurity programs. Without following ISP instructions and guidelines, ISP development becomes worthless. ISP awareness is considered an essential factor in impacting employees' behavior toward ISP compliance and information security behavior in general. Thus, it is

important to understand the factors of ISP awareness and its impact on beliefs and behavior relating to cybersecurity.

The role of information security awareness is attracting scientific researcher to investigate its impact on individuals' behavior in information security. Information security awareness, and particularly ISP awareness, has significant impacts on different behavioral aspects of information security behavior, such as attitude toward ISP compliance, intention to comply with ISP, actual behavior (actual ISP compliance), and other beliefs. However, there is a lack of empirical investigations to study the role of ISP awareness and its antecedents. In this section, the researcher discusses the implementation of ISA and ISP awareness in information security behavioral research.

Bulgurcu et al. (2010a) report that information security awareness, which is shaped by general ISA and ISP awareness, has a significance impact on employees' outcome beliefs and their attitude toward compliance. The authors confirm previous research results where ISA is found to be a significance predictor of employees' attitude toward ISP compliance (Bulgurcu, Cavusoglu, & Benbasat, 2009a).

Bulgurcu, Cavusoglu, & Benbasat (2009b) utilize the theory of planned behavior to examine the factors that lead employees to comply with the information security policy provided by their organization. The study reports that information security awareness and employees perceived fairness of the ISP, provided by their organization, influence the attitude of employees toward ISP compliance. With regard to using protective technologies, technology awareness is found to be efficient and influences the attitude toward using protective technologies and lead to increase the intention of employees to use the protective technology (T Dinev & Hu, 2007; Tamara Dinev et al., 2009).

Information security awareness and ISP awareness play a significant role when integrated into the general deterrence theory. D'Arcy et al. (2009) point out that information security awareness of security countermeasure, including security policy awareness, affects the perceived severity and certainty of organizational sanctions correlated with security violations and IS misuses. Increasing the perceptions of sanctions, including severity and certainty of sanctions, leads to reduce the number users' misuses and ISP violations. Table 1 summarizes the studies that address the role of information security awareness or ISP awareness in impacting different behavioral aspects.

Table 1: Empirical studies of ISA.

Independent variable	Dependent variable	Findings	Authors
ISP awareness and general ISA	Attitude toward ISP compliance and outcome beliefs	ISA has a significant impact on attitude toward compliance	(Bulgurcu et al., 2010a)
Information Security Awareness ISA	Attitude toward ISP compliance and outcome beliefs	ISA has a significant impact on attitude toward compliance	(Bulgurcu et al., 2009a)
ISA and ISP fairness	Attitude and intention to comply	ISA and ISP fairness have a significance impact on attitude and intention to comply	(Bulgurcu et al., 2009b)
Technology awareness	Attitude and intention toward using protective technologies	Technology awareness has a significance impact on attitude and intention toward using protective technologies	(T Dinev & Hu, 2007; Tamara Dinev et al., 2009)
User awareness of security countermeasures, such as ISP, education and training programs	Perceived certainty and severity of sanctions and user's intention to IS misuse	User awareness of security countermeasures affects their perceived certainty and severity of sanction and users' intention to IS misuse	(D'Arcy et al., 2009)

ISA- Information Security Awareness

Information Security Behavioral Approaches

Organizations are highly relying on information systems. Consequently, they need to develop technical and non-technical measures to mitigate information security threats (Aurigemma & Panko, 2012). The related literature reports that employees (insiders) are the weakest link in information security (M. Siponen & Iivari, 2006; Spears & Barki, 2010). Therefore, employees' behavior is attracting scientific researchers to explore and understand the proper behavior of using information systems with regard to information security and ISP compliance. Information security behavior represents individual actions and activities that impact the main security principles: confidentiality, integrity, and availability (Stanton et al., 2003).

ISP development and ISP awareness are some of the non-technical measures used to protect information systems (Bulgurcu et al., 2010a; D'Arcy et al., 2009; Pahnla et al., 2007; Rezgui & Marks, 2008; M. Siponen et al., 2007; M. T. Siponen, 2000a). ISP development is worthless if the employees do not comply with its rules and guidelines. Thus, enhancing the information security awareness of employees is essential in protecting information assets in organizations (Chen et al., 2006). Particularly, increasing the information security awareness levels about the security practices and information security policy in the organizations (Bulgurcu et al., 2010a; D'Arcy et al., 2009). In order to predict and understand employees' security behavior, the literature utilizes different theories from social psychology and criminology domains that explain the factors impacting individual behavior.

Particularly, there are four different theories that frequently used in information security domain (D'Arcy et al., 2009). These theories are: Theory of Reasoned Action/ Theory of Planned Behavior (TRA/TPB) (Ajzen, 1991), General Deterrence Theory (GDT) (Gibbs, 1975), Protection Motivation Theory (PMT) (Maddux, James E.; Rogers, 1983; Maddux J.E & R.W, 1983), and Technology Acceptance Model (TAM) (F. Davis, Bagozzi, & Warshaw, 1989). In fact, these behavioral theories are widely used in information systems domain in general not only the information security research. The following sections explain and summarize the premises of the four theories in prior research and the role of information security awareness.

Theory Based Literature Review

Theory of Reasoned Action/ Theory of Planned Behavior (TRA/TPB)

The Theory of Reasoned Action (TRA) is introduced by Fishbein & Ajzen in (1975). The main premise of TRA is to predict the intention of the individual to behave. According to TRA, attitude toward behavior and subjective norms are the two most important constructs that have a significance impact on the intention to behave construct. In 1991, Ajzen extended the TRA theory to include “perceived behavioral control” as a third construct to shape the intention. The new extended theory called the Theory of Planned Behavior (Ajzen, 1991). Both theories, TRA/TPB, assume that “intention to behave” is the immediate antecedent of the correspondent action (actual behavior). In the context of information security, employees’ evaluation of the compliance related behavior and their normative beliefs impact their intention toward complying with ISPs. Higher intention to comply results in greater likeability to take the action of compliance (Aurigemma & Panko, 2012; Bulgurcu et al., 2010a; Lebek, Uffen, Neumann, Hohler, & H. Breitner, 2014).

Several research articles have utilized TRA/TPB as a theoretical foundation to explain the information security behavior. Bulgurcu et al. (2010a) utilize the Theory of Planned Behavior along with normative beliefs and self-efficacy to build their research model, which explains how the attitude toward behavior along with normative beliefs and self-efficacy impact the employee intention to comply with ISPs. Based on that, the authors posit that attitude toward compliance is affected by both: the beliefs of the overall assessment of the compliance or non-compliance consequences and the information security awareness. Regarding the evaluation of beliefs, the authors state that it includes the benefit of compliance, the cost of compliance, and cost of non-compliance. With regards to information security awareness, they report that ISA is constructed by two factors, general ISA and ISP awareness. Bulgurcu et al. (2010a) test their model using a sample of 464 employees. Their model assessments conclude that attitude, normative beliefs, and self-efficacy have a significant impact on employees’ intention to comply with the ISP. Furthermore, they find that information security awareness has a significance impact on the attitude toward ISP compliance. The authors confirm the results of a previous study where information security awareness has been found to have a significance impact on the attitude and the outcome beliefs (Bulgurcu et al., 2009a).

Bulgurcu, Cavusoglu, and Benbasat (2009b) use TBP to investigate the factors that lead employees to comply with the information security policy. Their study concludes that information security awareness along with the perceived fairness of the ISP play a significant role in shaping employees attitude toward ISP compliance, and in turn, the attitude positively influences the intention to comply with ISP. Dinev and Hu (2007) develop a research model inspired by TPB and TAM to understand the factor that influences the intention to use protective technology. The researchers test their proposed model using a sample of 332 of IS professionals and students. The study findings show that employees technology awareness positively impact their confidence of using protective technologies and enhance their beliefs of having the necessary competence and skills. The study also finds that the factors extracted from TAM have no impact on the intention of employees to use protective technologies. Furthermore, the results show that self-efficacy is not a predictor of the intention to use the protective technologies.

Drawing upon the Theory of Planned Behavior and the Protection Motivation Theory, Ifinedo (2012) proposes a research model to explain the ISP compliance intention. He employs a sample of 124 business managers and IS professionals to assess the proposed model. The analysis reports that the factors from the TPB, such as attitude and subjective norms, have significantly impacted the intention toward ISP compliance. The TPB factors show more influence on the intention to comply with ISP than the PMT factors where one PMT factor only has a significance impact. The study shows the powerful capabilities of the TPB in predicting the intention to comply with ISP. Another study makes use of the social bonding theory and the social cognitive theory along with the TPB theory (Ifinedo, 2014). The study argues that researchers can utilize various theories to explain information security behavior. The author involves the influences of socialization and group influence from the social bonding theory and personal beliefs, self-efficacy, and cognition from the social cognitive theory on individuals attitude and intention toward ISP compliance from the TPB (Ifinedo, 2014). The analysis results report that social bonds in work environment largely impact attitudes toward ISP compliance. The results also report that the factors of the social cognitive theory, including locus of control and self-efficacy, along with subjective norms and attitude have a significant impact on employees intention to comply with ISP (Ifinedo, 2014).

Limayem and Hirt (2003) extend the TPB theory by adding subconscious (automatic) factors called habits. Habits indicate the automatically inculcated responses and non-deliberate

actions that users bring to IS usage. The study provides a validating idea that subconscious (habits) factors are influential of the intention of individuals to behave in a specific IS usage and their actual behavior.

In an attempt to understand the impact of top management in ISP compliance behavior, Hu, Dinev, Hart, and Cooke (2012) integrate the Theory of Planned Behavior with the role of top management and organizational culture. The model is tested using a sample of 148 of the alumni from MIS and MBA programs in large public school in the US. The analysis results report that top management participation in information security program has a direct and significant impact on the attitude, subjective norm of security, and intention of individuals to comply with ISP. Furthermore, their study discusses that top management has a significant impact on the organizational culture which in turn influences the attitude of employees toward ISP compliance.

Zhang, Reithel, and Li (2009) integrate the Risk Compensation Theory into the Theory of Planned Behavior to examine the factors affecting the security behavior of individuals, specifically, ISP compliance behavior. Risk Compensation Theory addresses the relationship between cautious behaviors and the protection level. The theory argues that individuals are expected to have less cautious behaviors when they have more protective measures, such as safety belts, driving helmets, or anti-lock braking systems (Peltzman, 1975; Sagberg, Fosser, & Saerermo, 1997). In the context of information security behavior, employees who think that their organization has advanced security technologies and security professionals will be less cautious which leads to ISP violations (Zhang et al., 2009). Thus, the proposed model combines perceived technical security protection into the TPB to investigate the role of technical security protection on the behavior of individuals toward ISP compliance. The empirical evaluation of a sample of 176 computer end-users reveals that perceived technical security protection has significant indirect (through perceived behavioral control) and direct impact on the intention to comply with ISP. The results confirm the strong effects of attitude toward ISP compliance and the intention to comply with ISP.

Table 2: Empirical studies based on TRA/TPB

Independent variable	Dependent variable	Findings	Theories	Authors
Attitude, self-efficacy, normative beliefs, and ISA	Intention to comply	ISA, attitude, self-efficacy, and normative beliefs have a significance impact on intention to comply.	TPB	(Bulgurcu et al., 2010a)
ISA, outcome beliefs, and attitude	Intention to comply	ISA, attitude, and normative beliefs have a significance impact on intention to comply.	TPB	(Bulgurcu et al., 2009a)
ISA and ISP fairness	Attitude and Intention to comply	ISA and ISP fairness have a significant impact on employees' attitude and intention to comply.	TPB	(Bulgurcu et al., 2009b)
Technology awareness, PU, PEOU, SE, Controllability	Attitude and intention to use protective technologies	Technology awareness has a significance impact on attitude and intention to use protective technologies.	TPB, TAM	(T Dinev & Hu, 2007)
Attitude, SN, SE, Perceived vulnerability, response efficacy	Intention toward ISP compliance	TPB's factors have significantly more impact on employees' intention to comply that PMT's factors.	TPB, PMT	(Ifinedo, 2012)
Social bonds, locus of control, self-efficacy, SN, and Attitude	Intention toward ISP compliance	Along with TPB, Social Bonding theory and social cognitive theory explain employees'	TPB, SBT, SCT	(Ifinedo, 2014)

		intention to comply with ISP.		
Habit, Affect, Perceived Consequences, Social Factors, Facilitating condition	Intention to behave and Actual behavior	The study provides a validating idea that subconscious (habits) factors are influential of the individual's intention to behave and actual behavior.	TPB	(Limayem & Hirt, 2003)
Top management, organizational culture	Attitude and intention toward ISP compliance	Senior management has a significant impact on individuals' beliefs toward ISP compliance.	TPB	(Hu et al., 2012)
Perceived security protection mechanism, PBC, attitude, and SN	Intention toward ISP compliance	perceived technical security protection has significant indirect (through perceived behavioral control) and direct impact on employees' intention to comply with ISP.	TPB and risk compensation theory	(Zhang et al., 2009)
Attitude, social influence, and perceived behavioral control	Intention to adopt anti-spyware software	attitude toward adopting anti-spyware, social influence, and perceived behavioral control affect users' intention to use anti-spyware software.	TPB	(Younghwa & Kozar, 2005)

ISA- Information Security Awareness, TPB- Theory of Planned Behavior, TAM-Technology Acceptance Model, PU- Perceived Usefulness, PEOU-Perceived Ease of Use, SN-Subjective Norms, SE-Self Efficacy, PMT-Protection Motivation Theory, PBC- Perceived Behavioral Control

Based on TPB, Younghwa and Kozar (2005) develop a research model which examines the factors affecting Internet users behavior toward adopting the anti-spyware software. The study objective is to provide a better understanding of the intention to use anti-spyware software. A sample data of 212 internet users is collected. The empirical analysis finds that attitude toward adopting anti-spyware, social influence, and perceived behavioral control affect the intention of internet users to make a decision to use anti-spyware software. Table 2 presents a summary of the independent and dependent variables used in the studies that utilized TRA/TBP as the backbone for their research models.

General Deterrence Theory

The General Deterrence Theory (GDT) is used in many studies as theoretical bases to examine the effectiveness of different security countermeasures. GDT is theoretically rooted in criminal justice research domain (Gibbs, 1975). The rationale of GDT is that security procedures and countermeasures represent the deterrent fence by leveraging the perceptions of the certainty and severity of punishment for security violations which result in reducing security incidences of improper behavior (D'Arcy et al., 2009). In other words, GDT assumes that the decision to engage in a crime or violate the rules is influenced by three factors: perceived severity of sanctions, perceived certainty of sanctions, and punishment. In information security behavioral research, several research articles utilize GDT as a premise to explain the behavior of information systems users.

D'Arcy et al. (2009) take advantage of the General Deterrence Theory to build a research model that explains IS misuse behavior. Their research model integrates GDT with information security awareness. The authors argue that information security countermeasures, such as user awareness of information security policies, security training, security education, and computer monitoring, have a significant impact on perceived certainty and severity of organizational sanctions of ISP violations (D'Arcy et al., 2009). The proposed model is tested with a sample of 269 computer systems users. The findings of the study highlight the significant role of user awareness of ISP, security training, education, and awareness on their sanctions perceptions which result in reducing IS misuses. Furthermore, the study finds that the perception of the severity of sanctions is more influential than the perception of certainty for sanctions.

Hovav and D'Arcy (2012) propose a research model to understand the culture differences impact on the deterrent capabilities of various security countermeasures. Their model and hypothesis are derived from their previous research (D'Arcy et al., 2009). The proposed model categorizes ISPs, and SETA programs into a single construct called procedural countermeasures. The authors tested their model in two different cultures: the US and South Korea. The study provides evidence that the deterrent effects of procedural countermeasures differ between the two cultures. The study proves that the deterrent capabilities in the US are more efficient than in South Korea. This result highlights the importance of considering culture differences when it comes to cybersecurity program development.

Relying on GDT, Kankanhalli, Teo, Tan, and Wei (2003) propose a research model to study security countermeasures role in protecting information resources, such as information systems and sensitive data, from unauthorized access and deliberate IS misuse actions. Particularly, the proposed model examines the impact of deterrent and preventive countermeasures and the organizational factors (top management support, organizational size, and industry type), on IS security effectiveness. For evaluation purposes, the authors collected a sample of 64 IS managers. The analysis results show that top management support has a significant effect on defensive efforts which in result affects cybersecurity effectiveness. Furthermore, the study concludes that enforcing more severe penalties does not completely prevent ISP violations and IS abuses.

Based on GDT, Straub (1990) develops a research model to explain how information security procedures prevent and deter ISP violations and IS abuses. To assess his model, a survey data of 1211 randomly selected managers from different organizations is used. The analysis results highlight the role of preventive and deterrent techniques in reducing ISP violations and IS misuses. The author argues that using preventive security software leads to reduce IS misuses and deterring the potential ISP violations. In another study, GDT is integrated along with other two theories, namely Rational Choice Theory and Individual Propensity Theory, adopted from the criminology discipline (Hu, Xu, Dinev, & Ling, 2010). Their research model aims to provide an understanding of computer systems offenses. The authors tested their model using a survey data of 207 employees working in large Chinese organizations. The study finds that the employee perceived benefits outperform their perceived risks of computer offenses when he/she is planning to act against computer systems. According

to the authors, this benefit-risk assessment mitigates the impact of deterrence on employee intention toward aggressive act.

In the context of ethical perspective, Harrington (1996) have the benefits of the General Deterrence Theory to evaluate the impact of the company generic code of ethics and IS-specific code of ethics on IS abuse judgments and the intention of abusing the computer systems. The findings of the study indicate that IS-specific code of ethics has a significant impact on computer sabotage judgments and the employee intention to abuse computer systems. As compared to IS-specific code of ethics, the company general code of ethics has no impact on the judgment of an employee and his/her intention to abuse computer systems. However, the study finds that general ethics has a significant impact on employees who tend to deny computer abuse responsibility.

Another study integrates GDT with the Social Control Theory to develop a model that addresses computer systems abuses performed by employees (Lee et al., 2004). The authors assume that information security policy, information security awareness programs, and cybersecurity programs have a significant impact on the intention of employees toward systems abuses by acting as deterrent factors. To test the proposed model, the authors collected a survey data of 182 MBA students and company managers in six Korean companies. The study finds that information security policy, information security awareness programs, and cybersecurity programs have a significant impact on self-defense intention and the decision to abuse computer systems.

Dugo (2007) consolidates GDT along with organizational commitment and cultural concepts into TPB to explain the employee intention to violate ISP rules. Particularly, their proposed model aims to provide an explanation of the impact of organizational security culture on employee intention to violate ISP rules and regulations. The empirical analysis of 113 participants in the study survey shows that perceived punishment certainty and perceived punishment severity greatly mitigate the intention to violate ISP. According to (Dugo, 2007), organizational commitment and security culture are not significant predictors of the intention toward ISP violations. Table 3 summarizes the independent variables used as predictors to the dependent variables in studies that used GDT as the main theoretical foundation and the key contribution of each study.

Table 3: General Deterrence Theory studies

Independent variable	Dependent variable	Findings	Theories	Authors
User awareness of ISP, SETA, severity and certainty of sanctions.	Intention toward IS misuse	User awareness of security countermeasures significantly impact their sanctions' perceptions and reduce IS misuse intention	GDT	(D'Arcy et al., 2009)
Procedural countermeasures, technical countermeasures, moral beliefs, age, and gender	Perceived certainty and severity of sanctions, IS misuse intentions.	The deterrent capabilities are varied by culture differences.	GDT	(Hovav & D'Arcy, 2012)
Organizational size, top management support, industry type	Deterrent efforts, deterrent severity, preventive efforts, and IS security effectiveness	IS security effectiveness is highly impacted by deterrent efforts, organizational size, top management support, industry type, and preventive efforts	GDT	(Kankanhalli et al., 2003)
Preventive and deterrents security software	Computer abuse	Effective deterrent and preventive security software result in reducing computer abuses	GDT	(D W Straub, 1990)
LSC, DET, PEB, PIB, PIR, PFR	Intention toward computer offense	Deterrence has less impact on computer offenses intention while rational choice approach has more impact	GDT, RCT, and SCT	(Hu et al., 2010)
General and IS-specific code of	Computer abuse	IS-specific code of ethics has a significant influence on Computer abuse	GDT	(Harrington, 1996)

ethics, denial of responsibility	judgment and intention	judgment and intention, but general ethics have no impact.		
Deterrence factors (perceived certainty and severity of punishment) and organizational commitment and security culture	Intention to violate ISP	Deterrence factors (perceived certainty and severity of punishment) have great impact on mitigating users' intention toward ISP violations	GDT, TPB	(Dugo, 2007)
information security policy, information security awareness programs, security programs, and organizational trust factors	Computer systems abuses	Information security policy, information security awareness programs, and security programs have a significant impact on self-defense intention and computer abuse.	GDT, and social cognitive theory	(S. M. Lee et al., 2004)

GDT- General Deterrence Theory, ISP- Information Security Policy, IS- Information Systems, SETA-Security Education, Training, and Awareness, PEB-Perceived Extrinsic Benefits, PIB- Perceived Intrinsic Benefits, PIR- Perceived Risks of Information Sanctions, PFR- Perceived Risks of Formation Sanctions, LSC-Lower Self Control, DET-Perceived Deterrence, RCT-Rational Choice Theory, SCT-Social Control Theory.

Protection Motivation Theory

The Protection Motivation Theory (PMT) is derived from health psychology domain. The theory explains the protective behaviors to cope with potential threats (Maddux, James; Rogers, 1983; Maddux; & R.W, 1983). With regards to information security, two factors, namely threat appraisal and coping appraisal, have a significant impact on the belief and attitude of employees toward cybersecurity related issues (Bulgurcu et al., 2010a; Bulgurcu, Cavusoglu, & Benbasat, 2010b). Employees with high awareness level (large knowledge and higher

understanding) of the potential cybersecurity threats (risks) form different attitudes toward perception of cybersecurity risks and coping appraisals than employees with low awareness level (C. L. Anderson & Agarwal, 2010; Herath & Rao, 2009a, 2009b; Lebek et al., 2014). PMT focuses more of the protective side which refers to the adoption of protective technologies, such as anti-spyware (Chenoweth, Minch, & Gattiker, 2009).

Although few research studies have addressed the protection motivation theory on its own, different studies have addressed PMT along with other theories in the context of information security behavior. In this section, the researcher focuses on the studies that utilize only PMT. Chenoweth et al. (2009) develop a PMT-based model to understand the factors that impact user intention to use protective technologies, such as antivirus and anti-spyware. The proposed model mainly hypothesizes that threat appraisal and coping appraisal affect behavioral intention through the mediator construct, maladaptive coping. To assess the model, a sample of 204 undergraduate students is used in the analysis process. The findings of the study conclude that perceived vulnerability, perceived severity, response efficacy, and response cost affect user intention to use the anti-spyware software as a protective technology.

Drawing upon PMT, Johnston and Warkentin (2010) propose a behavioral model to investigate the influence of fear appeals on ISP compliance that leads to threat mitigations. The study tested the proposed model using a sample of 275 experienced computer users from different large universities. The analysis findings show that fear appeal impact is inconsistent across all end users. Furthermore, the study concludes that user intention to behave toward ISP compliance is impacted by perceptions of self-efficacy, threat severity, response efficacy, and social influence.

