HOW EMPLOYEES INTEND TO CONTINUE COMPLYING WITH INFORMATION SYSTEMS' SECURITY POLICIES: INSIGHTS FROM INFORMATION SYSTEMS' CONTINUANCE MODEL

A THESIS SUBMITTED TO

GRADUATE SCHOOL OF INFORMATICS

OF

MIDDLE EAST TECHNICAL UNIVERSITY

BY

JAVAD ABED

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE

IN

THE DEPARTMENT OF INFORMATION SYSTEMS

JANUARY 2014

HOW EMPLOYEES INTEND TO CONTINUE COMPLYING WITH INFORMATION SYSTEMS' SECURITY POLICIES? : INSIGHTS FROM INFORMATION SYSTEMS' CONTINUANCE MODEL

Submitted by **Javad Abed** in partial fulfillment of the requirements for the degree of **Master of Science in information systems, Middle East technical university** by,

Prof. Dr. Nazife Baykal _____

Director, **Informatics Institute**

Prof. Dr. Yasemin Yardımcı Çetin _____

Head of department, **Information Systems**

Assoc. Prof. Dr. Sevgi Özkan Yildirim _____

Supervisor, Information Systems, **METU**

Examining committee members:

Prof. Dr. Yasemin Yardımcı Çetin _____

Information Systems, METU

Prof. Dr. Semih Bilgen _____

Electrical and Electronic Engineering, METU

Assoc. Prof. Dr. Sevgi Özkan Yıldırım _____

Information Systems, METU

Assist. Prof. Dr. Aysu Betin Can _____

Information Systems, METU

Assist. Prof. Dr. Pınar Karagöz _____

Computer Engineering, METU

Date: 22.01.2014

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Javad Abed

Signature: _____

Abstract

How employees intend to continue complying with information systems' security policies: Insights from information systems' continuance model

Javad Abed

M.S., Department of Information Systems

Supervisor: Assoc. prof. Dr. Sevgi Özkan

January 2014, 56 pages

Nowadays Information Systems (IS) are crucial for the survival of the modern organizations since they usually hold critical and valuable organizational data. Because of the potential threats like misuse, theft and destruction of the important data, It is obvious that organizations have to use several methods to keep their IS assets safe. In other words, the modern organizations should have a well-established IS security policy to address security issues. As employees are the weakest link in the security chain, having well-established security policies is not enough for solving security problems completely. They should also utilize proper methods for ensuring the employees' compliance with security policies. So investigating the employees' compliance behavior is important issue for IS security management success. Several researchers have studied the compliance behavior by using different conceptual models including technology acceptance model (TAM), theory of planned behavior (TPB), deterrence, neutralization and etc. However, there is no study for investigating continuance of the security compliance. It is very important for organizations that employees comply with IS security policies and continue complying. This study aims to fill this gap on IS security research and to probe the

important factors that lead employees to have continuous security compliance behavior by using IS continuance model. The analysis of data collected from 270 employees in banking organizations shows that employees' perceived satisfaction and perceived usefulness directly influence continuance intention to comply with IS security policies.

Keywords: IS security compliance, IS continuance model, Continuous security compliance, Information security management, ECM-IT

ÖZ

ORGANİZASYON ÇALIŞANLARININ BİLGİ SİSTEMLERİ GÜVENLİK POLİTİKALARINA UYMAYA DEVAM ETMELERİ: BİLGİ SİSTEMLERİ SÜREKLİLİĞİ MODELİNDEN ÇIKARIMLAR

Javad Abed

Yuksek lisans, Bilişim Sistemleri

Tez Yöneticisi: Doç. Dr. Sevgi Özkan Yildirim

Ocak 2014, 56 sayfa

Günümüzde kritik ve değerli kurumsal verileri tuttuklarindan dolayı, bilgi sistemleri (BS) modern organizasyonların yaşamaları için çok önemliler. Çünkü verilerin yanlış kullanımı, çalıntısı ve imhası gibi potansiyel tehditleri olurken , bu kuruluşların BS varlıklarını korumak için çeşitli yöntemler kullanmak zorunda oldukları açıktır. Yani modern organizasyonların, güvenlik sorunlarını çözmek için bir köklü BS güvenliği politikası olmalıdır. Öte yandan çalışanlar güvenlik zincirinin en zayıf halkası olduklarından, güvenlik politikalarına sahip olmak, güvenlik sorunlarını tamamen çözmek için yeterli değildir. Çalışanların güvenlik politikalarına uymaları için uygun yöntem kullanmak gerekir. Yani çalışanların uyum davranışlarını araştırmak, BS güvenlik yönetimi başarısı için önemli bir konudur. Çeşitli araştırmacılar TAM , TPB, caydırma ve nötralizasyon gibi farklı kavramsal modeller kullanılarak uyum davranışını incelemişler, ancak güvenlik politikalarına uyum sürmesini araştırmak için bir çalışma bulunmamaktadır. BS güvenlik politikaları ile uyumun devam etmesi organizasyonlar için çok önemlidir.

Bu çalışma,BS güvenliği alanındaki bu boşluğu doldurmak üzere, BS devamlılık modeli kullanarak çalışanların güvenlik uyum davranışlarının sürekliliğini sağlayan önemli faktörleri soruşturmayı amaçlamaktadır . Toplanan 270 verinin analizi, çalışan memnuniyeti ve fayda algısının doğrudan BS güvenlik politikalarına uymaya devam etme niyetini etkileyebildiğini göstermektedir.

Anahtar Kelimeler: IS güvenlik uyumu, IS sürekliliği modeli, Sürekli güvenlik uyumu, bilgi güvenliği yönetimi, ECM-IT

This thesis is dedicated to:

My Family

ACKNOWLEDGMENTS

First of all, I want to thank to my Thesis supervisor Dr. Sevgi Özkan for her valuable advices and mentoring during my MSc study. I really appreciate her efforts to make me familiar with IS research.

I am very thankful to my family for their continuous support during my whole life.

Finally, I would like to thank to the faculty members of Information System Department, especially Professor Yasemin Yardımcı Çetin for her support from the beginning of my MSc study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CFA	Confirmatory factor analysis
ECM	Expectation confirmation model
IS	Information Systems
PLS	Partial list squares
ISSP	Information systems security policies
IT	Information technologies
SBT	Social bond Theory
SCT	Social cognitive theory
SEM	Structural equations modeling
TPB	Theory of planned behavior
TAM	Technology acceptance model
UTAUT	Unified theory of acceptance and use of technology

CHAPTER I

INTRODUCTION

This chapter contains a brief explanation of IS security compliance and IS continuance theory. Furthermore, it contains objectives of this research, study design, research questions, research scope, significance and the structure of thesis.

1.1 Introduction to the IS security compliance and IS continuance

Information systems are one of the most important assets of modern organizations because they usually deal with the critical organizational data. Nowadays because of the complex operating environment, organizations need to invest heavily in information systems (Ifinedo, 2007). On the other hand, there are variety of unwanted or intentional threats to the IS information security including misusing, theft and destruction of data. By considering that in the last decade, information security incidents have increased significantly (M. Siponen, 2013) appropriate information security methods are compulsory for organizations. In order to address these issues various security technologies like firewalls, proxies and content monitoring systems are widely used. These technologies offer just technical solution for information security problems and usually they are not enough for the comprehensive protection of IS assets (T. Herath, 2009) (Rhodes, 2001) (A. Vance, 2012). The reason is that organizations should consider socio-organizational aspect for gaining the desired output in information security management issues. It means that they should focus on individuals as well as on technical tools for achieving complete solution for the