Workman, Bommer, and Straub (2008) use the PMT and the Social Cognitive Theory to articulate and understand why employees who have security training and awareness fail to comply with the instructions and rules included in the ISP. The study particularly aims to understand the gap between knowing and doing. According to the proposed theoretical model, threat assessment and coping assessment are some of the antecedents that impact individual behavior. Their study gathered survey data of 612 participants from large technology organizations to evaluate the model. Their analysis asserts that threat assessment and coping assessment have a significant impact on the individual subjective and objective omissive

behavior. Furthermore, their analysis confirms the strong influence of the Social Cognitive Theory, represented by self-efficacy and locus of control, on user omissive behavior.

Using PMT as the underlying conceptual foundation along with TRA and TPB, Anderson and Agarwal (2010) develop a theoretical model to understand the security behavioral intention of home users who are motivated to implement security countermeasures to secure their home computer and internet. The proposed model mainly hypothesizes that attitude toward security behavior, social influence, and psychological ownership of the relevant object affect home user intention toward security behavior. To evaluate the proposed model, a survey data of 594 home computer users is collected from undergraduate students. The findings of the study indicate that a combination of social, cognitive, and psychological components shape user intention toward security behavior. Onther study uses PMT as a theoretical base to understand the intention of home users toward security behavior (LaRose, Rifon, & Enbody, 2008). To evaluate the research model, a sample of 206 students is collected. The study finds that home user intention toward security behavior is affected by personal responsibility, self-efficacy and response efficacy. The authors argue that emphasizing the user personal responsibility leads to improve safety behavior.

Woon, Tan, and Low (2005) develop a theoretical model, inspired by the Protection Motivation Theory, to determine that factors affecting home user decision to implement security features on their own wireless network. A sample of 189 home users is used to assess the proposed research model. The empirical analysis reveals that perceived severity, response efficacy, self-efficacy, and response cost have a significant impact on the decision of home users to implement specific security measures in a bid to protect their home network. Table four concludes the research studies that used the Protection Motivation Theory as the main theoretical basis.

Table 4: Protection Motivation Theory studies

Independent variable	Dependent variable	Findings	Theories	Authors
Threat appraisal, coping appraisal,	Intention to use	Threat appraisal and coping appraisal have a direct and indirect impact on users'	PMT	(Chenoweth et al., 2009)

and maladaptive coping	protective technology	intention toward using protective technologies.		
Perceived threat severity, perceived threat susceptibility, response efficacy, self-efficacy, and social influence	Intention to comply with ISP	perceptions of self-efficacy, response efficacy, threat severity, and social influence affect users' intention to comply with ISPs	PMT and fear appeal	(Johnston & Warkentin, 2010)
Threat assessment factors and coping assessment factors	Subjective and objective Omissive behavior	Subjective and objective Omissive behavior is influenced by Threat assessment factors and coping assessment factors	PMT and social cognitive theory	(Workman et al., 2008)
Psychological ownership, descriptive norms, concern regarding security threats, attitudes, self-efficacy, SN, and perceived citizen effectiveness	Intention toward security behavior	A combination of social, cognitive, and psychological components shape users' intention toward security behavior	PMT	(C. L. Anderson & Agarwal, 2010)
Personal responsibility, self-efficacy and response efficacy	Intention toward security behavior	home users' intention toward security behavior is affected by personal responsibility, self-efficacy and response efficacy	PMT	(LaRose et al., 2008)
perceived severity, response efficacy, self-	Decision to implement security	perceived severity, response efficacy, self-efficacy, and response cost have a	PMT	(Woon et al., 2005)

efficacy, and response cost	measures on home wireless network	significant impact on home users' decision to implement specific security measures.		
-----------------------------	-----------------------------------	---	--	--

ISP- Information Security Policy, PMT-Protection Motivation Theory

Technology Acceptance Model

Technology Acceptance Model (TAM) is one of the popular behavioral models that explains the antecedent factors impacting users to accept certain technology (F. Davis et al., 1989). Davis et al. (1989) argue that the perceived usefulness and perceived ease of use have a significant impact the individual acceptance to use a certain technology. Perceived usefulness refers to user subjective assessment of the usefulness of certain system and the degree to which the system helps in improving their performance and productivity. While ease of use factor refers to user perception of the extent to which using the system is easy and requires a few efforts (Venkatesh, Morris, Davis, & Davis, 2003).

Using TAM as basic premises, Xue, Liang, and Wu (2011) integrate punishment research and justice theory into TAM model to understand the influence of punishment and perceived justice on user behavior toward ISP compliance. The proposed model is evaluated using a sample of 118 employees in one of the China's top enterprises. The assessment results provide evidence that perceived justice of punishment is a significant impactor of ISP compliance intention. The authors argue that perceived justice of punishment, actual punishment, and punishment expectancy have greater effects on ISP compliance intention than TAM factors, perceived usefulness and perceived ease of use. According to the analysis results, perceived usefulness has no impact on the compliance intention.

Al-Omari, El-Gayar, and Deokar (2012) uses TAM as a theoretical basis to develop a theoretical model that explains ISP compliance intention using the main TAM factors, perceived usefulness and perceived ease of use. The proposed model hypothesizes that information security awareness affects employee perception of usefulness and ease of use which in turn impact employee intention toward ISP compliance. Table five presents a summary of the independent and dependent variables along with the main contribution.

Table 5: Technology acceptance model studies

Independent variable	Dependent variable	Findings	Theories	Authors
perceived justice of punishment, actual punishment, punishment expectancy, perceived usefulness, perceived ease of use, and satisfaction	Compliance intention	perceived justice of punishment, actual punishment, and punishment expectancy have greater effects on ISP compliance intention than TAM's factors and satisfaction	TAM	(Xue et al., 2011)
Subjective norm, self-efficacy, controllability, ISA of ISP, SETA, and information security	Perceived usefulness, perceived ease of use, and ISP compliance intention	Subjective norm, self-efficacy, controllability, and user awareness of ISP and SETA have a significant impact on both Perceived usefulness and perceived ease of use which in turn affect the intention to comply.	TAM	(Al-Omari et al., 2012)

TAM-Technology Acceptance Model, ISA- Information Security Awareness, ISP-Information Security Policy, SETA-Security Education, Training, and Awareness

Theory Integration of the Main Theories: TRA/TPB, GDT, PMT, and TAM

In this section, the researcher discusses prior studies that integrate two or more theories of the four main theories used in information systems security research. In this regard, Pahlila, Siponen, Mahmood, et al. (2007) present a research model based on three theories TRA, GDT, PMT, and other factors from different theories and approaches. The theory of reasoned action is the backbone of the proposed model while GDT and PMT extend the TRA. The analysis results of the study sample (245 company employees) confirm the prediction power of the TRA

where it is found that along with habits, employee attitude and normative beliefs have a significant impact on his/her intention toward ISP compliance. Furthermore, the study shows that information quality has a strong effect on ISP compliance behavior. However, the findings of the study conclude that some factors, such as sanctions and coping appraisal, from GDT and PMT along with rewards have no impact on attitude toward ISP compliance nor on intention to comply.

Siponen et al. (2007) extend the protection motivation theory by integrating GDT and TRA with PMT. The main goal of the extended model is to understand employee adherence to information security policies using well-defined theories, PMT, GDT, and TRA. The proposed model is assessed using a sample of 917 employees from different companies. The study finds that threat appraisal, self-efficacy and response efficacy have a strong influence on ISP compliance intention. Moreover, sanctions have a significant impact on actual ISP compliance (actual behavior). Siponen, Adam Mahmood, and Pahnla (2014) conduct another study that proposes a multi-theory based model to explained employee adherence to organization ISP. The model integrates elements from TRA, PMT, and the Cognitive Evaluation Theory. The multi-theory based model is evaluated using a sample of 669 employees from four companies in Finland. According to the analysis results, the authors report that several factors, such as, perceived severity of potential information security threats, employee belief as to whether they can apply and adhere to information security policies, employee attitude toward complying with information security policies, perceived vulnerability to potential security threats, and social norms toward complying with information security policies, have a significant and positive effect on the intention to comply with information security policies (M. Siponen et al., 2014; M. Siponen, Pahnla, & Mahmood, 2010).

Inspiring from criminology research domain, Siponen and Vance (2010) utilize the neutralization theory to explain the ISP violations of employees. They argue that employees may use one or more neutralization techniques to justify their actions and allow them to minimize the perceived harm of ISP violations. According to authors, the behavior of using neutralization techniques mitigate the impact of the deterring factors derived from GDT, such as sanctions. Their proposed model covers six factors of neutralization, such as defense necessity, appeal to higher loyalties, condemn the condemners, the metaphor of ledger, denial of injury, and deterrence factors including formal and informal sanctions. The empirical results

of the study assert that Neutralization Theory is a significant predictor to explain employee intention toward ISP violations. The analysis results show that the impact neutralization techniques reduce the deterrence effects of deterrent factors (formal and informal sanctions) and make them insignificant.

Table 6: Integration of different theories

Independent variable	Dependent variable	Findings	Theories	Authors
Sanctions, threat appraisal, coping appraisal, normative beliefs, Info. quality, facilitating condition, habits, rewards	Attitude toward compliance, intention to comply, and actual compliance	Negative reinforcement has no impact on the central TRA's factors in the context of ISP compliance while information quality has a significant impact.	TRA, GDT, and PMT	(Pahnila et al., 2007)
Threat appraisal, response efficacy, self-efficacy, and sanctions	Intention to comply and actual compliance	threat appraisal, self-efficacy and response efficacy have a strong influence on intention to comply and sanctions have an impact on actual behavior	TRA, GDT, and PMT	(M. Siponen et al., 2007)
Severity, Vulnerability, Response efficacy, Self-efficacy, attitude, Normative beliefs, and rewards	Intention to comply and actual compliance	Elements from PMT and Cognitive Evaluation Theory have a significant impact on employees' intention to comply and actual compliance.	TRA, PMT, and Cognitive Evaluation Theory	(M. Siponen et al., 2014)

Neutralization factors and deterrent factors	Intention toward ISP violation	Neutralization techniques result in making the impact of deterrent factors insignificant.	Neutralization theory and GDT	(M. Siponen & Vance, 2010)
Organizational commitment, response efficacy, self-efficacy, perceived severity of security breaches, punishment severity, detection certainty	Intention toward ISP violation	Employees are less likely to comply with their organization's ISP if they think that ISP compliance will create difficulties for their day to day job activity	PMT, GDT, and DTPB	(Herath & Rao, 2009b)

TRA- Theory of Reasoned Actions, GDT-General Deterrence Theory, PMT- Protection Motivation Theory, DTPB-Decomposed Theory of Planned Behavior

By integrating several theories, including PMT, GDT, Decomposed Theory of Planned Behavior (DTPB), and organizational behavior, Herath and Rao (2009b) propose a theoretical model to understand the factors affecting ISP compliance intention. Particularly, the model investigates the role of threat appraisal and coping appraisal from PMT and organizational commitment, response efficacy, punishment severity, and detection certainty from GDT. To assess the proposed model, they rely on a sample data of 310 employees. The empirical analysis shows that the employee understanding of the severity of threat has a major impact on their concerns about security breaches. On the other side, the results show that the concerns an employee has about security breaches are not affected by the certainty of security breaches. The authors argue that employees are less likely to comply with ISPs if they think that ISP compliance will create difficulties for their day-to-day job activities. The results also provide an evidence of the important role of resource availability, self-efficacy, and perceived

effectiveness of employee actions on his/her behavior toward ISP compliance. Surprisingly, the empirical results find no impact of attitude toward ISP compliance on the intention of employees to comply with ISPs. Table six summarizes the independent and dependent variables and the main contribution to each study discussed in this section.

User Satisfaction

User satisfaction is one of the most used techniques that assess the information system. In this regard, Ives, Olson, and Baroudi (1983) define user satisfaction as the degree to which the user is satisfied with the information system that provides all the user needs. Another definition of the user satisfaction refers to a positive evaluation of the pleasant user experience of using an information system (Au, Ngai, and Cheng, 2008). In other words, user satisfaction depicts the psychological process that surrounds the experience of using information system and represents it in different levels of satisfaction or dissatisfaction (Au et al., 2008).

Several theories explain user satisfaction as a dependent variable. These theories are the needs theory, the expectation disconfirmation theory, and the equity theory (Au et al., 2008; Montesdioca & Maçada, 2015). The needs theory points out the three basic needs that any user desires to fulfill. The needs of the existence, the relatedness, and the growth (Alderfer, 1969). The existence need relates to physiological needs and material needs. The relatedness needs reflect the relationships with significant others. The growth needs to address the user development and meaningful creativity.

Oliver (1980) develops the expectation disconfirmation theory in the marketing domain. This theory explains the user comparative judgment about what he expected from the product and what he found (the actual performance). In other words, if the user has high expectation of a specific product that does not meet his expectation, the user satisfaction will be lower. On the other side, if the product performance is as expected or better than what is expected, the user satisfaction will be higher (Oliver, 1980). In information systems domain, several research studies use the expectation disconfirmation theory like (Liao, Chen, & Yen, 2007; Venkatesh & Goyal, 2010).

The equity theory is developed by (Adams, 1966). The main idea in this theory is to address user's perception of injustice in work environment that leads to making users (employees) dissatisfied. In other words, the user will be dissatisfied when the ratio of outcomes

to his input is unequal to the ratio of other persons. In information systems domain, several research studies use the Equity Theory like software privacy (Douglas, Cronan, & Behel, 2007; Morton, 2004) and user satisfaction with information systems (Hess & Hightower, 2002; Joshi, 1992).

Literature Gaps and Limitations

The researcher conducted a thorough analysis of the prior studies in the literature that related to the research objectives. The analysis shows that several behavioral theories have been employed to understand the personal attitude and intention toward cybersecurity behavior including ISP compliance, system misuses and abuses, and security measures implementation in a bid to protect information systems. Researchers of the prior studies relied on different behavioral theories to understand the factors affecting the behavior of users in cybersecurity era with focusing only on the four top theories including, TRA/TPB (Ajzen, 1991; Fishbein & Ajzen, 1975), GDT (Gibbs, 1975), PMT, and TAM. One limitation of employing these theories is the single level perspective (Lebek, Uffen, & Breitner, 2013). Each single theory addresses the individual behavioral factors and ignores the fact that other factors are influential too, such as organizational or work-related factors (Kukafka, Johnson, Linfante, & Allegrante, 2003). Ignoring these factors and their effects may result in making these theories inefficient. Therefore, there is still need to study more factors other than the individual behavioral factors. Further, cybersecurity domain relates toward applied sciences. This point advances the importance of theoretical and relevance balance (M. Siponen & Vance, 2013).

The prior research efforts in the past two decades of the cybersecurity behavior have mainly focused on deterrent or motivation models. Such studies based their models on one of the main four theories or combination of them. In all prior research, great effort has been made to understand the antecedent factors that collectively impact the individual behavior related to cybersecurity, specifically, ISP compliance. In almost all studies, an individual's planned decision, in the form of intentions, is considered as the main predictor of the actual behavior. While the literature is full of studies that have contributed to our understanding of many antecedent factors of cybersecurity behavior, more research still needed to address other factors and take advantage of other theoretical foundations. Thus, this study introduces the Innovation Diffusion Theory as a new theoretical foundation to be used in information security behavioral domain (Everette M Rogers, 1995). The main premise of the Innovation Diffusion Theory is

that knowledge or awareness impact the beliefs of individuals, such as attitude or satisfaction, which in turn impact their decisions (Everett M. Rogers, 2003).

While the prior studies have focused either on deterrent factors to impact the behavior or protection motivation factors to encourage desirable cybersecurity behavior, few number of studies have discussed the satisfaction with organization ISP and security practices in general and the factors affecting ISP satisfaction. This study provides a starting point toward considering the satisfaction with the organization ISP, and to highlight the importance of making ISP compliance desirable in the eyes of employees. Herath and Rao (2009b) argue that employees are less likely to comply with their organization ISP if they think that complying with ISP will negatively impact their work performance. Thus, it is important to understand the factors that impact employee satisfaction with the information security policy, which result in viewing ISP compliance as a beneficial instead of obstacles to their work.

Regarding information security awareness and ISP awareness, an extensive literature review has shown a lack of the empirical studies that address the drivers of information security awareness. Most of the previous efforts adopt the conceptual analysis as a research method instead of empirical methods and address the effect of information security awareness on other variables but not the antecedents of the information security awareness itself, and particularly ISP awareness. All prior studies, which involved ISA and ISP awareness, examine its impact on other dependent factors but none of these studies addressed the factors that may impact employees' ISP awareness. Furthermore, prior studies discussed the impact of information security awareness on employees attitude toward ISP compliance (Bulgurcu et al., 2010a), intention to comply with ISP (D'Arcy & Hovav, 2009; D'Arcy et al., 2009; Hovav & D'Arcy, 2012), actual behavior (computer abuse or actual compliance) (S. M. Lee et al., 2004), and perceptions (usefulness), but none of the previous studies addressed its influence on the satisfaction of employees with ISPs.

CHAPTER 3

CHAPTER THREE: RESEARCH MODEL AND HYPOTHESES

In a competitive world, using information systems is not a luxury anymore. It is a necessary component that organizations need to consider in order to be able to compete with their rivals. Using information systems in organizations lead to increase the productivity and save time and effort. However, information systems security risks remain one of the greatest concerns to organizational management. To make sure that information systems are protected, organizations implement technical security solutions like anti-virus and firewall management. Nevertheless, investing in technical solutions only to protect their information systems is not enough (Gurpreet Dhillon & Backhouse, 2001; M. T. Siponen, 2005; D W Straub, 1990), organizations also need to invest in the human factor. The human factor represents the employees who use the information systems and technology resources in organizations. Lack of the employee security skills and having less awareness about cybersecurity increase the risk of information security and threaten the confidentiality, integrity, and availability of information systems (Warkentin & Willison, 2009).

Organizations are encouraged to invest in improving the cybersecurity skills of their employees and involve them in safeguarding (protecting) responsibility of the information systems resources. Preparing well-developed information security policy and acceptable use policy is one of the cybersecurity measures that organizations in these days used to include in their cybersecurity strategies and programs. However, developing information security policy and providing acceptable use policy is worthless if the employees do not become aware of them. Therefore, increasing the information security awareness of employees is essential for organizations to protect their information assets (Chen et al., 2006). In particular, increasing information security awareness levels about the security practices and information security policy in the organizations. Many empirical studies have found a positive relationship of the employee ISA and attitude toward complying with information security policy, intention to comply, and actual compliance (Bulgurcu et al., 2008, 2010a; D'Arcy et al., 2009; Pahnla et al., 2007). Since ISA awareness is critical in any cybersecurity strategy, understanding the

factors that affect the awareness is important too to improve the ISP awareness in an organizational environment.

In this context, there are two motivational approaches of human behavior; the command-and-control approach and the self-regulatory approach (Tyler & Blader, 2005). The command-and-control approach represents the extrinsic motivational models where external effects such as rewards, sanctions, fairness, and quality influence the behavior of individuals. The self-regulatory approach represents the intrinsic motivational models where the connatural drivers such as self-efficacy, personal skills, and knowledge influence the behavior of individuals (Tyler & Blader, 2005). Comparing both approaches, intrinsic motivational models has better effects on the human behavior than the extrinsic motivational model (Son, 2011).

The current study combines both approaches to investigate the antecedents of the information security policy awareness. The antecedents are divided into two categories: organizational drivers, which represent the command-and-control approach and individual drivers, which represent the self-regulatory approach. Organizational drivers, including ISP fairness and ISP quality, are considered the extrinsic factors where the organizational management is responsible for shaping these factors. On the other hand, individual factors, including self-efficacy and technology security awareness, are considered intrinsic factors where they depend on the individuals themselves. Furthermore, the researcher uses, the Innovation Diffusion Theory (Dinev & Hu, 2007; Everette M Rogers, 1995), the Equity Theory (Adams, 1966), and the usefulness construct from technology acceptance model (TAM) (Davis et al., 1989) as the theoretical basis to build the research model.

The proposed research model represents two directions, the antecedents that impact ISP awareness and the effects of ISP awareness on the satisfaction with ISP and security practices. The research model focuses on ISP awareness as the core construct that affects personal satisfaction. Human satisfaction in the model is mapped to the attitude construct as explained in the Theory of Planned Behavior (Ajzen, 1991).

Theoretical Framework

Information Security Awareness

Today's highly networked systems environment highlights the importance of using effective cybersecurity programs. In order to develop strong cybersecurity architecture,

cybersecurity professionals implement information security controls and practices, which are well-known as information security policy. Information security policy is a high-level statement of guidelines, rules, principles, and protocols documented and used to assist organizations in instructing their employees of what to do and not to do regarding information systems to meet cybersecurity goals (Bulgurcu et al., 2010a; D'Arcy et al., 2009; Peltier, 2002; M. T. Siponen, 2000a). NIST has defined information security policy as “an aggregate of directives, rules, and practices that describe how an organization manages, protects, and distributes information” (NIST SP 800-100, 2006). Implementing the perfect information security controls and practices only leave some raised questions. These questions are: is it enough for an information security program to implement only the best security practices? What about the personnel in cybersecurity formula?

An effective information security awareness program is the answer to the above questions. Information security awareness is the complementary component of any information security program to ensure that the critical information assets are protected (H. H. Cavusoglu & Raghunathan, 2004; H. Cavusoglu et al., 2004a). According to the National Institute of Standards and Technology, security awareness program is a “blended solution of activities that promote security, establish accountability, and inform the workforce of security news and issues” (NIST SP 800-100, 2006).

There are different definitions of information security awareness regarding to the context where it is used (general security awareness, information security policy awareness, and education and training awareness). Bulgurcu et al. (2010b) define information security awareness (ISA) as the general knowledge of information security. They state that ISA may be developed from direct life experiences, like penalized for not complying with information security rules, harmed by virus attack, or getting information from a variety of resources such as workshops inside organizations, newspapers, or media. ISA has two dimensions: general information security awareness and ISP awareness (Bulgurcu et al., 2010a). Bulgurcu et al. (2010a) define general information security awareness as the overall knowledge and understanding of the information security issues and their ramifications, where they define ISP awareness as the overall knowledge and understanding of the information security policy requirements prescribed in ISP. Organization ISP reflects its expectations of their employees to

comply with ISP (Bulgurcu et al., 2010a). ISP awareness is specifically concerned about the awareness of the organization ISP and its content, principles, and security guidelines.

Bulgurcu et al. (2010b) state that ISP awareness is different from general awareness. For instance, general awareness may refer to the state where the employee is aware of using passwords as a security measure but may not know the exact specifications of that password like periodically changing the passwords, using certain length, or using a specific character compositions (Bulgurcu et al., 2010a). Hence, they state that both general ISA and ISP awareness constitute the information security awareness (ISA). However, they did not examine if there are any relationships between general ISA and ISP awareness. To address this issue, this study focuses on information security policy awareness (ISP awareness) as a core construct of the research model and conceptualizes that there is a state of general information security awareness that influences the next state where the employee has ISP awareness. In other words, general security awareness affects ISP awareness.

While D'Arcy et al. (2009) define information security awareness as whether the employee is aware or not of the existence of the ISP in their organization, other definitions state that information security awareness is the amount of knowledge and understanding that the employee has about his organization's ISP and its requirements (Bulgurcu et al., 2010a; M. T. Siponen, 2000a). In this study, the researcher believes that awareness is not a state where the employee knows (aware) or not about the existence of an information security policy in his/her organization (D'Arcy et al., 2009). Rather, the researcher believes that awareness reflects the amount of general knowledge and understanding of the requirements and issues of the organization ISP (Bulgurcu et al., 2010a; M. T. Siponen, 2000a).

Examining ISP awareness as a core construct in this study is consistent with the argument that information security awareness in organizations is an essential factor for employees to change their behavior toward ISP compliance (Siponen, 2000a). Information security policy can be useful only if individuals use it and comply with its instructions or it will lose their usefulness if it is misused (Ceraolo, 1996; Goodhue & Straub, 1991; Hoffer & Straub, Jr., 1989; Detmar W Straub & Welke, 1998). Siponen (2000) points out that two factors (framework and content) affect the level of awareness about security guidelines. The framework factor is closer to the engineering disciplines (i.e. using mathematics and/or philosophical logic) where structural manner and quantitative research may be formalized. NIST framework for

information security awareness represents an example of the framework factor and how it works toward increasing the employee information security awareness (NIST SP 800-100, 2006; NIST SP 800-50, 2003). The content factor on the other side refers to the informal interdisciplinary field of study where Siponen refers to that as “non-engineering area” (Siponen, 2000a). Siponen raised the issue that content factor is a matter too when it relates to the employee motivation to comply with information security policy (Siponen, 2000a). This is consistent, with the proposed research model in this study, in two ways. First, the researcher posits that ISP quality, which is the content factor in Siponen’s approach, is important to increase ISP awareness. Second, this study examines the satisfaction concept with information security policy which is consistent with Siponen’s approach about the importance of motivation in information security programs to motivate employees to follow information security guidelines and instructions (Siponen, 2000a).

Several researchers have studied different issues related to the employee security, particularly their awareness and behavior. A classification study analyzes and critiques different approaches used in information security related issues (Siponen, 2000b). The study classified the security approaches into two categories. The first category includes the approaches that use non-punishment strategy to affect users’ security behavior in order to reduce their misuses. The approaches in the first category rely on different means to influence users’ behavior such as increasing the motivation of users to use information systems correctly and follow security rules and guidelines to protect information systems. The second category includes those approaches that introduce punishment strategies as an external deterrence to reduce IS misuses (Siponen, 2000b). With regard to the first category, the study further divides the approaches into sub-categories. The first set of approaches analyzes the effects on a human while the other side is concerned about the contribution of security-related products. Information security awareness belongs to the first sub-category of the first category (Siponen, 2000b). Figure one shows that information security awareness is categorized as a non-punishment approach.



Figure 1: Taxonomy of information security research approaches.

Lebek et al., (2013) (2014) conducted a literature review related to information security awareness and security behavior. They analyzed 144 published papers in the period from 2000 to 2014. The study finds that 54 different theories are used to explain and understand information security awareness and behavior. Most of the 54 theories are used in two or fewer publications. Seven theories are found to be the most common theories to be used in this domain. The study classifies these theories into two categories: behavioral theories (four theories) and learning theory (three theories) (Lebek et al., 2014). The most frequently used behavioral theories are: Theory of Reasoned Action/ Theory of Planned Behavior (TRA/TPB), Protection Motivation Theory (PMT), General Deterrence Theory (GDT), and Technology Acceptance Model (TAM). In fact, these behavioral theories have attracted information systems researchers in general not only information security researchers, and have been seen to be well-developed and valid theories. The study developed a meta-model explaining the factors that affect the behavior of users by combining the core constructs in the four top theories (Lebek et al., 2013, 2014).

Theory of Planned Behavior (TPB) was introduced by (Ajzen, 1991). TPB is an extension of the Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1975). Those two theories assume that “intention” is the immediate antecedent of the correspondent action. TRA theory assumes that the state of intention is shaped from two constructs: attitude toward behavior and subjective norms concerning the behavior (Fishbein & Ajzen, 1975). TPB theory further extends TRA by including “perceived behavioral control” as a third construct to shape the intention (Ajzen, 1991). In cybersecurity behavioral context, the employee intention toward

complying with information security policy depends on their overall evaluation of compliance related behavior and their normative beliefs about ISP compliance. In other words, higher intention to comply with ISP comes as a consequence of the greater feeling of the reflected actual control over those behaviors (Aurigemma & Panko, 2012; Bulgurcu et al., 2010a; Lebek et al., 2014). In this regard, information security awareness (ISA) has a positive effect on the attitude toward ISP compliance (Bulgurcu et al., 2010a). Similar to attitude definition, satisfaction is defined as the positive evaluation of the pleasant user experience with information systems (Au et al., 2008). Since there is a positive influence of ISA on the attitude of employees toward ISP compliance (Bulgurcu et al., 2010a), the researcher conceptualizes that the level of ISP awareness positively influences the satisfaction with security guidelines and rules.

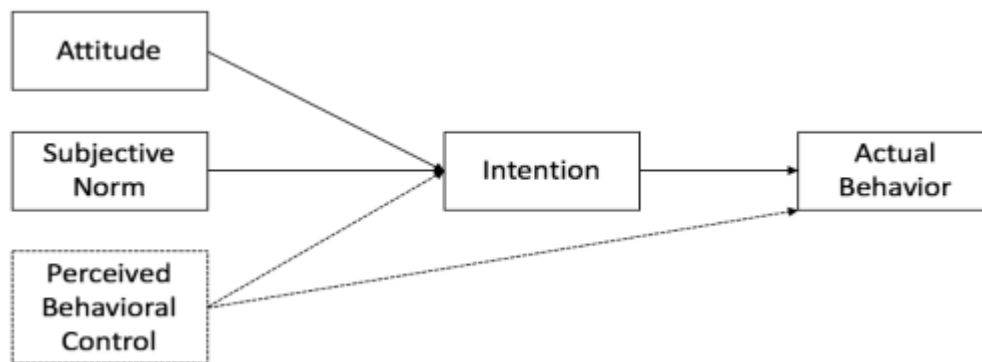


Figure 2: Theory of Reasoned Action/Theory Planned Behavior (TRA/TPB).

The General Deterrence Theory is adapted from criminal justice research (Gibbs, 1975). It assumes that employee decision to engage in a crime or violate the rules is influenced by three factors: perceived severity of sanctions, perceived certainty of sanctions, and punishment. Based on such influence, employees will balance the cost and benefits of rule violation (Lebek et al., 2013). In the information security behavioral research context, perceived severity of sanctions and perceived certainty of sanctions, or punishment affect ISP compliance decision by assessing the compliance cost and benefits (Bulgurcu et al., 2010a; D'Arcy et al., 2009).

Protection Motivation Theory is adapted from health psychology domain. The theory explains the protective behaviors to cope with potential threats (Maddux, James E.; Rogers, 1983; Maddux J.E & R.W, 1983). In information security context, the attitude of employees toward information security is shaped by two mediated factors: threat appraisal and coping

appraisal (Bulgurcu et al., 2010a, 2010b). Employees with high awareness levels (large knowledge and higher understanding) of the potential security threats and risks form different attitude toward perception of security risks and coping appraisals than employees with low awareness levels (C. L. Anderson & Agarwal, 2010; Herath & Rao, 2009a, 2009b; Lebek et al., 2014).

Technology Acceptance Model (TAM) is proposed by Davis et al. in (1989). The model presents the antecedent factors that affect technology acceptance. Particularly, the model proposes that perceived usefulness and perceived ease of use have a strong influence on individuals to make the decision to use a certain technology. Perceived usefulness indicates the employee subjective probability of the usefulness, where using a certain information system may lead to improving their performance and productivity. Perceived ease of use, on the other side, indicates the degree to which an employee perceives that using specific information system is easy and free of effort (Venkatesh et al., 2003). In the context of information security awareness, TAM asserts that both factors (perceived usefulness and perceived ease of use) have a significant influence on the employee intention to comply with information security policy (Al-Omari et al., 2012).

The theories presented in the above paragraphs explain different factors, which affect behavioral intention and actual behavior. Each theory has been tested and assessed multiple times in the literature. However, each theory focuses on individual behavioral factor and ignores other factors like organizational factors (Kukafka et al., 2003). Ignoring the effect of such factors may result in making these theories inefficient. Therefore, it is important to investigate additional factors beyond the main constructs presented in the main theories that may have an additional impact on employees security awareness and behavior (Lebek et al., 2013, 2014). Therefore, the researcher of this study investigates other organizational related factors from the equity theory and their influence on information security awareness and behavior.

Innovation Diffusion Theory

Innovation Diffusion Theory (IDT) is proposed by (Everette M Rogers, 1995). IDT explains the five stages of the innovation-decision process which include: awareness, attitude formation, decision, implementation, and confirmation (Dinev & Hu, 2007; Everette M Rogers, 1995). The first three constructs in the innovation diffusion model represent the causal chain,

which states that awareness (knowledge) influences the attitude (persuasion) of individuals, which, in turn, affects the decision (actual behavior) (Everett M. Rogers, 2003). In this study, the researcher adopts Rogers's causal chain model by viewing ISP awareness as knowledge and persuasion or attitude as satisfaction. Satisfaction construct represents the state where individuals are satisfied and persuaded by the performance, usefulness, or quality of any technology, which, refers to the attitude formation about that technology (Bulgurcu et al., 2010a). In the context of information security awareness, the level of ISP awareness influences the persuasion degree about the usefulness of ISP in organizations and increases the level of satisfaction with the organization ISP. Thus, ISP awareness is an antecedent for the attitude formation which is represented by the satisfaction construct in the current study.

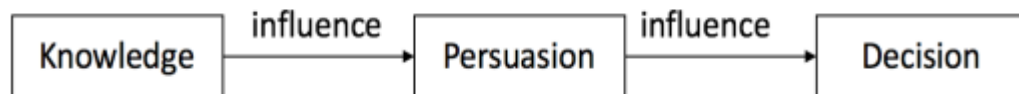


Figure 3: First three constructs of causal chain model.

Furthermore, Innovation Diffusion Theory argues that the innovation diffusion process involves two different players: organizational player and individual player (Everette M Rogers, 1995). The organizational player represents an organization or company that will adopt the technology or innovation. In the context of this study, organizational player represents the organizational factors including ISP fairness and ISP quality. Organizations are responsible for providing fair treatment regarding the ISP and developing ISP with acceptable quality. On the other side, individual player represents people who will use the technology or innovation (Everette M Rogers, 1995). In this study, the researcher presents the individual player as the individual factors, including self-efficacy and technology security awareness, which impact their awareness of the requirements and rules of their organization ISP.

Drawing on the Innovation Diffusion Theory (Everette M Rogers, 1995), the researcher categorizes the antecedents of ISP awareness into two categories: organizational and individual drivers. It is important to combine both categories in increasing individuals awareness about new technology where one category complement the other. This view is consistent with the

motivational approaches of human behavior proposed by (Tyler & Blader, 2005). The organizational category represents the extrinsic factors (command-and-control) where the organizational management is responsible for providing the organizational drivers that may motivate the motivation and learning process of their employees. On the other side, individual category represents intrinsic factors that depend on the individuals themselves (Tyler & Blader, 2005).

Both approaches that divide antecedents drivers, extrinsic and intrinsic motivational approach (Tyler & Blader, 2005) and organizational and individual drivers approach (Everette M Rogers, 1995), are consistent with technology to performance chain model (TPC) proposed by (Goodhue, Dale & Thompson, Ronald, 1995). The model explains the relationship between technology and performance at the individual level. Technology to performance chain model posits that the characteristics of the task, technology, and individual define the task-technology fit. The degree to which that the technology is fit for the task will impact technology acceptance and work performance (Goodhue, Dale & Thompson, Ronald, 1995). Hence, the characteristics of both technology and users are strongly affecting the performance of individuals and their decision to accept and use certain technology (Mălăescu & Sutton, 2015). In the same manner, the researcher argues that the characteristics of the target technology, which the information security policy in this study, and the characteristics of individuals play an important role in their ISP awareness.

Equity Theory vs. Information Security Awareness

Most of the research in the domain of information security behavior and awareness have focused on the main primary theories including TRA/TPB, GDT, PMT, and TAM. Ignoring other factors of other theories may result in inaccurate explanations of the behavior in information security domain. Therefore, researchers in the information security domain need to address additional factors and add theoretical extensions to narrow the gap between individual level factors and external level factors (Lebek et al., 2013, 2014).

In this study, the researcher introduces the equity theory as an external theoretical framework to extend the existing theoretical basis in information security behavior and awareness domain. The Equity Theory is developed by (Adams, 1966). The main idea behind the Equity (inequity) Theory is that individual's perception of injustice in work environment

influences his/her satisfaction. In other words, an employee will be dissatisfied when the ratio outcomes to his input are unequal (less) to other employees' ratio.

In information systems domain, several research studies use the equity theory in studies about software piracy (Douglas et al., 2007; Morton, 2004) and user satisfaction with information systems (Hess & Hightower, 2002; Joshi, 1990, 1992). Douglas uses the equity theory to explain the behavior of software piracy (Douglas et al., 2007). They investigate whether the fairness perception of users who use computer systems influences their decision to involve in software piracy. Their results show that the equity constructs (fairness perception) are significant constructs as a determinant of the behavior of software piracy (Douglas et al., 2007). Morton uses the equity theory in addition to other theories to study the factors that shape the user attitude toward online music piracy. He argues that users' perception of unfairness with their relationship with music industry may influence their behavioral beliefs of online music piracy (Morton, 2004).

The presence of inequity increases the tension of employees. Increasing tension motivates employees to achieve equity, which leads to unexpected behavior (Adams, 1966). In the context of information security awareness, the researcher conceptualizes that the presence of inequity will influence the behavior of employees and impact their awareness of the requirements of the ISP provided by their organizations. Therefore, the researcher argues that employees' belief in the justice (fairness) of their organization's ISP will increase their knowledge of rules and instructions of the information security policy.

Research Model and Hypotheses

Based on the Innovation Diffusion Theory (Everett M. Rogers, 2003; Everette M Rogers, 1995), ISP Awareness Model (ISPAM) is proposed, which will help explaining the employee awareness level about their organization ISP in two folds: the antecedents of ISP awareness and how it impacts the employee satisfaction with the ISP that is provided by their organization. IDT is developed on two premises; the first premise covers the causal chain model where persuasion is influenced by knowledge. The second premise points out that two categories of drivers (organizational and individual) are sharing the role that motivates the innovation process (Everett M. Rogers, 2003).

Analogous to this approach, ISPAM is based on similar premises, with the recognition that ISP awareness is similar to the knowledge that impacts the employee satisfaction with ISP where satisfaction is analogous to attitude formation in Rogers's causal chain model (Everett M. Rogers, 2003). In that regard, the researcher draws on Bulgurcu et al. (2010b) definition to ISP awareness as the knowledge that an employee has and his/her understanding of the requirements, content, responsibilities, and roles prescribed in their organization ISP and the objectives behind the ISP. There are various definitions and descriptions that have been used to define information security policy. ISP, in general, represents the set of technical and procedural guidelines that have been codified in the policy document (Whitman, Townsend, & Aalberts, 2001). The current research adopts the definition of ISP as a set of rules, guidelines, and responsibilities of the proper use of the IS resources to safeguard the informational assets. The adopted ISP definition is consistent with ISP definition in the literature (Bulgurcu et al., 2010a; D'Arcy et al., 2009; Whitman et al., 2001).

The current study will investigate the effect of organizational drivers (extrinsic variables), namely ISP fairness (Adams, 1966; Bulgurcu et al., 2008, 2010b) and ISP quality (Bulgurcu et al., 2010b), and individual drivers (intrinsic variables), namely self-efficacy (Bandura, 1986, 1993) and technology security awareness (T Dinev & Hu, 2007), on the employee ISP awareness. Both organizational and individual drivers are hypothesized to directly influence ISP awareness. Furthermore, ISP awareness is hypothesized to directly influence the employee satisfaction with their organization ISP which will help in forming the attitude of them toward complying with ISP and other cybersecurity behaviors.

As for the knowledge (awareness) usage in the original Rogers's (2003) causal chain model, the proposed model in current study focuses on the satisfaction construct with ISP instead of the attitude toward behavior construct, since both satisfaction and attitude toward behavior impact and shape the individual beliefs and perceptions about any information system (Ajzen, 1991; Au et al., 2008). The employee satisfaction refers more to positive beliefs and positive evaluation of the pleasant experience with an information system (Au et al., 2008). Attitude toward behavior defines as "the degree to which a person has a favorable or unfavorable evaluation or appraisal of the behavior in question" (Ajzen, 1991). However, since both constructs, attitude toward behavior and satisfaction, are similar, most of the research studies in information security behavior literature focused more on attitude toward behavior

and neglecting the satisfaction concept and its effects on user security behavior. Therefore, this study will concentrate on the personal satisfaction with their organization ISP which is the starting point to investigate the role of satisfaction in the behavior of employees, specifically, the associated behavior with information security. The below figure four and table seven represent the proposed research model, named ISPAM, and the description of the constructs used in this study.

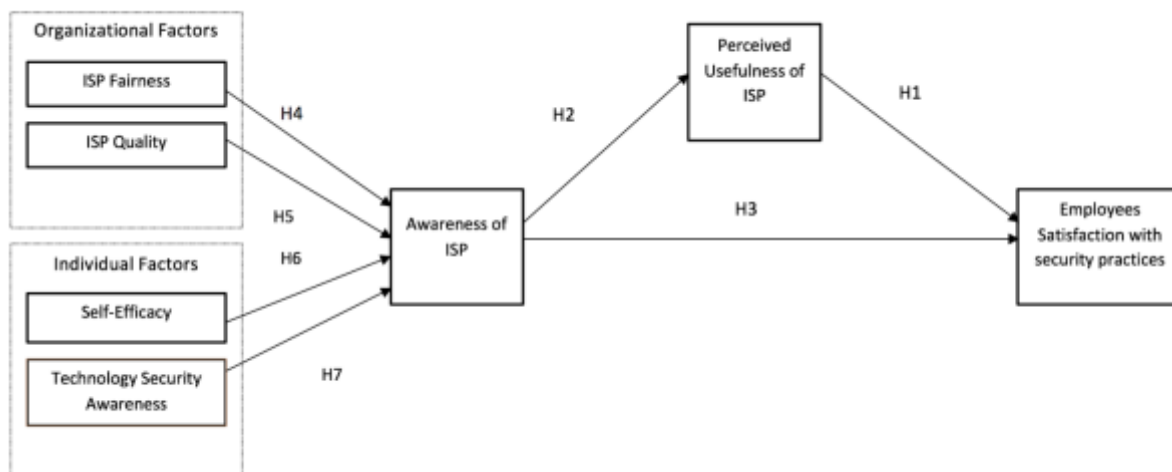


Figure 4: Research model- ISP Awareness (ISPAM)

Table 7: ISPAM constructs name, description, and resources.

Construct	Description	Source
Employee satisfaction with ISP security practices	The degree to which the employee is satisfied with the information security practices in his organization in relation to ISP and information security in general.	(Montesdioca & Maçada, 2015).
Perceived usefulness of ISP	The degree to which an individual believes that following ISP rules and guidelines, to protect the information assets of organizations, would enhance his/her job performance.	(Davis et al., 1989).

ISP awareness	The degree to which that an employee has knowledge and understanding of the rules and security guidelines in their organization ISP and their responsibilities toward it.	(Bulgurcu et al., 2010a).
Organizational factors	The organizational drivers to inspire security skills and knowledge of organization ISP to develop ISP awareness.	(Lin, 2006, 2007; Everette M Rogers, 1995).
ISP fairness	An employee beliefs and perceptions of the justice of the organization ISP.	(Bulgurcu et al., 2010b).
ISP Quality	An employee belief that their organization ISP is well developed in terms of clarity, completeness, and consistency which meets his/her expectations or requirements.	(Bulgurcu et al., 2010b).
Individual factors	The individual drivers to inspire security skills and knowledge of an organization ISP to develop ISP awareness.	(Lin, 2006, 2007; Everette M Rogers, 1995).
Self-efficacy	The beliefs of an employee about his competency, skills, and knowledge to meet the security requirements of their organization ISP to protect the information assets.	(Bandura, 1994).
Technology security awareness	The employee consciousness and interest in information technology associated with cybersecurity tools and strategies.	(T Dinev & Hu, 2007).

Perceived usefulness and employee satisfaction with security practices

The researcher first traces the relationship between perceived usefulness of ISP and the satisfaction with ISP and security practices. The perceived usefulness as a construct has its root

in the literature, in the Technology Acceptance Model, which refers to the degree to which a user believes that using a particular information system would bring valuable benefits and add value to his/her job (Davis et al., 1989). Perceived usefulness is one of the primary factors that impacts the individual acceptance to use certain technology and affects his/her beliefs of the benefits of using that system (Bhattacharjee & Premkumar, 2004).

In information security, perceived usefulness of protection and understanding the consequences of not following the rules and instructions of ISP affects the behavior of employees (Aytes & Connolly, 2004). Albrechtsen (2007) argues that users who are aware of the importance of information security and understand the benefits of protection will not perceive cybersecurity practices as restrictions even with complex security practices. Many studies investigated the influence of perceived usefulness on attitude toward security behavior and on the intention to behave, to comply with ISP, to secure information assets (Al-Omari et al., 2012; Dinev & Hu, 2007; Tamara Dinev et al., 2009; Xue et al., 2011). These studies have confirmed the positive influence of perceived usefulness of protection on the individual beliefs toward security behavior which is translated to ISP compliance or using protective technology.

Since personal satisfaction is analogous to attitude toward behavior, this study investigates the satisfaction of individuals instead of their attitude toward behavior. In fact, the satisfaction of individual refers more to positive beliefs and evaluation of the pleasant experience with an information system (Au et al., 2008). Individual satisfaction is selected as it seems to explain more intrinsic motivation and belief in greater depth than the attitude toward behavior. The literature has proved the strong relationship of perceived usefulness of information systems with user satisfaction (Calisir & Calisir, 2004; F. D. Davis, 1989; Igarria, Guimaraes, & Davis, 1995). For instance, the users who believe that using information systems will increase their productivity and improve their performance are more likely to be more satisfied with that information system (Mawhinney & Lederer, 1990; Vlahos & Ferratt, 1995). A review study of the variables affecting information systems satisfaction shows that usefulness variable has a strong relationship with satisfaction (Adam Mahmoud, Burn, Gemoets, & Jacquez, 2000).

With regards to personal satisfaction with ISPs and cybersecurity practices, it is important to make executing security guidelines desirable in the eyes of the employees (Siponen, 2000a). Further, Siponen (2000a) argues the significant role of perceived usefulness,

in terms of TAM, on user motivation which in turn affect their satisfaction. In line with the literature and consistent with Siponen's (2000a) arguments, the researcher hypothesizes that employees who believe that information security practices are useful for data protection are likely to be more satisfied with the ISP and security practices. Therefore, the researcher forms the following hypothesis:

H1: Employee perceived usefulness of ISP influences their satisfaction with ISP and other security practices.

ISP Awareness and perceived usefulness of ISP

Information security awareness is defined in two ways in the literature. First, awareness is defined as a two-sided concept where it refers to having awareness (knowing of the existence of the ISP or not) or not with regard to ISP awareness (D'Arcy et al., 2009). Second, awareness is defined as knowledge. With regards to information security, awareness refers to the degree to which that an employee has knowledge and understanding of the rules, instructions, and guidelines in their organization ISP and their responsibilities to it (Bulgurcu et al., 2010a). Information security awareness influences misuse behaviors, compliance behaviors, and the beliefs of users. Several studies have shown the effects of awareness on the behavior of system misuse, where more awareness leads to less system misuse (D'Arcy & Hovav, 2009; D'Arcy et al., 2009; D. W. J. Straub & Nance, 1990). For compliance behaviors, awareness of information security policy influences the behaviors of employees toward compliance with ISP (Bulgurcu et al., 2010a).

Regarding beliefs, the literature states the importance of awareness in shaping users beliefs about information security (Goodhue & Straub, 1991). Awareness is considered one of the powerful drivers to influence personal beliefs and perception (Goodhue & Straub, 1991). Lack of awareness may lead to greater potential abuse, while more security awareness of abuses consequences leads to shape the belief that security measures in the organization are unsatisfactory because the employees understand more the implications of security threats (Goodhue & Straub, 1991). In this regard, employees who have a high level of security awareness would believe that security measures provided by their organization are inadequate and they expect more security countermeasures. Siponen (2000) denotes to the role of information security awareness in shaping human belief and as a factor of motivation for users to aware of and commit to cybersecurity instructions and guidelines. Herath and Rao (2009)

find that employees believe that complying with security policies is useful for organizations. Bulgurcu et al. (2010a) point out the association of information security awareness and the general perception of what it entails. Al-Omari et al. (2012) find that awareness of training programs and technology awareness affect employees' beliefs about the usefulness of protection of information systems. Straub (1990) generalizes that as users are aware and understand the security regulations and the consequences of not compliance with ISP, their perception of usefulness will be greater.

Previous studies state that there is an association between ISP awareness and the user beliefs about the usefulness of information security practices. For instance, people who are more aware of information security policy and its consequences have a positive perception of the usefulness of the cybersecurity practices. This argument is consistent with the objectives of security people. Security people, who develop ISP, strive for individuals to internalize and follow cybersecurity guidelines, presented in ISP, rather than only be aware of them (Siponen, 2000a). Internalization means the subjective beliefs and the motivations from inside to comply with ISP (Siponen, 2000a). This issue is one of the challenges regarding ISP compliance where individuals know the security guidelines prescribed in ISPs, but they fail to comply with it correctly (Warman, 1992). Motivating the beliefs from inside can be achieved using external and internal motivations. With regards to internal motivation, moral responsibility plays an important role where individual moral concerns motivate them to do the right thing (Ladd, 1982). In information security context, moral responsibility is achieved if the security actions implemented within organizations are seen desirable and justified in the eyes of the employees. With regard to information security awareness, creating the basics of security awareness affect the inside motivation, intention, and usefulness in terms of TAM (Siponen, 2000a). Therefore, the current study hypothesizes that the awareness of organization ISP influences the perceived usefulness of ISP compliance.

H2: ISP Awareness positively influences the perceived usefulness of ISP.

ISP Awareness and user satisfaction with security practices

The employee awareness of information security is an essential element in information security management program that affects users' behavior to comply with information security policy (Bulgurcu et al., 2010a). Bulgurcu et al. (2010a) define the employee awareness of

information security as their knowledge of information security and their awareness of the organization policy of information security.

Goodhue and Straub (1991) address the role of awareness in affecting and shaping the employee beliefs and perceptions about information security. They claim that three constructs are affecting the concerns about security including industry risk, company actions, and awareness. They point out that when the industry risk is high, employees would feel that security measures are inadequate and unsatisfactory. They also denote that when organizations provide more security actions like hiring security people and provide security software and tools, employees would be more satisfied with security and their concerns would be low (Goodhue & Straub, 1991). They further investigate the association between awareness and satisfaction where employees with more awareness would be less satisfied with cybersecurity strategies of their organization. Herath and Rao (2009b) argue that employees are less likely to comply with their organization ISP if they think that ISP compliance will create difficulties for their day-to-day job activities. Thus, it is important to understand the factors that impact the employee satisfaction with their organization ISP, which result in viewing ISP compliance as a beneficial factor instead of obstacles to their work.

Information security awareness should increase the individual insight and answer the “why and how” type questions. Answering this kind of questions should increase motivation toward information security and influence individual beliefs (M. T. Siponen, 2000a). This argument is consistent with Rogers’s causal chain model, presented in the Innovation Diffusion Theory, where knowledge influences persuasion and persuasion influences decision making (Everett M. Rogers, 2003). In information security context, knowledge represents the awareness that influences attitude toward behavior (Bulgurcu et al., 2010a). Both satisfaction and attitude toward behavior constructs impact and shape the individual beliefs and perception about the targeted information system (Ajzen, 1991; Au et al., 2008). Therefore, this study expects a direct association between the employee ISP awareness and his/her satisfaction with security practices. Following the Innovation Diffusion Theory, this study hypothesizes that ISP awareness influences the personal satisfaction with ISP and other security practices.

H3: ISP Awareness positively influences the employee satisfaction with ISP and security practices.

ISP Awareness Antecedents

In this study, the researcher divides the factors that affect information security awareness into two criteria namely, organizational and individual factors. This categorization is consistent with the Innovation Diffusion Theory, that refers to organizations and individuals as both involved in the innovation diffusion process (Everette M Rogers, 1995). Regarding to IDT, organizations will adopt the innovation or the new technology, while the individuals will use the innovation or the new technology (Everette M Rogers, 1995). Using factor categorizations (organizational and individual) is studied in different research areas in information systems (Lin, 2007; Sliat & Alnsour, 2013). In the context of this study, organizational player represents the organizational factors including ISP fairness and ISP quality. Organizations are responsible for providing fair treatment regarding the compliance with ISP and offer an acceptable quality level of ISP. On the other side, individual player represents individuals who will use the technology or innovation (Everette M Rogers, 1995). Along with organizational factors, the current study involves the individual factors that impact their awareness of the requirements and rules of their organization's ISP.

Drawing on the Innovation Diffusion Theory about the two players approach (Everette M Rogers, 1995), the researcher classifies the antecedents of ISP awareness into two categories: organizational and individual factors. Organizational factors involve ISP fairness and ISP quality, while individual factors involve self-efficacy and technology security awareness. It is important to combine both categories to increase the individual awareness about any new technology where one category complements the other. This view is consistent with the motivational approaches of human behavior proposed by Tyler & Blader (2005). The organizational category represents the extrinsic factors (command-and-control) where the organizational management is responsible for providing organizational drivers that may motivate the motivation of employees and their learning process. On the other side, individual category represents intrinsic factors that immersed inside people and affecting their beliefs and behaviors (Tyler & Blader, 2005).

Organizational Factors

Siponen (2000) argues that ISA indicates that users are aware of information security practices and regulations and should comply with security policy provided by their organization. Organizational factors refer to the organizational effort of implementing security

measures, developing ISP, and educating the employees about the ISP and other security practices and technologies used by the organization (M. T. Siponen, 2000a) (Goodhue & Straub, 1991).

Information security policy is defined as the organizational countermeasures to protect information assets and deter information system misuses (Straub, 1990). In this regard, Bulgurcu et al. (2010) define ISP as “state of the rules and responsibilities of the employees to safeguard the information and technology resources of their organizations”. Herath and Rao (2009) discuss that developing ISP is the responsibility of organizations to protect their information assets by informing employees what to do and not to do, represented in the form of guidelines and regulations. In parallel with ISP development, organizations adopt security training programs as a control measure to protect their information assets (G Dhillon, 1999; Detmar W Straub and Welke, 1998). Security training programs aim to educate employees and increase their awareness about the benefits of information security (Detmar W Straub and Welke, 1998).

In this study, the researcher investigates the organizational factors: ISP fairness and ISP quality. Bulgurcu et al. (2010) highlight the importance of ISP characteristics, and they considered ISP fairness and ISP quality as organizational resources to improve information security. They define the ISP fairness as “an employee belief in the justice of the organization rules and regulations regarding security, which are prescribed in the ISP”. This definition is consistent with the Equity Theory (Adams, 1966). The Equity Theory addresses the user perception of injustice in work environment that leads to making employees dissatisfied. In line with the Equity Theory, people who believe that their organization ISP is fair and provides appropriate processes and treatments would be more satisfied with it and affect their behavior (Aquino, Tripp, & Bies, 2006). Consistent with this view, group engagement model also addresses that procedural justice is essential in shaping social identities within groups, which in turn positively affect perceptions, attitudes, values, and behavior (Exline et al., 2003). In information security, Bulgurcu et al. (2010b) study the association of ISP fairness with employees compliance. They find that ISP fairness positively influences user behavior toward complying with security polices. In this study, the researcher plans to investigate the effect of fairness on the awareness of ISP. People who believe that their organization provides ISP fairness they would be more interested in their organization security which turns into increasing

consciousness of the ISP. In line with the Equity Theory and the literature, the researcher hypothesizes that ISP fairness positively affects employees awareness of their organization ISP. The researcher forms hypothesis 4:

H4: ISP fairness (Organizational factor) positively influences employees ISP awareness.

The literature has investigated the concept of quality in several ways considering the context, means conformance to requirements (Crosby, 1979), conformance specification (Gilmore, 1974), and meeting customer expectation (Gronroos, 1984). Crosby (1979) defines the quality concept considering the expectations and requirements of customers from the product. In line with Crosby's definition, Bulgurcu et al. (2010) state that the quality of ISP is associated with the employee requirements or expectations from the ISP document. They indicate that quality is the employee's perceptions of ISP quality. Bulgurcu et al. (2010) measure ISP quality by compromising three aspects: clarity, completeness, and consistency.

The perception of quality concept influences several constructs including but not limited to perceived value, satisfaction, and employee behavior. High-quality perception of a service or product leads to more satisfaction and giving more values to the product or service (Cronin, Brady, Hult, & Tomas, 2000; Zeithaml, 1988). Service marketing theory confirms the relationship between quality and satisfaction (Cronin et al., 2000). Giving high value or being satisfied with a product or service influence users intention to use and the actual behavior of using that product or service. In information security, Bulgurcu et al. (2010b) reveal a strong relationship between the perception of quality and employees intention to comply with ISP. They investigate the perception of ISP quality on employees ISP compliance. The perception of quality influences users awareness about a product or a service. Yuan and Jang (2008) find a strong relationship of wine festival quality on winery awareness. In line with service marketing theory and literature, the researcher conceptualizes that ISP quality influences employees awareness of their organizations ISP and form the following hypothesis:

H5: ISP Quality (Organizational factor) positively influences employees ISP awareness.

Individual Factors

Individuals awareness of the information security is the knowledge and understanding of information security and the related issues. There are several factors shaping the individual awareness of cybersecurity including but not limited to: life experience, such as opening unknown emails, being attacked by a virus or other security attacks, being penalized for not complying with security policies and regulations, reading about information security from external resources such as newspapers, the Internet, or security journals (Bulgurcu et al., 2010a).

In this study, the researcher investigates the role of self-efficacy and technology security awareness as the individual factors that affect employees awareness. Self-efficacy highlights the self-assessment based on the capabilities and skills of employees to manage and perform a set of required actions necessary for their assigned tasks and achieve a good level of performance (Bandura, 1986). Furthermore, it refers to employees' thinking that they are capable of creating effects (Bandura, 1994). Users who think they can perform well on a given task will do better than users who believe that they will fail.

Drawing on the Social Cognitive Theory, self-efficacy of users encourages the enhancement of employees skills that can cause associated manners (Bandura, 1986). Self-efficacy affects cognitive efforts and leads to knowledge development (Bandura, 1993). People who have higher self-efficacy can build and master their knowledge properly comparing to people with low self-efficacy (Bandura, 1993).

In the context of information security, self-efficacy shapes employees beliefs about their abilities to comply with information security policies and regulations (Maddux J.E & R.W, 1983). Several studies have examined the role of self-efficacy in protecting and securing information assets by affecting employees attitude toward complying with security policies (Pahnila et al., 2007). Rhee et al. (2009) find a relationship between self-efficacy in information security with employees intention to strengthen information security in their organization. Drawing on the Social Cognitive Theory and consistent with previous studies, the researcher conceptualizes that self-efficacy will positively influence the employee awareness about information security issues. Based on that, the researcher forms the following hypothesis:

H6: Employees' self-efficacy (Individual factor) positively influences employees ISP awareness.

Technology security awareness reflects employees consciousness of and interest in learning about technological information and strategies to work with them (Dinev & Hu, 2007). There are several studies that have discussed the importance of security awareness and employees security conscious in protecting information resources (Dinev and Hu, 2007; Rhee, Kim, and Ryu, 2009). Furnell et al. (1996) argue that awareness of cybersecurity tools and technology influences employees awareness of the information security standards and regulations provided in their organization ISP. Rezgui and Marks (2008) concludes that employees security conscientiousness of information security issues and consequences (awareness of security technology and its effects) impact their ISP awareness. In this regards, the researcher hypothesizes that security conscious will influence the ISP awareness. Based on that, the researcher forms the following hypothesis:

H7: Employees' technology security awareness (Individual factor) positively influences employees ISP awareness.

CHAPTER 4

CHAPTER FOUR: RESEARCH METHODOLOGY

Chapter four addresses the research methodology of this study. The chapter introduces the research design, instrument design, and survey instruments validation. Finally, the chapter concludes with data collection procedures and sample data discussion.

Research Design

The research model proposed in this study, information security policy awareness model (ISPAM), is based on the Innovation Diffusion Theory (Everett M. Rogers, 2003; Everette M Rogers, 1995). The basic premise of IDT is constructed by two approaches. The first approach is represented in the casual chain model where knowledge influences persuasion, and persuasion influences decision making (Everett M. Rogers, 2003). Analogous to this approach, ISP awareness is similar to the knowledge that impacts the individual attitude toward behavior which is represented in this study by employees satisfaction with security practices and ISP (Bulgurcu et al., 2010a). The second approach classifies the antecedent drivers of awareness into two categories: organizational drivers and individual drivers. IDT argues that the innovation diffusion process involves two different players: organizational player and individual player (Everette M Rogers, 1995).

This approach is consistent with Technology to Performance Chain model (TPC) proposed by Goodhue, Dale, Thompson, and Ronald (1995). The model explains the relationship between technology and performance at the individual level. TCP model posits that the characteristics of the task, technology, and individual define the task-technology fit. With that regard, the features of both technology and users are strongly affecting individuals performance and their decision to accept and use that technology (Mălăescu & Sutton, 2015). Comparable to this approach, this study argues that the characteristics of the target technology (ISP in this research) and the characteristics of the individuals play a major role in employees ISP awareness.

The organizational category represents the extrinsic factors (command-and-control) where the organizational management is responsible for providing the organizational drivers that may affect the motivation of employees and their learning process. On the other side, individual category represents intrinsic factors that depend on the individuals themselves (Tyler & Blader, 2005). In the context of this research, organizational drivers represent the organizational factors including ISP fairness and ISP quality (Bulgurcu et al., 2010b). On the other side, individual drivers include self-efficacy (Bandura, 1986) and technology security awareness (Dinev & Hu, 2007).

The constructs included in the proposed research model are hard to measure and observe directly because they represent internal beliefs. Therefore, this study will measure these constructs using indirect indicators (Hair, Black, Babin, & Anderson, 2009). In order to get accurate information of individuals internal state such as beliefs and perceptions, this study utilizes the self-report technique. The self-report technique is one of the common ways to gather data in social sciences using surveys and interviews methods (Kline, Sulsky, & Rever-Moriyama, 2000).

In order to collect data from research subjects, this study utilizes the survey method. Survey method is one of the most important areas of measurement in behavioral research (Trochim and Donnelly, 2006). Using survey method can provide the information needed for the research (Fowler, 2013). In other words, using the survey as research method can help collecting the needed information to examine the research questions and test the proposed model hypotheses. Survey method brings three different methodologies: sampling, designing questions, and data collection (Fowler, 2013). In this regards, Pinsonneault and Kraemer (1993) refer to survey research as a quantitative method that gathers standardized information from and/or about the subject being studied. Furthermore, survey research method helps in collecting information about the characteristics, actions, or opinions of a large group of people, referred to as a population. Gable (1994) defines survey as a group of methods related to quantitative research methodology where data for a large population of organizations are collected through some gathering method like mail questionnaire, telephone interviews, and an online questionnaire.

Also, survey method is one of the most common research methods in information systems discipline. IS scholars use the survey method to examine values and relationships

between the research constructs and examining IS theories and hypotheses that used in their research (Newsted, Huff, and Munro, 1998). Therefore, survey method seems to be appropriate for such kind of study. In this context, many research studies used survey research method to examine the study constructs and to test their research hypotheses (Bulgurcu et al., 2010a, 2010b; Johnston & Warkentin, 2010; Li, Zhang, & Sarathy, 2010; M. Siponen et al., 2014, 2010).

Survey Instrument Design

Based on extensive and comprehensive literature review, the survey instruments are developed including research constructs and measurement items. The measurement items of the research model are developed based on constructs that are validated in previous research studies with minor modifications made to fit the study context. (Bulgurcu et al., 2010a, 2010b; F. Davis et al., 1989; T Dinev & Hu, 2007; Montesdioca & Maçada, 2015). Using validated measurement items from the relevance literature improves the validity and reliability of the results (Bulgurcu et al., 2010a; D'Arcy et al., 2009; Montesdioca & Maçada, 2015). The proposed model, ISPAM, includes seven constructs, namely satisfaction with ISP and security practices, perceived usefulness of ISP, ISP awareness, ISP fairness, ISP quality, self-efficacy, and technology security awareness. The survey also gathered basic demographic information. The model includes four reflective constructs and three formative constructs. Each construct is measured with multiple measurement items using a seven-point Likert scale. As a preliminary step, the researcher conducts a pre-test to the developed instruments by conducting a revision process with a group of information systems researchers, university employees, and faculty member of IS department in the United States. Table 8 presents the constructs' names, type, source, and the number items.

Inclusion Criteria: This study adopts the ISP awareness definition from (Bulgurcu et al., 2010a; M. T. Siponen, 2000a) where ISP awareness is the level of knowledge and understanding about the requirements and content of the information security policy. Therefore, the researcher assumes that the participants know of the existence of an information security policy at their organizations. In order to exclude the participants who are unaware at all of the existence of ISP at their organization or do not know if their organization has established an

ISP, the study includes a filter question to make sure that the survey participants are those who aware of the ISP existence in their organizations.

Table 8: Constructs items number and source

Construct	Type	Items	Source
Employees' satisfaction with security practices	Reflective	4	(Montesdioca & Maçada, 2015).
Perceived usefulness of ISP	Reflective	6	(F. Davis et al., 1989).
ISP awareness	Formative	4	(Bulgurcu et al., 2010a) (D'Arcy et al., 2009).
ISP fairness	Formative	3	(Bulgurcu et al., 2010b).
ISP Quality	Formative	5	(Bulgurcu et al., 2010b).
Self-efficacy	Reflective	4	(Bulgurcu et al., 2010a) (Al-Omari et al., 2012).
Technology awareness	Reflective	4	(T Dinev & Hu, 2007).

Demographics: In order to understand the study sample and participants' characteristics, some demographic information is collected including gender, age, educational level, job title, organization's name, experience, years of experience in using computers, number of hours of using computer at works, and software types that the participants have used in their work. Some research studies in the literature have investigated the impacts of demographic information as control variables on information security behavior. However, investigating the impacts of demographic information is beyond the scope of this study. Demographic information is collected to describe and understand the study sample.

Employees satisfaction with security practices: Satisfaction with security practices refers to the degree to which an employee is satisfied with the information security policy and other security practices in his/her organization with regard to ISP (Montesdioca & Maçada, 2015). This construct is measured using four items developed by (Montesdioca & Maçada, 2015). The measurement items assess the satisfaction of employees with information security

practices, training, and ISP. These measurement items are recently developed to be a starting point of using satisfaction construct in information security behavior. Montesdioca and Maçada (2015) have assessed the reliability of the four measurement items. They stated the satisfaction construct is reliable with Cornbach's value of 0.95. The participants in this study were asked to report the degree of their satisfaction with security practices on a Seven-Likert scale with a range from strongly disagree to strongly agree. Higher scores indicate higher satisfaction.

Perceived usefulness of ISP: Perceived usefulness of ISP assesses the degree to which an individual believes that following the rules and guidelines of ISPs to protect the information assets of their organization would enhance his/her job performance and improve information security (Al-Omari et al., 2012; F. Davis et al., 1989). Six measurement items are used to measure the usefulness construct with one item is developed to fit the research context and five items adopted from (Davis et al., 1989). The measurement items address two aspects about the usefulness of ISP, namely improve security and protection and enhance job productivity. There are several studies in the literature that have tested the reliability of the perceived usefulness. Al-omari (2012) reports that perceived usefulness is reliable with 0.891 Cronbach's value. Xue et al. (2011) conduct a reliability test for perceived usefulness with 0.84 Cronbach's alpha value. Dinev and Hu (2007) confirm the reliability of the perceived usefulness with 0.81 reliability value. In information security behavior and awareness, the literature confirms that the perceived usefulness construct is reliable and rigorous (Lebek et al., 2013, 2014). The participants in this research were asked to report their perceived usefulness of the ISP provided by their organization and how it impact their security needs and job performance. Seven-Likert scale is used with values ranging from one to seven where higher values indicate higher perception of usefulness.

ISP awareness: ISP awareness assesses the degree to which that an employee has knowledge and understanding of the rules and security guidelines embedded in their the ISP, and his/her responsibilities toward it (Bulgurcu et al., 2010a; M. T. Siponen, 2000a). Five items are used to measure this formative construct with two items adopted from D'Arcy et al. (2009) and three items adopted from (Bulgurcu et al., 2010a). In information security behavior and awareness, the literature confirms that ISP awareness as a construct is reliable and rigorous with campsite reliability values of 0.958 and 0.826 in Bulgurcu et al. (2010a) and Al-omari (2012) consequently. The participants in this research were asked to report their ISP awareness level.

Seven-Likert scales are used with values ranging from one to seven where higher values indicate higher ISP awareness level.

ISP fairness: ISP fairness gauges the degree to which an employee believes that rules and regulations presented in their organization ISP is just and fair (Bulgurcu et al., 2010b). ISP fairness is a formative construct in the current study where four measurement items adopted from Bulgurcu et al. (2010b) are used to measure it. In their research papers, Bulgurcu et al. have found that ISP fairness is a reliable and rigorous construct with composite reliability value of 0.97 (Bulgurcu et al., 2009b, 2010b). The participants in this research were asked to report their beliefs of the justice and fairness of their organization ISP. Seven-Likert scales are used with values ranging from 1 to 7 where higher values indicate higher fairness perceptions.

ISP quality: ISP quality measures people beliefs that their organization ISP document meet his/her expectations or requirements (Bulgurcu et al., 2010b). ISP quality is a formative construct in this study where three aspects, namely clarity, completeness, and consistency, are used to form the quality construct (Bulgurcu et al., 2010b). Five measurement items are used to measure ISP quality construct and adopted from a previous study (Bulgurcu et al., 2010b). In a previous study, ISP quality is measured using three separate sub-constructs representing clarity, completeness, and consistency with a composite reliability value greater than 0.94 for each sub-construct (Bulgurcu et al., 2010b). In this study, five measurement items from each of the sub-constructs are combined to form the ISP quality. The participants in this study were asked to report their beliefs about the quality of their organization ISP. Seven-Likert scales are used with values ranging from one to seven where higher values indicate higher quality beliefs.

Self-efficacy: Self-efficacy represents an employee's beliefs about his/her competency, skills, and knowledge to meet cybersecurity requirements of the organizations' ISP in order to protect information resources (Bandura, 1986). Four measurement items are used to measure self-efficacy where two items are adopted from Bulgurcu et al. (2010a) and two items adopted from (Al-Omari et al., 2012). Self-efficacy has been used extensively in information systems research and information security behavior and awareness where several research studies have confirmed the strong reliability and validity with composite values greater than 0.89 (Al-Omari et al., 2012; Bulgurcu et al., 2010a; T Dinev & Hu, 2007). The respondents to this item are expected to report their beliefs about their ability, skills, and knowledge with regard to

complying with the ISP. Seven-Likert scales are used with values ranging from one to seven where higher values indicate higher self-efficacy.

Technology security awareness: Technology security awareness measures employees consciousness and interest in information technology that addresses cybersecurity tools and strategies (T Dinev & Hu, 2007). Four measurement items are used to measure the technology awareness with regard to their knowledge about cybersecurity. The items address employees interest of cybersecurity issues and tools and their consequences (T Dinev & Hu, 2007). The respondents to this construct are expected to report their interests in cybersecurity technologies and news related to it. Seven Likert scales are used with values ranging from one to seven where higher values indicate higher technology awareness.

Survey Instrument Validation

Face and Content Validity

This study started the process of item development by an extensive investigation of the related research studies and literature. Most of the measurement items are developed based on items designed and validated in the literature. As a preliminary step, the researcher has conducted a pretest to the instruments of the study by reviewing the measurement items by faculty members in information security and assurance departments in the United States and Jordan (four faculty members). Furthermore, the researcher has conducted a reviewing process including information system researchers (four researchers) and four university employees in the United States. In addition, the survey was reviewed by a graduate student in English department to review the language and to fix any verbal or grammar mistakes. Two faculty members received a paper copy of the instruments, and the rest of individuals received an electronic copy of the survey including the purpose of the study and the measurement items with Seven-Likert scales.

The questionnaires were returned to the researcher from the faculty member, IS researchers, university employees, and the graduate student in the English department. Each individual in the reviewing process provides valuable comments regarding the time it takes to complete the questionnaire, the wording of some questions, and item deletion or addition. All the received comments are taken into account, and the researcher updated the survey

considering the comments. As a secondary step, the updated survey was reviewed by one university employee, and one IS researcher for any further comments.

Construct and Measurement Model Evaluation

The researcher has built the research model and identifies the constructs based on a comprehensive literature review. Most of the measurement items are developed based on constructs validated and tested in previous studies. Employees satisfaction with ISP and cybersecurity practices construct is developed from Montesdioca & Maçada (2015). Perceives usefulness of ISP as a construct has rooted in TAM model (Davis et al., 1989). The researcher has adopted the ISP awareness construct from (Bulgurcu et al., 2010a). The organizational constructs (ISP fairness and ISP quality) are developed from (Bulgurcu et al., 2010b). Self-efficacy construct is developed from (Bulgurcu et al., 2010a; Herath & Rao, 2009b). Technology security awareness is adopted from (Dinev & Hu, 2007).

The study has assessed the construct validity by conducting validity tests based on the type of the construct. For reflective constructs, the study followed the validity tests of the reflected established constructs including reliability (Internal Consistency), convergent validity, and discriminant validity (Hair et al., 2009; Hair, Hult, Ringle, & Sarstedt, 2016, 2013). On the other side, the study has conducted validity test to formative constructs, including convergent validity, collinearity test, and the significance and relevance of outer weight test (Hair et al., 2016).

As mentioned in previous sections, most of the measurement items are developed based on reliable and validated constructs in previous studies in the literature with only one new item. However, it is recommended to confirm the validity and reliability tests when researchers conduct any new survey (Gefen, Straub, & Boudreau, 2000; J. Hair et al., 2016). To evaluate the constructs and measurement model, this study started with internal consistency evaluation of the four reflective constructs. To assess the internal consistency, the researcher conducted two evaluation measures, namely Cronbach's alpha test and composite reliability (CR) test. Internal consistency evaluation provides an estimate of the reliability based on the inter-correlations of the indicators in the measurement model (Hair et al., 2016). Cronbach's alpha test is sensitive to the number of items in each construct which sometimes affect the internal consistency results. However, Cronbach's alpha may be used as a more conservative measure

of reliability. Due to Cronbach's alpha limitation, composite reliability (CR) test is used as a more appropriate measure to internal consistency (Hair et al., 2016).

Unlike Cronbach's alpha, CR uses the difference of outer loadings between indicators (Hair et al., 2016). Both measures vary between 0-1, with higher values indicate higher reliability. As a rule of thumb, values between 0.6 to 0.7 are considered acceptable in exploratory research and values above 0.7 are desirable (J. Hair et al., 2016). According to Gefen et al., (2000), reliability is achieved if we have CR equal to 0.7 or greater, high Cronbach's Alpha values, and AVE equal to 0.5 or higher.

In order to evaluate the convergent validity, this study uses two measures: outer loading and average variance extracted (AVE). Higher outer loading refers that the associated measurement items have much in common. As a rule of thumb, outer loading of 0.708 or higher is desired. AVE is a common measure to assess the convergent validity. AVE is the grand mean value of the squared outer loadings of the linked items with specific construct. AVE values of 0.5 or higher indicate that on average the construct explains more than 50% of the measurement item (Hair et al., 2016).

Discriminant validity is the degree to which a construct is empirically distinct from other constructs in the research model. Therefore, discriminant validity indicates that a construct is unique in the research model and captures phenomena not represented by other constructs. In order to assess the discriminant validity, this study uses two measures: cross loading and Fornell-Larcker tests. Cross loading test is the first step to evaluate the discriminant validity. Specifically, the outer loading of an item that is associated with one construct should be higher than any outer loadings with other constructs in the same model (J. Hair et al., 2009, 2016). The second approach to evaluating the discriminant validity is Fornell-Larcker test. This test calculates first the square root of AVE for each reflective construct. Then, a comparison test of the square root of AVE with the constructs correlations with other constructs in the research model is conducted by the researcher. The correlations with any other constructs should be less than the square root of AVE (J. Hair et al., 2016).

Unlike reflective constructs, formative constructs use other measures to assess the reliability and validity of the measurement model. There are three general assessments to evaluate the measurement model in formative constructs: convergent validity, collinearity assessment, and assessing the significance and relevance of the formative construct items.

Convergent validity refers to the degree to which an item correlates positively with other items linked to the same construct (J. Hair et al., 2016). To evaluate the convergent validity of formative constructs, the researcher needs to test if there are high correlations between formative constructs with a reflective measure of the same constructs (Hair et al., 2016).

Collinearity refers to the problem when a high correlation is found between two measurement items of the formative construct. This issue is called multicollinearity when more than two items have high correlations (Hair et al., 2016). In order to evaluate the level of collinearity, two measures are used: Tolerance (TOL) and Variance Inflation Factor (VIF) (Hair et al., 2016). Tolerance refers to the amount of variance of one formative measurement item (i.e. X1) not explained by the other items within the same constructs. In other words, the test should run a series of regression models with each item serves as the dependent variable and the other items as independent variables (D'Arcy et al., 2009; Hair et al., 2016). For each regression model, TOL values are computed based on the following equations: $TOL = 1 - R^2$. As a rule of thumb, TOL values of 0.1 or lower indicate a potential collinearity problem and TOL values of 0.2 or greater is desirable (Hair et al., 2016). Variance Inflation Factor (VIF) is the reverse value of the tolerance where $VIF = 1/TOL$. As a rule of thumb, a VIF value less than 10 is acceptable, and a value of 5 or lower is considered appropriate (Hair et al., 2016).

Table 9: Constructs and measurement model evaluation

Constructs and measurement model evaluation	
Reflective measurement model	Formative measurement model
Internal Consistency Cronbach's Alpha Composite Reliability (CR)	Convergent validity
Convergent validity Outer loading Average variance extracted (AVE)	Collinearity between indicators
Discriminant validity Cross loading Fornell-Larcker	Significance and relevance of outer weight

The third assessment of the formative measurement model is used to evaluate the significance and relevance of each formative measurement item. The assessment examines first

the significance of the outer weight. If the outer weight is not significant, we analyze the outer loading, if it greater than 0.5 we keep that indicator, else we delete it (see figure 6) (Hair et al., 2016). Table 9 shows the required assessments to evaluate the measurement model of both reflective and formative constructs (Hair et al., 2016).

Population Sampling and Data Collection

Sample Size

The sample size is a controversial issue, and there is no specific approach to handle this issue, where different approaches recommend various recommendations. Hair et al. (2009) argued that sample size is correlated with the number of constructs and their items. They suggested that at least 100 responses for a research model with five or fewer constructs, 150 responses for seven or fewer constructs, and 500 for a large number of constructs. They suggested a minimum sample size of 200 participants as a rule of thumb. Another sample size approaches adopt the number of measurement items. Gorsuch (1983) recommends a ratio of five responses for each item with 100 responses at least. Chin (1998) also argues that PLS method can be used with studies that have at least five responses to each path loading. Other research suggested a ratio of 10 responses for each measurement items (Bentler & Chou, 1987; Everitt, 1975). Another approach for determining the sample size is the ten rules approach (Gefen, Rigdon, & Straub, 2011; Hair et al., 2013). The first rule recommends a minimum sample size to be 10 times the largest number of indicators for any single construct in the model (Gefen et al., 2011; J. Hair et al., 2013). In our study, the construct with the largest number of indicators is the self-efficacy construct with six indicators. Based on this approach, the recommended minimum size would be 60 participants. The second rule recommends a minimum sample size equal to 10 times the number of structural paths (hypothesis) in the research model models. Based on the second rule, the proposed research model has seven structural paths, and the recommended sample size would be 70 participants.

In this research, the researcher follows the approach by Hair et al. (2009). Based on that, the researcher is required to collect data from at least 165 participants based on the 5:1 ratio approach, the number of constructs (7 constructs), and 200 participants at least, based on a rule of thumb by (Hair et al. 2009). Therefore, the researcher set the target sample size to be above 200 participants.

Data Collection

The population of this study is the university employees in the United States of America who are required to comply with the information security policy of their universities. The population includes all employees who are working in the United States universities that have developed ISP. The target sample of this study is a broad mix of university employees from different universities in the United States who are aware of the existence of information security policy at their universities. The population includes faculty of any academic department and staff of different managerial units, such as HR and financial units.

There are several reasons behind selecting the population of the current study. First reason is that universities in the world and particularly in the United States have moved to rely on information technology. Nowadays, most employees at universities in the U.S. have access to university networks and access to sensitive information like student personal information and employee information. Knowing such information facilitate identity theft attackers and may result in cybersecurity breach. Second, most of the previous studies focused on employees who are working at banks, financial institutions, or company since they are the prime target for attackers neglecting other types of institutions such as universities, which include different type of sensitive data. However, we live in the era where data and information are considered as a commodity that can be sold to other organizations for data analysis purposes. University now has a massive infrastructure of networks and data centers that store a significant amount of data related to students, employees, payments, and research projects. Therefore, hackers nowadays are targeting any organization, regardless of its type, that could provide them with any sort of data. Finally, universities employ individuals with a different range of educational levels, ages, and job titles. This diversity represents a suitable option for a representative data sample.

The sample data were collected from the United States of America for several reasons. First, the researcher is a doctoral student at a university in the United States which provides the researcher some access to connect with the participants. Second, the United States of America is one of the advanced countries in the world that rely on institutional laws and has implemented matured ISPs, regulations, and acceptable use policies regarding the information technology resources. Third, most of the work is automated within the United States' institutions and especially universities.

A list of eight universities from different States that developed ISPs is selected. The researcher, his supervisor Dr. Kevin Streff, and some researcher's personal contacts have disseminated the survey to university employees. The Office of Institutional Effectiveness and Assessment at Dakota State University helps with the questionnaire distribution to South Dakota State University.

The study relies on an online questionnaire using Google forms. The online survey is selected since it not expensive, easy to use, save time, and can deliver to participants at various geographical locations. A list of the randomly selected university employees is collected from universities formal websites. The researcher has distributed the survey using e-mail to the participants in the period between February 2016 to May 2016. The participants have received an email including the link to access the survey along with a consent letter showing the purposes of the study and some contact information to the researcher and the supervisor. The survey is anonymous in nature and confidential. The participants are not required to provide the names or any personal information. The participation is optional, and participants could withdraw from the survey without any consequences. The researcher assumes that the participants know about the existence of an information security policy at their organizations. In order to exclude the participants who are unaware at all of the existence of ISP at their organization or do not know if their organization has established an ISP, the study include a filter question to make sure that participants who only know of the ISP existence in their organizations are considered in this study.

The questionnaire was distributed to one thousand nine hundred and fifty-four (1954) employees. Two hundred and ninety-four (294) employees have filled out the survey with 15 percent of response rate. The researcher analyzed the questionnaire and deleted incomplete and unusable responses from the dataset. The total number of the fully completed questionnaire is two hundred and thirty-six (236) which is 80 percent of total participants. With regard to sample size, the researcher follows the approach by (Hair et al. (2009). Based on that, the researcher is required to collect data from at least 160 participants based on the 5:1 ratio approach, the number of constructs (seven constructs), and 200 participants at least based on the rule of thumb by (Hair et al. 2009). Therefore, 236 of the fully completed responses is appropriate to this study purposes.

CHAPTER 5

CHAPTER FIVE: DATA ANALYSIS AND RESULTS

This chapter explains the process of data analysis and presents the results of the empirical measures evaluation for both: measurement model evaluation and structural model evaluation. Measurement model evaluation addresses the relationships between measurement items (indicators) with their associated constructs. The structural model evaluation addresses the relationships between constructs (hypotheses testing) (Gefen et al., 2000; Hair et al., 2009). The chapter introduces first the description of the sample data with an initial evaluation. Then, the chapter explains the evaluation stages of the research model using Structural Equation Modeling – Partial Least Square (SEM-PLS) to evaluate the measurement model and structural model. Finally, the chapter presents the analysis result.

Sample Data Description and Statistics

The study population is the employees at universities in the United States of America that have information security policy or acceptable use policy. The population includes both, faculty and staff employees. A random sample was collected from individuals who are working in 8 different universities. Table 10 shows the demographic information of the study participants.

The table presents some descriptive analysis of the sample data. The analysis shows that of 236 participants, 56.77% are female, and about 75% are in 40-49 age range and above 50 years' age. Most of the participants in the sample have university degree where 22.02% of the sample have a bachelor degree, 22.46% have a master degree, and 45.76% have a doctoral degree. The sample data shows that 115 out of 236 are faculty members and 114 are staff. Work experience shows a diverse distribution with the experience year ranges 16-20 and above 20 are 25% and 29.66% consequently.

Table 10: Sample data description statistics

Variable	Grouping	Frequency	Percentage
Gender	Female	134	56.77%
	Male	102	43.22%
Age	<=20	0	0
	20-29	10	4.24%
	30-39	49	20.76%
	40-49	83	35.17%
	>=50	94	39.83%
Educational Level	High School	6	2.54%
	College	14	5.93%
	Bachelor's Degree	52	22.03%
	Master's Degree	53	22.46%
	Doctoral Degree	108	45.76%
Other	3	1.27%	
Job Title	Faculty	115	48.73%
	Staff	114	48.31%
	Other	7	2.97%
Experience	1-5 years	40	16.95%
	6-10	36	15.25%
	11-15	31	13.14%
	16-20	59	25%
	> 20	70	29.66%
Years of using the computer	1-5 years	6	2.54%
	6-10	40	16.95%
	11-15	19	8.05%
	16-20	40	16.95%
	> 20	169	71.19%
Using computer at work hrs./day	0-1	0	0
	1-4	10	4.24%
	4-8	157	66.53%
	>8	69	29.24%
Computer systems and applications used for job-related work	Spreadsheet (i.e. MS Excel)	228	96.61%
	Word processing	236	100%
	Email	235	99.58%
	University's special application (i.e. D2L)	196	83.05%
	Application packages (i.e. HR software, payroll systems)	164	69.49%
	Programming languages	99	41.95%
	Database systems	132	55.93%

The descriptive analysis indicates that 66.53% of the study participants are using computer systems at work for 4-8 hours per day and more than 29% are using computer systems at work for more than 8 hours per day. The participants of the study have reported that they used different computer software and applications for their job including spreadsheets, word processing, email, database applications, university-related applications, application packages for HR or payroll purposes, programming languages, and other applications. The sample data is a good representative sample of the study population where it includes respondents with different work experiences, job titles, and educational level. The collected sample data reports that the survey participants are using different computer systems at their job which raise the importance to make them aware of the threats and risks related to information systems.

Research Model Evaluation Overview

To assess the prediction power of the proposed model, it is important first to assess the quality of the results. The model evaluation covers empirical measures that assess the relationships between construct indicators as well as between the constructs of the model themselves. The proposed research model is first developed based on the theoretical basis that developed the structural model and the associated measurement items. Now, it is time to assess and compare the proposed model with reality, as presented in the collected sample data. Specifically, to show how the proposed theoretical model fits with the sample data (Hair et al., 2009).

This study adopts the evaluation criteria of the Structural Equation Modeling (SEM) using the Partial Least Square (PLS) path model evaluation. The main premise of the PLS-SEM is maximizing the explained variance of the endogenous latent variables in the structural model (Hair et al., 2016). Therefore, the evaluation process in PLS-SEM highlights predictive capabilities of the proposed model. The researcher used smartPLS version 2.0 to evaluate the model.

Recently, there is great interest in applying PLS-SEM to evaluate structural modeling. Gefen et al. (2000) show that PLS-SEM is the most common method used as a structural equation modeling evaluation tool for the period of 1994-1997 in three prestigious journals in information systems, namely I&M, information system research (ISR), and management information system Quarterly (MISQ). PLS-SEM is a “silver bullet” method for path modeling

and evaluation purposes in many theoretical models, where PLS-SEM has demonstrated many technical advancements (Hair, Ringle, & Sarstedt, 2011). An assessment study of PLS-SEM usage in the 30 top ranked marketing journals over 30 years (1981-2010) demonstrates the widely uses of the method to evaluate structural models (Hair, Sarstedt, Ringle, & Mena, 2012). Applying PLS-SEM method has increased exponentially in top marketing and management journals including MISQ in various disciplines. This increment of using PLS-SEM demonstrates that PLS-SEM distinctive methodological features make it an appropriate alternative to the previously known approach, covariance-based-SEM (CB-SEM) (Hair et al., 2016, 2013).

Table 11: PLS-SEM systematic evaluation

Research Model Evaluation Using PLS-SEM	
Stage 1: Measurement model evaluation	
Reflective measurement model	Formative measurement model
Internal Consistency Cronbach's Alpha Composite Reliability (CR)	Convergent Validity
Convergent validity Outer loading Average variance extracted (AVE)	Collinearity between indicators
Discriminant validity Cross loading Fornell-Larcker	Significance and relevance of outer weight
Stage 2: Structural Model Evaluation	
1	Path Significance
2	Path Coefficients
3	Coefficient of determination
4	Total effect

PLS-SEM modeling assessment represents the systematic evaluation process of the primary criteria used for PLS path modeling. The systematic evaluation of PLS-SEM involves two stages, namely measurement model evaluation and structural model evaluation (Hair et al., 2016). Each stage includes a set of systematic assessments to evaluate the quality and

significance of the results and the relationships between structural model components. Table 11 represents the systematic evaluation of the proposed model using PLS-SEM approach.

The first phase in PLS-SEM evaluation is the measurement model evaluation. As a first step in the structural model analysis, the researcher needs to evaluate the reliability and validity of the construct indicators (Gefen & Straub, 2005; Gefen et al., 2000). Reliability and validity help to assess the degree to which that constructs are accurately represented by the associated indicators. There are two different evaluation measures to evaluate reflectively and formatively developed constructs (Hair et al., 2016). Since the proposed model in this study contains both types of constructs, the researcher follows two approaches to assess reflective and formative constructs. After evaluating the measurement model, the second phase is to evaluate the structural model and test the research hypotheses (paths between constructs) and assess the significance of paths within the research model (Hair et al., 2009).

Measurement Model Evaluation

Measurement model assessment is the first step in PLS-SEM analysis approach and it precedes the structural model evaluation that includes hypotheses testing. This analysis phase helps the researcher to evaluate the quality of the research instruments and the research results. Specifically, measurement model evaluation assesses constructs reliability and validity relying on a set of assessments. There are two broad types of measurement instrument: reflective and formative constructs. Each type has its own approach to assessing the quality, reliability, and validity of the construct. The evaluation process of reflectively developed construct includes internal consistency evaluation (composite reliability), convergent validity, and discriminant validity (Gefen & Straub, 2005; Gefen et al., 2000; J. Hair et al., 2009, 2016). On the other side, the evaluation of formatively developed constructs includes convergent validity, collinearity assessments, and assessing the significance and relevance of outer weight (Hair et al., 2016).

Reflective Measurement Model Evaluation

The reflective measurement model is related to the reflectively developed constructs. In social sciences, constructs are represented by measures or manifestations (Hair et al., 2016). The measurement items are affected by the associated constructs, where the causal relationship is from the construct to its manifest indicators. In other words, the change in the original construct (latent variable) is reflected in the observed measurement items, where changes in the

construct value cause a change in the observed indicators (Christophersen & Konradt, 2012). Therefore, the observed measurement items are expected to have high correlation values between the indicators of the same construct. The high correlation is expected because all the indicators are impacted by the same source (construct) (Christophersen & Konradt, 2012). The expected high value of correlations between the indicators of the particular construct is an indication of the internal consistency of that construct. There are mainly three assessments to evaluate the reliability and validity of reflective model constructs, namely internal consistency assessment, convergent validity, and discriminant validity (Hair et al., 2016).

Internal Consistency

The core traditional criterion to evaluate the measurement model is the internal consistency which measures the degree to which the proposed construct is reliable (Hair et al., 2016). To assess the internal consistency, the researcher assessed two quality measures: Cronbach's Alpha and Composite Reliability (CR). Cronbach's Alpha measures the reliability of the reflectively developed constructs based on the interrelations between the observed measurement items (Hair et al., 2009). However, this quality measure assumes that all measurement items are equally reliable while PLS-SEM weights them based on their individual reliability. Furthermore, Cronbach's alpha test is sensitive to the number of indicators in each construct which sometimes affect and underestimate the internal consistency results. Nevertheless, Cronbach's alpha may be used more with conservative measures for reliability.

Due to the limitations associated with Cronbach's alpha test, composite reliability (CR) test is used as a more appropriate measure to internal consistency in measurement model evaluations (Hair et al., 2016). Unlike Cronbach's alpha, CR uses the difference between outer loadings of the indicators which meet the PLS-SEM approach of prioritization for the associated indicators (Hair et al., 2016). Both measures vary between 0 to 1, with higher value indicates higher reliability. As a rule of thumb, values between 0.6 to 0.7 are considered acceptable in exploratory research and values above 0.7 are desirable (J. Hair et al., 2016). According to Gefen et al., (2000), reliability is achieved if we have CR equal to 0.7 or greater, high Cronbach's Alpha values, and AVE equal to 0.5 or higher.

In the current study, four reflective constructs are developed, namely satisfaction with ISP and security practices (SAT), perceived usefulness of ISP (PUOP), self-efficacy (SE), and

technology security awareness (TSA). Table 12 shows the internal consistency measures of this study. As shown in Table 12, all the values support the internal consistency reliability tests where Cronbach's alpha and CR values are satisfactory with values greater than 0.84. Furthermore, AVE values for all reflective constructs are higher than the threshold 0.5 Gefen et al., (2000). The results confirm the reliability of the reflective constructs used in the proposed research model.

Table 12: Cronbach's alpha, CR, AVE

	Cronbach's Alpha	CR	AVE
ISPF	-	-	-
ISPA	-	-	-
ISPQ	-	-	-
SAT	0.957	0.940	0.85
SE	0.924	0.890	0.753
TA	0.895	0.844	0.681
PUOP	0.925	0.903	0.675

Convergent Validity

Convergent validity assesses the degree to which a measurement item correlates with alternative measures of the associated construct. In other words, convergent validity evaluates the proportion of variance of the construct shared by each measurement item (Gefen & Straub, 2005; Gefen et al., 2000; Hair et al., 2009). According to Hair et al. (2016), the measurement items of the reflectively developed constructs are considered as alternative approaches to measuring the constructs. Therefore, the measurement items in reflective measures should share a high proportion of variance.

In order to evaluate the convergent validity, PLS-SEM approach uses two assessments: outer loading of the reflective construct indicators and the average variance extracted (AVE) (Hair et al., 2016). Outer loading measures the extent to which that measurement items have in common with the associated construct. Higher outer loading on the associated construct represents how much in common the measurement items have (Hair et al., 2016). In other words, the outer loading value is usually representing the measurement items reliability with higher value indicates higher reliability. As a rule of thumb, a desirable outer loading should be 0.708 or higher (Hair et al., 2009, 2016; J. F. Hair et al., 2011). As shown in Table 13, all outer loadings values of the reflective constructs in the current study are higher than the threshold

value (0.708). The analysis results of the outer loadings conclude that all the measurement items are strongly linked with their theoretically associated constructs.

Table 13: Measurement items loadings and reflective construct's AVE

Construct	Measurement items (Questions)	Mean	STD	Loading
SAT <u>AVE=0.85</u>	Satisfaction with ISP and security practices			
	I am satisfied with the information security practices of my organization.	5.547	1.338	0.925
	I am satisfied with the information security training provided by my organization.	4.602	1.646	0.839
	I am satisfied with the information security policy of my organization.	5.458	1.363	0.959
	Overall, I am satisfied with the information security in my organization.	5.492	1.357	0.960
PUOP <u>AVE=0.67</u>	Perceived Usefulness of ISP			
	I believe that following my organization information security policy addresses my job-related security needs.	5.809	1.259	0.806
	I believe that following my organization information security policy enables me to accomplish tasks more securely.	5.919	1.226	0.848
	I believe that following my organization information security policy enhances my effectiveness on the job.	4.979	1.537	0.844
	I believe that following my organization information security policy improves the quality of the work I do.	4.644	1.624	0.794
	I believe that following my organization information security policy protects my organization's information systems.	6.072	1.067	0.763
	Overall, I find following my organization information security policy is useful to my job.	5.555	1.400	0.869
	Self-Efficacy			
SE <u>AVE=0.75</u>	I have the required skills to fulfill the requirements of my organization's information security policy.	6.042	1.170	0.881
	I have the required knowledge to fulfill the requirements of my organization's information security policy.	5.606	1.299	0.903
	I can easily comply with my organization's information security policy whenever I have the desire to that.	5.932	1.256	0.845
	I do not need any help in order for me to comply with most of my organization's information security policy.	5.517	1.439	0.838
TSA <u>AVE=0.68</u>	Technology Security Awareness			
	I follow news and developments about anti-virus technology.	4.610	1.796	0.820
	I discuss with friends and people around me Internet security issues or anecdotes.	4.127	1.699	0.803
	I read the news about malicious attacks on Internet users.	4.784	1.566	0.876
	I am aware of the spyware issues and consequences.	5.280	1.455	0.798

The second measure to assess the convergent validity is the average variance extracted (AVE). Unlike outer loading, AVE measures the convergent validity on the construct level. AVE calculates the mean value of the squared loadings of the measurement items linked with the associated construct in the research model. In other words, AVE value indicates how much variance of the measurement items is explained by the associated construct. Therefore, AVE

values of less than 0.5 mean that more than half of the variance is not explained and remains in the measurement error. As a rule of thumb, AVE of values equal to 0.5 or more are considered satisfactory (Hair et al., 2016). As shown in table 12, AVE values for the four reflective constructs in this study are within the desirable range where values are higher than 0.5 which indicate that the constructs in the proposed research model explain the higher variance of the associated measurement items.

Discriminant Validity

Discriminant validity is one of the reflective construct evaluation. It measures the degree to which a certain construct is different from other constructs within the same model (Hair et al., 2009). In other words, discriminant validity indicates that a specific construct is unique and captures a distinct phenomenon that is not captured by other constructs in the same research model (Hair et al., 2016). Conventionally, the first step to assess the discriminant validity is to analyze the cross loadings. Cross-loadings approach is typically a comparison of the outer loadings for each measurement item with all the constructs in the research model.

Table 14: Cross loadings analysis

	SAT	SE	TSA	USOP
S1	0.925213	0.48617	0.227704	0.761102
S2	0.839476	0.458731	0.273185	0.595136
S3	0.958976	0.529809	0.236913	0.779301
S4	0.960452	0.517345	0.208001	0.777013
SE1	0.424106	0.881644	0.37651	0.347137
SE2	0.472015	0.90386	0.350116	0.399269
SE3	0.499072	0.845131	0.240647	0.502706
SE4	0.48382	0.838866	0.338659	0.441051
TA1	0.235644	0.314258	0.820929	0.297266
TA2	0.22021	0.315495	0.803477	0.277514
TA3	0.174652	0.268023	0.876255	0.225145
TA4	0.207413	0.333111	0.798828	0.148691
U1	0.756211	0.484592	0.202982	0.806744
U2	0.668463	0.397519	0.175846	0.848536
U3	0.597322	0.306115	0.266976	0.844385
U4	0.572019	0.255892	0.257196	0.79469
U5	0.603954	0.505342	0.250133	0.763338
U6	0.681451	0.40307	0.239917	0.869084

According to some research scholars, outer loadings with the associated construct should be higher than any outer loadings with other constructs in the same model (Gefen & Straub, 2005; J. F. Hair et al., 2011, 2012; J. Hair et al., 2016). As a rule of thumb, loadings of

0.7 and above are desirable with at least 0.1 greater than the loadings with other constructs in the same model (Gefen & Straub, 2005). Table 14 shows that each measurement item has, as recommended, higher outer loading with its theoretically associated construct than with other constructs in the proposed research model. For instance, the result clearly shows that the measurement items S1, S2, S3, and S4 have higher outer loadings with their theoretically corresponding construct (satisfaction in this case) than with other constructs in the model. The same thing with the measurement items of the other constructs. But one item, U1 that is theoretically associated with perceived usefulness of ISP, has cross loading with SAT construct with only 0.05 lesser than with perceived usefulness. It is worth noting, however, that satisfaction and perceived usefulness of ISP are highly correlated at 0.79 as shown in Table 15. This is typically considered a serious problem if the correlation between two variables is greater than 0.8 (Bagozzi, Yi, & Phillips, 1991). Thus, the cross loading analysis revealed that all reflective constructs are empirically distinct.

Table 15: Fornell-Larcker evaluation

	AVE	ISPF	ISPA	ISPQ	SAT	SE	TA	PU
ISPF	-	Formative						
ISPA	-	0.591	Formative					
ISPQ	-	0.718	0.731	Formative				
SAT	0.85	0.645	0.673	0.690	<u>0.922</u>			
SE	0.753	0.496	0.699	0.648	0.54	<u>0.867</u>		
TA	0.681	0.167	0.468	0.257	0.253	0.375	<u>0.825</u>	
PUOP	0.675	0.549	0.67	0.625	0.793	0.486	0.28	<u>0.821</u>

The second step toward discriminant validity evaluation is to conduct the Fornell-Larcker test (Hair et al., 2016). Fornell-Larcker evaluation approach first calculates the square root of the AVE values and compare the square root values with other correlation scores in the correlation matrix (Hair et al., 2016). The square root value of AVE for any construct should be greater than any correlations with other constructs. Table 15 shows how Fornell-Larcker approach evaluates the discriminant validity. The analysis results report that the AVE square root values of the constructs in this study are greater than the corresponding off-diagonal correlations of the constructs to their latent variables. For instance, the square root of the SAT AVE equal to 0.922 which is greater than the correlations with other constructs. Both

assessments, cross-loadings and Fornell-Larcker, confirm that the discriminant validity conditions are met for all reflective constructs of the proposed research model in this study.

Formative Measurement Model Evaluation

Formative measurement models refer to the models that include formatively developed constructs. Unlike reflectively developed constructs, the causal relationships in formative constructs are from the measurement items to their associated constructs (Hair et al., 2016). In other words, the measurement items are assumed to cause the constructs (Christophersen & Konradt, 2012). In formatively developed constructs, measurement items are not interchangeable like in the case of reflective constructs. In fact, each item captures a specific aspect to form the concepts of the formative constructs. Jointly, the measurement items define the meaning of the formatively developed constructs (Hair et al., 2016).

One main different of the formatively developed constructs is that internal consistency between items is not applied as the case in reflective constructs. Indicators that form the formative constructs do not covary. Therefore, considering correlations between measurement items in the same construct have negative consequences on the content validity of the construct indicators (Hair et al., 2016). In this regard, PLS-SEM is the appropriate analysis approach to assess research models that include formative constructs (Hair et al., 2012). Instead of using quality assessments such as composite reliability and AVE assessments, this study employs other criteria to measure the quality of formatively developed constructs including convergent validity assessment for formative constructs, collinearity assessment, and assessing the significance and relevance of formative indicators (Hair et al., 2016).

Convergent Validity of Formative Construct

Convergent validity refers to the degree to which an indicator correlates positively with other indicators associated with the same construct (Hair et al., 2016). To evaluate the convergent validity of formative constructs, the researcher needs to test if there are high correlations between formative constructs with a reflective measure of the same constructs (Hair et al., 2016). Chin (1998) name this type of analysis as redundancy analysis. Specifically, the researcher needs to analyze the correlations between the formatively developed construct ($X_{\text{formative}}$) and reflectively developed construct ($X_{\text{reflective}}$) of the same construct, where the formatively developed construct is considered as an exogenous variable and the reflectively

developed construct is the endogenous variable. Then, the researcher has to analyze the path coefficient between the two constructs to assess the convergent validity of the formative construct (Chin, 1998; Hair et al., 2016). The path coefficient of values less than 0.7 is considered a threat to the convergent validity and values of 0.8 or greater are desirable.

Table 16: Formatively developed constructs and global item

Construct	Measurement items (Questions)	Mean	STD
ISP F	ISP Fairness		
	I believe the requirements of my organization's information security policy are reasonable.	5.902	1.121
	I believe the requirements of my organization's information security policy are just.	5.978	1.102
	I believe the requirements of my organization's information security policy are equitable.	5.860	1.176
ISPF global item	I believe the requirements of my organization's information security policy are fair.	5.957	1.068
ISP Q	ISP Quality		
	I believe the requirements of my organization's information security policy are clear.	5.569	1.411
	I believe the requirements of my organization's information security policy are easy to understand.	5.510	1.354
	I believe the requirements of my organization's information security policy are complete.	5.392	1.387
	I believe the requirements of my organization's information security policy are comprehensive.	5.548	1.280
	I believe the requirements of my organization's information security policy are consistent.	5.645	1.262
ISPQ global item	I believe that my organization has high quality information security policy.	5.580	1.147
ISP A	ISP Awareness		
	I am aware that my organization's information security policy prevents employees from installing their own software on work computers.	5.244	1.824
	I am aware that my organization's information security policy describes acceptable use of computer passwords.	6.198	1.167
	I am aware that my organization's information security policy prevents employees from data modifications in an unauthorized way.	5.835	1.387
	I understand my responsibilities to enhance information security as prescribed in my organization's information security policy.	5.611	1.235
ISPA global item	I understand the rules and regulations prescribed by my organization's information security policy.	5.624	1.213

The research model of the current study includes three formative constructs, ISP fairness, ISP quality, and ISP awareness. The researcher draws on scales from the literature to develop the formative constructs indicators. In order to assess the convergent validity, the

global item can be used as a reflective measure that summarizes the essence of the formative measure indicators (Hair et al., 2016; Sarstedt, Wilczynski, & Melewar, 2013).

Table 16 shows the formative indicators and the global items of the formative constructs. Table 17 presents the convergent validity analysis. The researcher tested the convergent validity of each formative construct by creating a model where the formative construct represents the independent variable and the reflective version of the same construct represents the dependent variables. As shown in the convergent validity assessments, the path coefficient for each construct is higher than the suggested threshold (0.8) (Chin, 1998; Hair et al., 2016). For instance, the path coefficients for the formative models are 0.853 for ISP fairness, 0.844 for ISP quality, and 0.817 for ISP awareness. Therefore, all the proposed formatively developed constructs in this study meet the convergent validity requirements.

Table 17: Path coefficient for formative convergent validity

	ISPF reflective	ISPQ reflective	ISPA reflective
ISPF formative	0.853		
ISPQ formative		0.844	
ISPA formative			0.817

Collinearity Assessment

Collinearity is one of the issues related to formatively developed constructs. Collinearity indicates the problem when high correlations between two formative indicators occurred which lead to a problematic issue from a methodological and interpretational standpoint. Unlike reflectively developed measures, formative measures are not expected to have high correlations, and each formative indicator should play a significant role in forming the concept and meaning of the formative construct (Chin, 1998; Hair et al., 2016). There are typically two measures to evaluate the collinearity issue in formative constructs: tolerance (TOL) and the variance inflation factor (VIF) (J. Hair et al., 2016). Both measures are reciprocal to each other.

The tolerance (TOL) measure represents the amount of variance of one formative measurement item (i.e. X1) that is not explained by the other measurement items (i.e. X2,...) linked the same constructs (Hair et al., 2016). In this study, the researcher needs to run a series of regression models where each item serves as the dependent variable and the other as

independent variables. For each regression model, the researcher has to calculate TOL and VIF where $TOL=1-R^2$ and $VIF = 1/TOL$.

As a rule of thumb, TOL values of 0.1 or lower indicate a potential collinearity problem and TOL values of 0.2 or greater is considered appropriate. For VIF, a VIF value less than 10 is acceptable, and a value of 5 or lower is deemed appropriate (J. Hair et al., 2016). Table 18 shows that all the formative measures are appropriate, which means that there are no collinearity issues. For instance, all the tolerance values for the formative indicators are greater than 0.2 which meet the ideal case of TOL requirements. However, one measurement item (F2) is a little bit less than 0.2 which is still acceptable and does not represent a severe collinearity problem.

Table 18: Collinearity analysis

Indicators	R2	TOL	VIF
ISA1	0.346	0.654	1.529051988
ISA 2	0.406	0.594	1.683501684
ISA 3	0.454	0.546	1.831501832
ISA 4	0.473	0.527	1.897533207
F1	0.709	0.291	3.436426117
F2	0.807	0.193	5.18134715
F3	0.6	0.4	2.5
Q1	0.662	0.338	2.958579882
Q2	0.661	0.339	2.949852507
Q3	0.678	0.322	3.105590062
Q4	0.702	0.298	3.355704698
Q5	0.681	0.319	3.134796238

Assessing the Significance and Relevance of the Formative Indicators

Another significant evaluation of the formative indicators and its relevance is outer weight analysis. In this analysis, the researcher needs to assess if the outer weight is significant or not. If t-value is 1.96 or higher at (0.05), the outer weight will be considerable. If not, the researcher needs to check the outer loading value. If the outer loading is greater than 0.5 we keep the indicator, else, we delete that indicator. Figure six shows how to assess the significance and relevance of the formative indicators.

Table 19 shows the analysis results of the significance and relevance of the formative indicators. The results show that most of the formative indicators have significant outer weight values which is an empirical support to retain the indicator. However, three formative indicators

(F3->ISPF, ISA3-> ISPA, and Q3-> ISPQ) are not significance in terms of outer weight results but the outer loading values are relatively high and statistically significance, which is an indication to keep these indicators.

The analysis of the significance and relevance of the formative indicators concludes the evaluation of formatively developed constructs. Considering the results from the evaluation of reflective measurement model and formative measurement model, all measurement items (reflective and formative) exhibits satisfactory levels of quality which is a statistical support to retain all indicators. Thus, the researcher can proceed further with structural model evaluation.

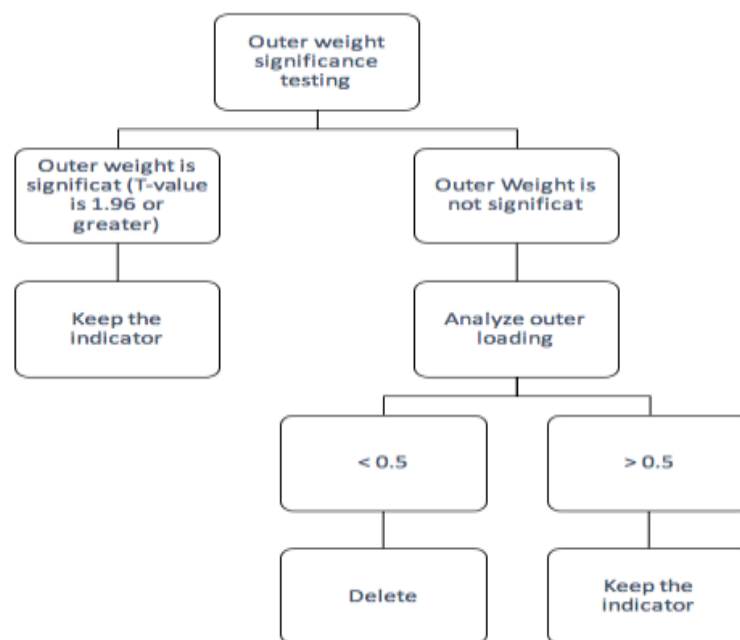


Figure 5: Significance and relevance assessment of formative indicators

Table 19: Outer weight and outer loadings values for formative indicators

Indicator	T-Statistics (O/STERR)	Significance	Outer Loading	Keep the indicator
F1 -> FISP	2.393118	Yes	0.9525	Yes
F2 -> FISP	3.068866	Yes	0.946541	Yes
F3 -> FISP	1.094833	No	0.844457	Yes
ISA1 -> ISA	4.779126	Yes	0.530344	Yes
ISA2 -> ISA	5.802346	Yes	0.672411	Yes

ISA3 -> ISA	1.064884	No	0.622625	Yes
ISA5 -> ISA	6.347811	Yes	0.896278	Yes
Q1 -> QISP	1.981431	Yes	0.923302	Yes
Q2 -> QISP	2.983428	Yes	0.965294	Yes
Q3 -> QISP	1.58957	No	0.764311	Yes
Q4 -> QISP	3.212728	Yes	0.742833	Yes
Q5 -> QISP	2.544443	Yes	0.813191	Yes

Structural Model Evaluation

Once confirming the reliability and validity of constructs measurement items, the next step is to address the evaluation of the structural model that represents the underlying structural model (theories and concepts) (Hair et al., 2009, 2016). Structural model evaluation determines the power of the model to predict the target constructs. As discussed in the research methodology, this study uses PLS-SEM approach to the measurement model and structural model. The researcher ran PLS algorithm and bootstrapping (re-sampling) method with 236 sample size and 5000 re-samples to estimate and evaluate the performance of the proposed research model. The researcher used SmartPLS version 2.0 as the analysis tool.

In order to evaluate the proposed structural model, this study assesses the main measures used in structural model evaluation including the assessment of path significance, path coefficient, coefficient of determination (R^2), and total effects (Chin, 1998; Gefen et al., 2000; Hair et al., 2009, 2016).

Path Significance and Coefficient Assessment

The first step toward structural model evaluation is to test whether the paths of the proposed model are statistically significant or not. Testing the path significance depends on the t-values computed by bootstrapping method. If the t-value is equal or greater than the critical value, the path is considered significance. Typically, path significance assessment uses two-tailed tests where the critical values of t-test should be 1.96 or greater at 0.05 significance level (Chin, 1998; Gefen et al., 2000; J. Hair et al., 2009, 2016).

Table 20: Path significance and coefficient

H #	Path Coefficient	Path coefficient	T-Statistics (O/STERR)	Significance	Supported
1	USOP -> SAT	0.621387	6.767487	Yes	Yes
2	ISA -> USOP	0.670483	6.214173	Yes	Yes
3	ISA -> SAT	0.256837	2.306844	Yes	Yes
4	FISP -> ISA	0.127504	0.709906	No	No
5	QISP -> ISA	0.385951	3.532244	Yes	Yes
6	SE -> ISA	0.297493	2.575429	Yes	Yes
7	TSA -> ISA	0.236257	3.349611	Yes	Yes

The second step is to assess the path coefficients. Higher values of path coefficients indicate stronger relationships. Table 20 demonstrates that all the paths in the proposed research model are significant except the path between ISP fairness and ISP awareness (t-value= 0.709 < 1.96). Therefore, all the proposed hypotheses are empirically supported by the analysis results. Furthermore, the analysis finds that perceived quality of ISP has the strongest influence on the awareness of ISP.

Coefficient of Determination (R²) and Total Effects

The coefficient of determination is the most commonly used measure to assess the structural model which is a measure of the model predictive power. R² represents the amount of variance in the endogenous constructs explained by all exogenous constructs linked to it. R² values range between 0 to 1. As a rule of thumb, R² values of 0.75, 0.5, and 0.25 respectively described as substantial, moderate, and weak (Hair et al., 2016). Table 21 shows that the structural model could explain 61.3 percent of the variance for ISP awareness, 65.8 percent for satisfaction variance, and 35.3 percent of perceived usefulness variance.

Total effect analyzes the change in R² values when a specified exogenous construct is omitted from the model. In other words, total effect measure is used to assess the effect of each exogenous construct on the endogenous constructs regardless of other constructs impact in the model. Total effect results, as shown in table 22, clearly demonstrate that ISP quality has the larger impact on ISP awareness, which is one of the organizational drivers in the proposed model. Furthermore, the results demonstrate the strong linkages between ISP awareness and usefulness and satisfaction as well.

Table 21: Coefficient of determination

	R Square
FISP	
ISA	0.613366
QISP	
SAT	0.574181
SE	
TSA	
USOP	0.341364

Table 22: Total effects

	FISP	ISA	QISP	SAT	TSA	USOP
FISP		0.071964		0.043931		0.042761
ISA				0.610466		0.594201
QISP		0.396867		0.242274		0.235819
SAT						
SE		0.275748		0.168335		0.16385
TSA		0.251369		0.153453		0.149364
USOP				0.664633		

The structural model evaluation concludes the assessment of the proposed research model to explore the antecedents of ISP awareness and its impacts on the perceptions of usefulness and satisfaction. As shown in the above figure, the proposed research model is consistent with the real data analysis and supports the proposed hypotheses except for one hypothesis (H4). The above figure confirms the strong relationship between perceived usefulness and satisfaction where the perceived usefulness of ISP has a significant impact on the satisfaction with security practices (Path coefficient = 0.664); therefore, H1 is supported. The analysis results of the research model find a strong impact of ISP awareness on the perceived usefulness of ISP where the path coefficient is 0.594; therefore, H2 is supported. The

model assessment provides a proof of the ISP awareness effects on the satisfaction with security practices where the path coefficient in H3 is 0.215 which indicates that the proposed hypothesis between ISP awareness and satisfaction is supported. Therefore, the structural model evaluation provides a proof for the direct and indirect impacts of ISP awareness on satisfaction with ISP and other security practices. Therefore, perceived usefulness of protection partially mediates the relationships between ISP awareness and satisfaction.

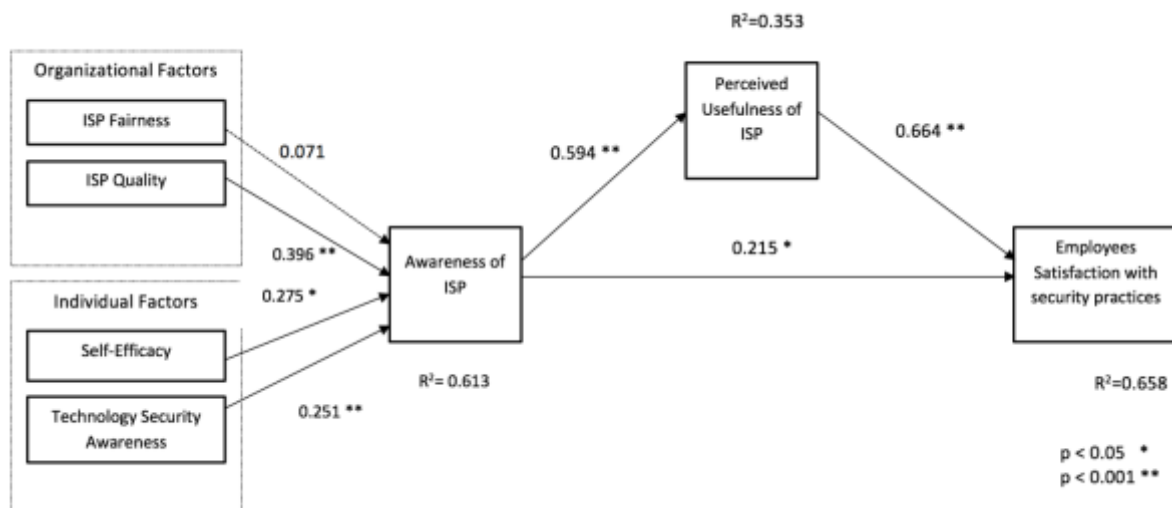


Figure 6: Structural model evaluation

On the left side of the proposed research model, three of the antecedent factors have significant influence on employees' awareness of their organization ISP. However, the analysis results show that ISP fairness has not established a significance relationship with ISP awareness (H4 is not significance). As shown in the above figure, ISP quality is matter and play a significant role in affecting the employee ISP awareness with path coefficient equal to 0.396. Therefore, H5 is supported. Individuals characteristics are found to be important when it comes to their ISP awareness. The model evaluation shows significant relationships between the individual factors (Self-efficacy and technology security awareness) and ISP awareness with path coefficients of 0.275 and 0.251 for self-efficacy and technology security awareness consequently. Therefore, H6 and H7 are supported.

CHAPTER 6

CHAPTER SIX: DISCUSSION AND IMPLICATIONS

Overview of the Study and Findings

Cybersecurity risks remain one of the greatest concerns to current organizations which need to deal with cybersecurity threats and challenges carefully. One of the cybersecurity threats facing organizations these days is insiders. Insiders represent the human factor (employees) who work inside organizations and have access to several information systems resources within organizations (Straub, 1990). Lack of employees security skills and awareness of information security and the associated consequences increase cybersecurity risks and vulnerabilities that threaten confidentiality, integrity, or availability of information systems (Warkentin & Willison, 2009).

Organizations should develop ISPs and acceptable use policies to govern and guide how employees can use information technology, such as email, password specifications, and accessing stored data. Having ISP is one of the countermeasures that organizations should consider in their information security programs to face cybersecurity risks. However, developing ISP and providing acceptable use policies are worthless if employees do not comply with its rules and are aware of them (Warkentin & Willison, 2009). Therefore, organizations should understand how to reduce ISP violations which significantly mitigates information security vulnerabilities and threats and reduces security breaches (D'Arcy et al., 2009). This study focuses on the views that make cybersecurity practices and ISP compliance desirable in the eyes of employees by addressing the role of satisfaction with security practices in information security domain (Montesdioca & Maçada, 2015).

There are several approaches to decrease ISP violations and help understand individuals' behavior when it comes to information security behavior and ISP compliance (Lebek et al., 2014; Tyler & Blader, 2005). Different taxonomies classify the various approaches used in information security behavior. One classification classifies the approaches into punishment and non-punishment (Siponen, 2000b). Another taxonomy classifies the used approaches based on the motivation: extrinsic motivational models (command-and-control) and

intrinsic motivational models (self-regulatory) (Tyler & Blader, 2005). Extrinsic motivational models are based on the idea that involve external motivational factors in a bid to make positive behavior changes such as rewards, sanctions, ISP quality, and training and awareness programs (D'Arcy et al., 2009; M. Siponen et al., 2010; M. Siponen & Vance, 2010). The intrinsic motivational models involve internal motivations and individuals' characteristics, such as self-efficacy, personal skills, and knowledge, (Tyler & Blader, 2005). In comparing both approaches, intrinsic motivational models had better effects on the individual behavior than the extrinsic motivational model (Son, 2011).

Within intrinsic motivational models, 54 different theories used to explain and understand human behavior when it comes to information security and how human perceptions impact their behavior. Of 54 different theories, four theories have been found to be the most frequently used in information security behavior domain. These theories include Theory of Reasoned Action/ Theory of Planned Behavior (TRA/TPB), Protection Motivation Theory (PMT), General Deterrence Theory (GDT), and Technology Acceptance Model (TAM) (Lebek et al., 2013, 2014). These four theories explain the different factors influencing the intention to behave and the actual behavior. However, these theories are ignoring to classify the exogenous factors into external and internal factors or even individual and organizational factors (Kukafka et al., 2003). Presenting exogenous factors in such taxonomies help senior management understanding which taxonomy has more influence.

This study utilizes different factors taxonomies including organizational drivers, which represent the command-and-control approach, and individual drivers, which represent the self-regulatory approach, to develop the research model. Further, the current study investigated the influence of ISP awareness on other perception other than attitude and intention, which is satisfaction. Employees satisfaction signifies more of positive beliefs and evaluation of the pleasant experience with an information system (Au et al., 2008). Therefore, satisfaction accurately presents the desirability of information security practices in the eyes of employees which impact their security behavior (Siponen, 2000a).

Drawing on the Innovation Diffusion Theory (Everett M. Rogers, 2003; Everette M Rogers, 1995), ISP awareness model (ISPAM) is proposed, which will help explain employees awareness level about their organization ISP in two sides: the antecedents of ISP awareness and how it will impact their satisfaction of ISPs. IDT is developed on the premise that two categories

of drivers (organizational and individual) are sharing the role to motivate the innovation process. Furthermore, IDT shows the causal chain of knowledge (awareness) and persuasion (satisfaction) (Everett M. Rogers, 2003). The model is evaluated using survey data collected from university employees in the United States. The assessments of both measurement model and structural model conclude that constructs validity and reliability are achieved and the results are appropriate for the study purposes, and the analysis results of the real data have been found consistent with the theoretical model and support most of the proposed hypotheses.

Study Findings Discussion

This study presents ISP awareness model (ISPAM) that underscores the antecedents of ISP awareness and its impacts on the satisfaction with ISP and security practices. The proposed research model represents a novel approach that used different theoretical approaches including the Innovation Diffusion Theory to explain the role of ISP awareness on the perceptions of information security practices and ISPs and the factors that impact ISP awareness. The proposed research model posits that ISP awareness likely plays a significant role in shaping beliefs about the perceived usefulness of ISPs and affecting the satisfaction with ISPs and other security practices within organizations. The analysis of the survey data supports the validity and reliability of ISPAM model as a useful theoretical approach to explain the antecedents of ISP awareness and predict employees' satisfaction toward security practices.

The ISPAM model explains 65.8 percent of the total variance of the satisfaction, which is a dependent variable, and 61.3 percent of the ISP awareness. These results confirm the ability of ISPAM model in predicting the core dependent variables. Consistent with the predictions of ISPAM, perceived usefulness of security practices and ISP awareness both have a significant impact on the satisfaction with ISP and security practices. The proposed hypothesis (H1) which suggested that perceived usefulness of security practices positively affect the satisfaction with ISP and security practices is supported where the path is statistically significant (path coefficient = 0.664) at p-value < 0.001 significance level. The analysis results confirm the strong relationship between usefulness perception and user satisfaction in information systems domain (Adam Mahmoud et al., 2000; Calisir & Calisir, 2004; Igarria et al., 1995).

ISPAM model finds that employees awareness of information security policy (ISP awareness) has positive effects on perception of usefulness which assumes that information

security policy is important and useful in protecting information resources (H2). Unlike the findings of Al-Omari et al. (2012), ISPAM model evaluation results conclude that the path of H2 is statistically significant and the direction of the relationship is consistent with the proposed theoretical model (path coefficient = 0.594, p-value < 0.001). This finding is consistent with Straub's (1990) argument which indicates that as users are aware and understand the security regulations and the consequences of not complying with ISPs, their perception of usefulness will be greater. This result suggests that universities in the United States have to apparently develop information security policies that define the proper and improper usage of information systems (Straub, 1990). The result is consistent with prior research that ISPs play a significant role in mitigating IS misuses (D'Arcy et al., 2009).

Structural model assessment reports that ISP awareness has a positive and significant impact on employees' satisfaction with ISP and security practices (path coefficient = 0.215, p-value < 0.05). This result suggests that improving ISP awareness in the organizational environment has a positive impact on the satisfaction with ISP and other security practices. ISPAM model highlights the importance of information security awareness in general, and ISP awareness in particular, in shaping the beliefs and attitude about security practices and improving their satisfaction with ISP, which it turns to actual security behavior. The analysis results of ISPAM model is consistent with the argument that the awareness of individuals affect their beliefs and perception about information security (Goodhue & Straub, 1991). In fact, leveraging ISP awareness level increases the understanding of why ISP is important and how to comply with the ISP, which is provided by their organizations. Siponen (2000a) points out that ISP awareness should clearly answer questions of type "why and how" (e.g. why ISP compliance is necessary? And how to comply with security instructions?), which impact their motivation toward information security and safeguarding the information assets. Furthermore, ISPAM model evaluation of the collected data is consistent with Rogers's causal chain model where knowledge influences persuasion and persuasion influences decision making (Everett M. Rogers, 2003). In the context of this study, knowledge represents the awareness that influences attitude toward behavior, where attitude is mapped to satisfaction in this study (Bulgurcu et al., 2010a).

ISPAM model assumes that ISP awareness is affected by four antecedents grouped into two categories (organizational and individual). This assumption is consistent with many

theoretical bases including the innovation diffusion theory that separates antecedent factors into two groups: organizational and individual factors (Everette M Rogers, 1995). Three factors are found to have a significant impact on ISP awareness including ISP quality, self-efficacy, and technology awareness. The analysis result predicts that ISP quality has a significant and positive impact on ISP awareness (path coefficient = 0.396, p-value < 0.001). This finding is consistent with many prior research that ISP quality does matter when it comes to influencing perceptions, awareness, and satisfaction according to service marketing theory (Cronin et al., 2000; Yuan & Jang, 2008). The result suggests that high ISP quality in terms of clarity, completeness, and consistency plays a significant role in shaping ISP awareness which lead to motivating their positive behavior toward information security. This finding represents an indication for organizations to pay more attention to the quality factor at the ISP development time and review their ISPs to make sure that their policy is with high quality.

ISPAM model assessment emphasizes the important role of self-efficacy in shaping ISP awareness. The finding shows that self-efficacy has a significant and positive influence on the ISP awareness where employees who have high self-confidence in their capabilities and skills will have higher ISP awareness (path coefficient = 0.275, p-value < 0.05). This result is consistent with the Social Cognitive Theory that associates self-efficacy with cognitive efforts and leads to knowledge development (Bandura, 1993). Thus, people who have higher self-efficacy are able to build and master their knowledge properly than people with low self-efficacy (Bandura, 1993). Prior research highlights self-efficacy as an essential factor in shaping employees attitude toward complying with security policies and their intention to strengthen information security (Pahnila et al., 2007; Rhee et al., 2009). The analysis of the structural model concludes that ISP awareness level depends on the self-efficacy of employees. Thus organizations should consider improving their employees' self-efficacy in a bid to increase their awareness and knowledge about the security policies and cybersecurity programs in general.

The analysis result of the current study asserts the influence of technology security awareness, related cybersecurity and protection technologies, on the awareness of ISPs. The finding of the present study reports that technology security awareness has a statistically significant relationship with ISP awareness where it positively influences ISP awareness. The result of the ISPAM model analysis is consistent with prior research about the importance role of technology awareness in developing employees ISP awareness (Al-Omari et al., 2012; T

Dinev & Hu, 2007; Rhee et al., 2009). This result suggests that organizations should consider the technological awareness of their employees during their cybersecurity awareness programs. In other words, along with security training and ISP development, cybersecurity awareness programs should introduce employees to general information about the latest security tools and technologies and how to use them.

The structural model analysis shows that ISP fairness has no impact (the path is statistically not significant) on ISP awareness in the U.S. universities. ISP fairness refers to “an employee’s belief in the justice of the organization’s rules and regulations regarding security, which are prescribed in the ISP” (Bulgurcu et al., 2008, 2009b). This result suggests that ISP awareness is not affected by the fairness treatment about ISP. The result can be explained by assuming that the top management at American universities provide fair treatment when it comes to ISP compliance and the research participants have not experienced any unfair treatment related to fairness and equity. Another explanation is that when it comes to fairness concerns, employees who afraid to meet unfair treatment will be more cautious with ISP compliance to avoid any potential punishment.

In conclusion, the finding of the current study suggests that ISP awareness is impacted by several antecedent drivers which shape the awareness and knowledge of information security. Furthermore, ISPAM asserts that both organizations and individuals share the role of developing the ISP awareness where organizations should provide high-quality policies, so that improve their employees’ awareness about cybersecurity rules and regulations. Organizations should also consider the self-efficacy factor of employees and should encourage their technological interest in information security in a bid to increase their ISP awareness. Another interesting finding is the critical role of ISP awareness in protecting informational assets. The proposed research model (ISPAM) reveals the influence of ISP awareness on employees’ satisfaction with ISP and other security practices which help to make information security rules, instructions, guidelines, and practices desirable in the eyes of employees. This is an important point toward information security behavior. The structural model assessment finds that ISP awareness affects satisfaction directly and indirectly. The results confirm the direct significant relationship between ISP awareness and satisfaction (the direct path is statistical significance). ISP awareness has an indirect influence on employees’ satisfaction through impacting their perception of usefulness. Thus, perceived usefulness of ISP partially mediate the relationship

between ISP awareness and the satisfaction with ISP. The research model and the analysis results of the surveyed data highlight the role of ISP awareness in cybersecurity programs. This study is a starting point to explore more about how to shape employees' awareness and how it impact their information security behavior.

Theoretical Contribution

There are several behavioral theories used to explain behaviors associated with information security. Four behavioral theories are frequently used as a theoretical foundation for information security behavioral research domain. These theories include the Theory of Reasoned Action/ Theory of Planned Behavior (TRA/TPB) (Ajzen, 1991; Fishbein & Ajzen, 1975), General Deterrence Theory (GDT) (D'Arcy et al., 2009), Protection Motivation Theory (PMT) (Maddux, James E.; Rogers, 1983; Maddux J.E & R.W, 1983), and Technology Acceptance Model (TAM) (F. Davis et al., 1989). However, each theory focuses on individual behavioral level and ignoring other factors like organizational level (Kukafka et al., 2003). Ignoring the potential effects of factors from other theories may result in making these theories inefficient. Therefore, it is important to investigate additional factors beyond the main constructs presented in the main theories that may have an impact on the security awareness and behavior (Lebek et al., 2013, 2014).

Accordingly, this research study is the first to develop a model, ISP Awareness (ISPAM), utilizing a new theory, the Innovation Diffusion Theory, to explain how awareness of ISP impact the persuasion (satisfaction). Innovation Diffusion Theory offers an essential addition to the theoretical foundation of information security awareness and behavioral research (Everett M. Rogers, 2003). IDT provides a reasonable explanation of how the awareness and knowledge impact the persuasion of employees which results in actual behavior. Therefore, this study relies on IDT as theoretical bases to justify how ISP awareness changes employees' satisfaction with ISP and security practices.

Another valuable contribution this study makes to the behavioral research of information security field is clearly categorizing the drivers of ISP awareness constructs into two types: organizational and individual drivers. This issue is important so that researchers can understand how to determine antecedent factors and the significance of including factors based on their category. For instance, this study assumes that both organizational and individual

factors are important to understanding ISP awareness development. The researcher believes that organizations have the responsibility of developing high-quality ISPs and provide fair treatment. Other organizational factors can be included in future research like management support, rewards, or sanctions. Furthermore, the researcher points out the role of the attributes of employees (i.e. self-efficacy and technology awareness) and its impact on their ISP awareness.

There is lacking research that views the concept of information security awareness and its impact on information security behavior. Most of the prior research in this field employs different behavioral theories that shape employee's intention to comply, actual compliance, or even computer misuses. Thus, the current study lays out the concept of awareness as a crucial component when it comes to information security behavior and contribute to the body of knowledge of information security awareness.

Additionally, this study is the first to investigate ISP awareness antecedents and assesses the impact of awareness on the satisfaction with ISP which significantly influences their behavior. ISPAM model introduce the satisfaction concept as an influential factor when it comes to affect cybersecurity behavior. Satisfaction positively affects behavior where it helps presenting cybersecurity measures and ISP compliance desirable in the eyes of employees.

Practical Contribution

The findings of the current study will assist senior executive management to understand the factors that shape the awareness of information security policy, which will lead to positive information security behavior. Reaching to such a positive behavior will result in reducing employees' misuses and unintentional errors which help to reduce the whole cybersecurity cost. According to the findings of the current study, ISP quality has the highest impact on the ISP awareness. This means that the level of awareness an employee has about the information security policy is significantly influenced by the quality of the policy, which is measured in terms of three aspects: clarity, completeness, and consistency. In this regard, prior research acknowledged that high-quality perception of a service or product result in more satisfaction and more valuing to the product or service (Cronin et al., 2000; Zeithaml, 1988). From marketing discipline, the Service Marketing Theory confirms the relationship between quality and satisfaction (Cronin et al., 2000). Giving high value or being satisfied with a product or

service, influence the intention to use or the actual behavior of using the product or the service. In information security, Bulgurcu et al. (2010b) reveal a strong relationship between the perception of quality and employees intention. Thus, when organizations developing their ISP, management and information security officers need to consider the quality of the policy and to make sure that the ISP is clear, well presented, comprehensive, detailed, direct, concise, and consistent.

The analysis results provide significant evidence that ISP awareness is associated with the attributes of employees and their behavior. The results prove that self-efficacy has significantly impacted the knowledge and awareness of cybersecurity and ISPs. Based on the Social Cognitive Theory, self-efficacy plays an essential role in the cognitive efforts which affect knowledge development and knowledge management (Bandura, 1993). Prior research highlighted the important role of self-efficacy in impacting the behavior associated with information security such as ISP compliance (Maddux J.E & R.W, 1983; Pahnla et al., 2007; Rhee et al., 2009). Therefore, senior management and information security officers need to be aware of self-efficacy as a crucial factor in cybersecurity behavior and should design specific programs for self-efficacy development.

Moreover, the structural model evaluation asserts the role of technology awareness in shaping ISP awareness. This means that if an employee has an interest in technologies related to cybersecurity and follow the related news, such as data breaches, cybersecurity attacks, or privacy issues, will have more awareness of his/her organizations' ISP. Dinev and Hu (2007) state that technology awareness means the consciousness of and interest in learning about technological information and strategies to work with them. Thus, the senior management and information security officers should design cybersecurity awareness programs that motivate employees to learn more about cybersecurity technology and present to them real security incidents and its consequences.

As the structural model assessment shows, ISP awareness is found to have a significant direct impact on the satisfaction with ISP and security practices. Goodhue and Struab (1991) address the role of awareness in affecting and shaping the beliefs and perception about information security. This study states that employees should be aware of the rules and guidelines of the ISP and aware of the importance of ISP in terms of different aspects, such as why the ISP is important, information security risks, security breaches, benefits of ISP

compliance, consequences of non-compliance, and how to comply with ISPs. Awareness of these aspects influences the employees' satisfaction of the security practices and ISPs which result in making the security practices and ISPs desirable and justified in their eyes. Therefore, the ISPAM model evaluation motivates organizations to make ISPs and other security practices desirable and justified for their employees as much as possible in a bid to enhance employees' satisfaction.

Furthermore, the results of this study confirm the influence of ISP awareness on the perception of ISP usefulness. Albrechtsen (2007) argues that users who are aware of the importance of information security and understand the benefits of protection will not perceive information security practices as restrictions even with complex security practices. Many studies investigate the influence of perceived usefulness on attitude toward security behavior and on intention to behave to secure information assets (T Dinev & Hu, 2007; Tamara Dinev, Goo, Hu, & Nam, 2009; Xue, Liang, & Wu, 2011). Therefore, the assessment of the research model in this study motivates organizations to present ISPs as a useful tool to protect informational assets and not contradict their primary work. It is important not to make employees perceive information security practices as restrictions.

Limitations

As with any other empirical study, this study has some limitations. The first limitation is related to the population of the survey. This study surveyed only university employees, which reflects only the academic environment. However, other types of organizations like banking, healthcare, or governmental organizations are not considered in this study. This may impact the generalizability of the study findings to cover different sectors. Future research is needed to replicate the study in other environments and compare the results.

A second limitation has also related to the population. This study focuses only on university employees in the United States, which reflects only the culture associated with the American environment in higher education institutions. Other cultures, such as European, Asian, or middle east, may have different aspects and characteristics that may impact the results. Therefore, future research is required to understand the impact of the culture factor on the ISP awareness. In this regard, the researcher is planning to replicate the study in Jordan, a country in the middle east, and compare the results with the findings of this study.

A third limitation is related to the job role of the university employees. This study considered that both faculty and staff are university employees. Thus, understanding the impact of the job role of the employees on ISP awareness and their satisfaction with ISP is beyond the objectives of the current study. Future research may investigate the impact of job role by comparing the role of faculty and staff.

A fourth limitation is related to the proposed research model. ISPAM addresses the antecedents of ISP awareness and the impact of ISP awareness on the satisfaction of ISP and other security practices. Understanding the impact of satisfaction on employees' intention to comply with ISP is beyond the objectives of this study. Future research may investigate further constructs like the intention to comply with ISP and actual compliance.

Conclusion and Future Work

This study presents the information security policy awareness model (ISPAM) that underscores the antecedent factors of ISP awareness and addresses the impact on employees' satisfaction with security practices. The proposed research model represents a novel approach that utilizes new theoretical foundation in information security awareness field. Drawing on the Innovation Diffusion Theory, ISPAM model explains how ISP awareness impact the perceived usefulness of information security policy and the satisfaction with ISP and security practices. The study posits that ISP awareness has direct and indirect positive impact on satisfaction with security practices. This study is a starting point toward using satisfaction concept in information security domain and investigating its role in affecting employees' behavior.

The study posits that among different antecedent factors, ISP quality likely plays a significant role in shaping employees' ISP awareness. Thus, organizations need to develop a clear, well presented, comprehensive, detailed, direct, concise, and consistent ISPs. The study further finds that employees' ISP awareness depends on employees' characteristics, such as self-efficacy and technology awareness. Therefore, organizations need to focus on employees' motivations toward information security technology by designing motivation workshops or consider information security aspects at the hiring time through job interviews.

REFERENCES

- Abraham, S. (2011). Information security behavior: Factors and research directions. *17th Americas Conference on Information Systems 2011, AMCIS 2011*, 5, 4050–4062.
- Adam Mahmoud, M., 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.
- Adams, J. S. (1966). Inequity in social exchange. *Advances in Experimental Social Psychology*, 2(C), 267–299.
- Ajzen, I. (1991). The Theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179–211.
- Al-omari, A. (2012). *Information security policy compliance: A user acceptance perceptive*. Dakota State University, Madison, SD.
- Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security policy compliance: User acceptance perspective. *45th Hawaii International Conference on System Sciences*.
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276–289.
- Alderfer, P. C. (1969). An empirical test of a new theory of human needs. *Organizational Behavior and Human Performance*, 4(2), 142–175.
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly: Management Information Systems*, 34(SPEC. ISSUE 3), 613–643.
- Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, 22(4), 308–313.
- Aquino, K., Tripp, T. M., & Bies, R. J. (2006). Getting even or moving on? power, procedural justice, and types of offense as predictors of revenge, forgiveness, reconciliation, and avoidance in organizations. *Journal of Applied Psychology*, 91(3), 653–668.
- Au, N., Ngai, E. W. T., & Cheng, T. C. E. (2008). Extending the understanding of end user information systems satisfaction formation: An equitable needs fulfillment model approach. *MIS Quarterly*, 32(1), 43–66.
- Aurigemma, S., & Panko, R. (2012). A composite framework for behavioral compliance with

- information security policies. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 3248–3257).
- Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices : A rational choice perspective. *Journal of Organizational and End User Computing*, *16*(3), 22–40.
- Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly*, *36*(3), 421–458.
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory* (1st ed.). Englewood Cliffs, NJ: PrenticeHall.
- Bandura, A. (1993). Perceived self-efficacy in cognitive development and functioning. *Educational Psychologist*.
- Bandura, A. (1994). Self-Efficacy. *Encyclopedia of Human Behavior*, *4*(1994), 71–81.
- Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. *MIS Quarterly*, *22*(1), 31–60.
- Barman, S. (2001). *Writing IS security policies* (1st ed.). New Riders Publishing.
- Baskerville, R. (1993). Information implications systems security design methods: for information systems development. *ACM Computing Surveys*, *25*(4), 375–414.
- Beachboard, J., Cole, A., Mellor, M., Hernandez, S., Aytes, K., & Massad, N. (2008). Improving information security risk analysis practices for small- and medium-sized enterprises : A Research Agenda. *Issues in Information Science and Information Technology*, *5*.
- Bentler, P. M., & Chou, C.-P. (1987). Practical issues in structural modeling. *Sociological Methods & Research*, *16*(1), 78–117.
- Bhattacharjee & Premkumar. (2004). Understanding changes in belief and attitude toward information technology usage : A theoretical model and longitudinal test. *MIS Quarterly*, *28*(2), 229–254.
- Brancheau, B. J. C. (1994). Key issues in information systems management : 1994-95 SIM Delphi results. *MIS Quarterly*, *20*(2), 225–242.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2008). Analysis of perceived burden of compliance: The role of fairness, awareness, and conditions. *Workshop on Information Security & Privacy*, 19–25.

- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009a). Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, 3, 476–481.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009b). Roles of information security awareness and perceived fairness in information security policy compliance. *15th Americas Conference on Information Systems 2009, AMCIS 2009*, 5, 3269–3277.
- 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-A7.
- 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. *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 1–7.
- Calisir, F., & Calisir, F. (2004). The relation of interface usability characteristics, perceived usefulness, and perceived ease of use to end-user satisfaction with enterprise resource planning (ERP) systems. *Computers in Human Behavior*, 20(4), 505–515.
- Cavusoglu, H. H., & Raghunathan, S. (2004). Economics of IT security management - four improvements to current security practices. *Communications of the Association for Information Systems*, 14, 65–75.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004a). A model for evaluating IT security investments. *Communications of the ACM*, 47(7), 87–92.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004b). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1), 69–104.
- Ceraolo, J. (1996). Penetration testing through social engineering. *Information Systems Security*, 4(4), 37.
- Chen, C. C., Shaw, R. S., & 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. *Proceedings of the 42nd Hawaii International Conference of System Sciences*, 1–10.
- Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, (JANUARY 1998), 295–336.
- Christophersen, T., & Konradt, U. (2012). The development of a formative and a reflective scale for the assessment of on-line store usability. *Behaviour & Information Technology*, 31(9), 20.
- Cronin, J., Brady, M., Hult, G., & Tomas, M. (2000). Assessing the effects of quality, value, and customer satisfaction on consumer behavioral intentions in service environments. *Journal of Retailing*, 76(2), 193–218.
- Crosby, P. (1979). *Quality is free: The art of making quality certain: How to manage quality - so that it becomes a source of profit for your business* (1st ed.). McGraw-Hill Companies.
- 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., Bagozzi, R., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8).
- Davis, F. D. (1989). Perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- Denning, D. (2000). Information warfare and security. *ACM Press*, 27(December), 1–2.
- Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, 7(4), 441–469.
- Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspective. *Information Systems Journal*, Volume: 65(Issue:), Pages: 43-59.
- 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), 386–408.
- Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25(1), 55–63.
- Douglas, D. E., Cronan, T. P., & Behel, J. D. (2007). Equity perceptions as a deterrent to software piracy behavior. *Information and Management*, 44(5), 503–512.
- Dugo, T. M. (2007). *The insider threat to organisational information security: A structural model and empirical test*. Auburn University.
- Durgin, M. (2007). Understanding the importance of and implementing internal security measures. *SANS Institute: InfoSec Reading Room*.
- Everitt, B. (1975). Multivariate analysis: The need for data, and other problems. *The British Journal of Psychiatry*, 126(237–240).
- Exline, J. J., Worthington, E. L., Hill, P., McCullough, M. E., Exline, J. J., Worthington, E. L., ... McCullough, M. E. (2003). The group engagement model: Procedural justice, social identity, and cooperative behavior. *Personality and Social Psychology Review*, 7(4), 337–348.
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley Pub. Co.,.
- Fowler, F. J. (2013). *Survey research methods*. SAGE Publications.
- Furnell, S. M., Gaunt, P. N., Holben, R. F., Sanders, P. W., Stockle, C. T., & Warren, M. J. (1996). Assessing staff attitudes towards information security in a European healthcare establishment. *Medical Informatics*, 21(2), 105–112.
- Gable, G. (1994). Integrating case study and survey research methods: an example in information systems. *European Journal of Information Systems*, 3, 112–126.
- Gefen, D., Rigdon, E. E., & Straub, D. (2011). An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly*, 35(2), iii–A7.
- 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(5), 91–109.

- Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural equation modeling and regression : guidelines for research practice. *Communications of the Association for Information Systems*, 4(October), 7.
- Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. Elsevier Science Ltd.
- Gilmore, H. L. (1974). Product conformance cost. *Quality Progress*, 7(5), 16–19.
- Goel, S., & Chengalur-Smith, I. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19(281–295).
- Goodhue, Dale, L., & Thompson, Ronald, L. (1995). Task-technology fit and individual performance. *MIS Quarterly*, 19(2), 213–236.
- Goodhue, D. L., & Straub, D. W. (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* (2nd Editio).
- Gronroos, C. (1984). *Strategic management and marketing in the service sector*. Krieger Pub Co.
- Gurkok, C. (2014). Managing information security. *Managing Information Security*, (April 2001), 275–311.
- Haeussinger, F. J., & Kranz, J. J. (2013). Information security awareness: Its antecedents and mediating effects on security compliance behavior. In *Thirty Fourth International Conference on Information Systems* (pp. 1–11). Milan.
- Hair, J., Black, W., Babin, B., & Anderson, R. (2009). *Multivariate data analysis* (7th ed.). Prentice Hall;
- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139–152.
- Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, 40(3), 414–433.
- Hair, J., Hult, G., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares - structural equation modeling (PLS - SEM)* (2nd ed.). SAGE Publications, Inc.
- Hair, J., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2013). *A primer on partial least squares structural equation modeling (PLS-SEM)* (1st ed.). SAGE Publications, Inc.
- Harrington, S. J. 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.
- 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(2), 106–125.
- Hess, T., & Hightower, R. (2002). Using equity theory to understand user satisfaction with ERP systems: Extending and advancing the equity-implementation model. *ICIS 2002 Proceedings*.
- Hoffer, J. A., & Straub, Jr., D. W. (1989). The 9 to 5 underground: Are you policing computer crimes? *Sloan Management Review*, 30(4), 35–43.
- Höne, K., & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? *Computers & Security*, 21(5), 402–409.
- Hovav, A., & Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information and Management*, 49(2), 99–110.
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615–660.
- 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. *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*, Paper 132.
- Humaidi, N. (2016). *An investigation of health information system security policy compliance behavior*. University of Malaya - Kuala Lumpur.
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, 31(1), 83–95.
- Ifinedo, P. (2014). Information and management information systems security policy compliance : An empirical study of the effects of socialisation , influence , and cognition.

- Information & Management*, 51(1), 69–79.
- Igbaria, M., Guimaraes, T., & Davis, G. B. (1995). Testing the determinants of microcomputer usage via a structural equation model. *Journal of Management Information Systems*, 11(4), 87–114.
- Ives, B., Olson, M. H., & Baroudi, J. J. (1983). The measurement of user information satisfaction. *Communications of the ACM*, 26(10), 785–793.
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, 34(3), 549-A4.
- Joshi, K. (1990). An investigation of equity as a determinant of user information satisfaction. *Decision Sciences*, 21(4), 786–807.
- Joshi, K. (1992). A causal path model of the overall user attitudes toward the MIS function: The case of user information satisfaction. *Information & Management*, 22(2), 77–88.
- 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, 139–154.
- Kirsch, L. J., & Boss, S. R. (2007). The last line of defense: Motivating employees to follow corporate security guidelines. *Twenty Eighth International Conference on Information Systems*, 1–18.
- Kline, T. J., Sulsky, L. M., & Rever-Moriyama, S. D. (2000). Common method variance and specification errors: a practical approach to detection. *The Journal of Psychology*, 134(4), 401–421.
- Kovacish, G. L., & Halibozek, E. (2003). *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Butterworth-Heinemann.
- Kukafka, R., Johnson, S. B., Linfante, A., & Allegrante, J. P. (2003). Grounding a new information technology implementation framework in behavioral science: A systematic analysis of the literature on IT use. *Journal of Biomedical Informatics*, 36(3), 218–227. <http://doi.org/10.1016/j.jbi.2003.09.002>
- Ladd, J. (1982). Collective and individual moral responsibility in engineering: some questions. *IEEE Technology and Society*, 1(2), 3–10.
- LaRose, R., Rifon, N. J. N., & Enbody, R. (2008). Promoting personal responsibility for

- internet safety. *Communications of the ACM*, 51(3), 71–76.
- Lebek, B., Uffen, J., & Breitner, M. H. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. In *46th Hawaii International Conference on System Sciences* (pp. 2978–2987).
- Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information Security Awareness and Behavior: A Theory-Based Literature Review. *Management Research Review*, 37(12), 1049–1092.
- Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, 10(2), 57–63.
- Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management*, 41, 707–718.
- 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.
- Liao, C., Chen, J.-L., & Yen, D. C. (2007). Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: An integrated model. *Computers in Human Behavior*, 23(6), 2804–2822.
- Limayem, M., & Hirt, S. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems*, 4, 65–95.
- Lin, H.-F. (2006). Impact of organizational support on organizational intention to facilitate knowledge sharing. *Knowledge Management Research & Practice*, 4(1), 26–35.
- Lin, H.-F. (2007). Knowledge sharing and firm innovation capability: an empirical study. *International Journal of Manpower*, 28(3/4), 315–332.
- Maddux, James E.; Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change : A revised theory of protection motivation. *Social Psychophysiology: A Source Book*, 19(January 1983), 469–573.
- Maddux J.E, & R.W, R. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479.
- Mălăescu, I., & Sutton, S. G. (2015). The effects of decision aid structural restrictiveness on

- cognitive load, perceived usefulness, and reuse intentions. *International Journal of Accounting Information Systems*, 17, 16–36.
- Martins, A., & Eloff, J. (2002). IS security culture. In *Proceedings of IFIP TC-11 17th International Conference on IS security (SEC2002)*.
- Mawhinney, H., & Lederer, L. (1990). A Study of personal computer utilization by managers. *Information & Management*, 18(5), 243–253.
- McCumber, J. (2005). *Assessing and managing security risk in IT systems* (2nd editio). Auerbach Publications, ISBN 0849322324.
- McCumber, J. (2007). *Assessing and Managing Security Risk in IT Systems* (2nd editio). Auerbach Publications, ISBN 0849322324.
- Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, 48, 267–280.
- Morton, N. (2004). Understanding attitudes toward online music piracy. *AMCIS 2004 Proceedings*.
- Murray, B. (1991). Running corporate and national security awareness programs. In *Proceedings of the IFIP TC11 Seventh International Conference on IS security*. (pp. 203–207).
- Neumann, P. (1999). Risks of insiders. *Communications of the ACM*, 42(12), 160.
- Newsted, P., Huff, S., & Munro, M. (1998). Survey instruments in information systems. *MIS Quarterly*, (December), 553–555.
- NIST SP 800-100. (2006). Information security handbook : A guide for managers (special publication 800-100). *National Institute of Standards and Technology, NIST*, (October).
- NIST SP 800-50. (2003). Building an information technology security awareness and training program. *National Institute of Standards and Technology, U.S. Department of Commerce*, 50(October).
- NIST SP 800-53 rev4. (2013). Security and privacy controls for federal information systems and organizations SP 800-53 rev 4. *National Institute of Standards and Technology, NIST*.
- Oliver, R. R. L. (1980). A cognitive model of the antecedents and consequences of satisfaction decisions. *Journal of Marketing Research*, XVII(November), 460–470.
- Pahnila, S., Siponen, M., Mahmood, A., Box, P. O., Oulun, F.-, & Siponen, E. M. (2007).

- Employees' behavior towards IS security policy compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*. Los Alamitos, CA: IEEE Computer Society Press., 156–166.
- Peltier, T. R. (2002). *Information security policies, procedures, and standards* (1st ed.). Auerbach Publications.
- Peltier, T. R. (2010). *Information security risk analysis* (3d ed.). Auerbach Publications.
- Peltzman, S. (1975). The effects of automobile safety regulation. *Journal of Political Economy*, 83, 677–725.
- Pfleeger, C., & Pfleeger, S. L. (2006). *Security in computing* (4th ed.). Prentice-Hall.
- Pinsonneault, A., & Kraemer, K. L. (1993). Survey research methodology in management information systems: An assessment. *Center for Research on Information Technology and Organizations*.
- Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, 20(1), 121–139.
- Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27(7–8), 241–253.
- Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, 28(8), 816–826.
- Rogers, E. M. (1995). *Diffusion of innovations* (Fourth). New York: Free Press.
- Rogers, E. M. (2003). *Diffusion of innovation* (5th ed.). Free Press.
- Sagberg, F., Fosser, S., & Saerermo, I.-A. (1997). An investigation of behavioural adaptation to airbags and antilock brakes among taxi drivers. *Accident Analysis & Prevention*, 29(3), 293–302.
- Sarstedt, M., Wilczynski, P., & Melewar, T. C. (2013). Measuring reputation in global markets-A comparison of reputation measures' convergent and criterion validities. *Journal of World Business*, 48(3), 329–339.
- Siponen, M., Adam Mahmood, M., & Pahlila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217–224.
- Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines.

- Journal of the Association for Information Systems*, 7(7), 445–472. <http://doi.org/Article>
- Siponen, M., Pahnla, S., & Mahmood, A. (2007). Employees' adherence to information security policies? an empirical study. *Pacis 2007 Proceedings*, 438–439.
- Siponen, M., Pahnla, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *IEEE Computer Society*, 43(2), 64–71.
- Siponen, M. T. (2000a). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, (Table I), 31–41.
- Siponen, M. T. (2000b). Critical analysis Of different approaches to minimizing user-related faults in information systems security: Implications for research and practice. *Information Management & Computer Security*, 8(5), 197–209.
- Siponen, M. T. (2001). Five dimensions of information security awareness. *Computers and Society*, 31(June), 24–29.
- Siponen, M. T. (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., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-A12.
- Siponen, M., & Vance, A. (2013). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems*, 23(February 2012), 1–17.
- Sliat, R., & Alnsour, M. (2013). Business innovation through knowledge sharing: An applied study on the Jordanian mobile telecommunications sector. *European Journal of Business and Management*, 5(18), 8–18.
- Son, J. Y. (2011). Out of fear or desire? toward a better understanding of employees' motivation to follow IS security policies. *Information and Management*, 48(7), 296–302.
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 34(3), 503-A5.
- Stanton, J. M., Stam, K. R., Guzman, I., & Caledra, C. (2003). Examining the linkage between organizational commitment and information security. *Proceeding of IEEE International Conference on Systems, Man and Cybernetics. Conference*, 3, 2501–2506.
- Stewart, J., Chapple, M., & Gibson, D. (2012). *CISSP: Certified information systems security professional* (6th ed.). John Wiley & Sons Inc.

- Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276.
- Straub, D. W. J., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45–60.
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(December), 441–469.
- Straub, D., & Welke, R. (1998). Coping with Systems Risk : Security planning models for management decision-making. *Mis Quarterly, (404)*. Retrieved from <http://www.jstor.org/stable/249551>
- Theoharidou, M., Kokolakis, S., & Karyda, M. (2005). The insider threat to information systems and the effectiveness of ISO 17799. *Computers & Security, 24*, 472–484.
- Trochim, W., & Donnelly, J. (2006). *The research method knowledge base* (3rd ed.).
- 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.
- Venkatesh, V., & Goyal, S. (2010). Expectation disconfirmation and technology adoption: Polynomial modeling and response surface analysis. *MIS Quarterly, 34*(2), 281–303.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27*(3), 425–478. <http://doi.org/10.1017/CBO9781107415324.004>
- Vlahos, G. E., & Ferratt, T. W. (1995). Information technology use by managers in Greece to support decision making: Amount, perceived value, and satisfaction. *Information & Management, 29*(6), 305–315.
- 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.
- Warman, a. R. (1992). Organizational computer security policy: the reality. *European Journal of Information Systems, 1*(5), 305–310.
- Whitman, M., Townsend, A., & Aalberts, R. (2001). Information systems security and the need for policy. In G. Dhillon (Ed.), *Information security management: Global challenges in the New Millennium* (pp. 9–18). London. <http://doi.org/10.4018/978-1-878289-78-0.ch002>

- Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A protection motivation theory approach to home wireless security. *Twenty-Sixth International Conference on Information Systems*, 367–380.
- 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.
- Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research*, 22(2), 400–414.
- Younghwa, L., & Kozar, K. a. (2005). Investigating factors affecting adoption of anti-spyware. *Communications of the ACM*, 48(11), 72–78.
- Yuan, J., & Jang, S. (2008). The Effects of Quality and Satisfaction on Awareness and Behavioral Intentions: Exploring the Role of a Wine Festival. *Journal of Travel Research*, 46(3), 279–288. <http://doi.org/10.1177/0047287507308322>
- Zeithaml, V. A. (1988). Consumer perceptions of price, quality, and value: A means-end model and synthesis of evidence. *Journal of Marketing*, 52(3), 2–22. <http://doi.org/10.2307/1251446>
- Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, 17(4), 330–340.

APPENDIX A: COVER LETTER

Dear University employees:

Thank you for participating in this survey. I'm conducting an academic research project titled "Information Security Awareness: Antecedents and A User Satisfaction Perspective" as part of a dissertation at Dakota State University.

The purpose of this study is to examine the factors that affect the user's awareness of information security policy and the influence of the user's awareness of information security policy on the user's satisfaction with security practices.

You as a university employee are invited to participate in the study by completing the attached online 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 approximately 15 minutes of your time. Your participation will contribute significantly to the successful completion of this study. Your participation in this study 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, personal information, or other information that may reveal your identity. The collected data will not be used for any purposes other than the research purposes as stated in paragraph 2. When the data and analysis are presented, you will not be linked to the data by your name, title, or any other identifying item. I request information regarding "university name" for the purpose of ensuring this study includes responses from numerous and varying institutions. Your institution's name will not be published.

If you have any questions, now or later, you may contact us at the email address below. Thank you very much for your time and assistance. If you have any questions regarding your rights as a research participant in this study, you may contact the DSU Office of Sponsored Programs at 605-256-5100, irb@dsu.edu.

Yazan Alshboul

Kevin Streff

yaalshboul@pluto.dsu.edu

kevin.streff@dsu.edu

Dakota State University

College of Business and information Systems

ISP Quality

5- I believe the requirements of my organization's information security policy are clear.

Strongly disagree 1 2 3 4 5 6 7
 Strongly Agree

6- I believe the requirements of my organization's information security policy are easy to understand.

Strongly disagree 1 2 3 4 5 6 7
 Strongly Agree

7- I believe the requirements of my organization's information security policy are complete.

Strongly disagree 1 2 3 4 5 6 7
 Strongly Agree

8- I believe the requirements of my organization's information security policy are comprehensive.

Strongly disagree 1 2 3 4 5 6 7
 Strongly Agree

9- I believe the requirements of my organization's information security policy are consistent.

Strongly disagree 1 2 3 4 5 6 7
 Strongly Agree

10- I believe that my organization has high quality information security policy.

Strongly disagree 1 2 3 4 5 6 7
 Strongly Agree

Individual Factors

The individual factors to foster the knowledge of security skills and requirements to develop a security awareness.

Please answer the following questions (from 11 to 18).

Self-Efficacy

11- I have the required skills to fulfill the requirements of my organization's information security policy.

Strongly disagree 1 2 3 4 5 6 7
 Strongly Agree

12- I have the required knowledge to fulfill the requirements of my organization's information security policy.

Strongly disagree 1 2 3 4 5 6 7
 Strongly Agree

13- I can easily comply with my organization's information security policy whenever I have the desire to that.

1 2 3 4 5 6 7

Strongly disagree Strongly Agree

14- I do not need any help in order for me to comply with most of my organization's information security policy.

Strongly disagree ¹ ² ³ ⁴ ⁵ ⁶ ⁷ Strongly Agree

Technology Security Awareness

15- I follow news and developments about anti-virus technology.

Strongly disagree ¹ ² ³ ⁴ ⁵ ⁶ ⁷ Strongly Agree

16- I discuss with friends and people around me Internet security issues or anecdotes.

Strongly disagree ¹ ² ³ ⁴ ⁵ ⁶ ⁷ Strongly Agree

17- I read the news about malicious attacks on Internet users.

Strongly disagree ¹ ² ³ ⁴ ⁵ ⁶ ⁷ Strongly Agree

18- I am aware of the spyware issues and consequences.

Strongly disagree ¹ ² ³ ⁴ ⁵ ⁶ ⁷ Strongly Agree

Information Security Policy Awareness

The employees' knowledge of the security requirements of his organization's information security policy.

Please answer the following questions (from 19 to 23)

ISP awareness

19- I am aware that my organization's information security policy prevents employees from installing their own software on work computers.

Strongly disagree ¹ ² ³ ⁴ ⁵ ⁶ ⁷ Strongly Agree

20- I am aware that my organization's information security policy describes acceptable use of computer passwords.

Strongly disagree ¹ ² ³ ⁴ ⁵ ⁶ ⁷ Strongly Agree

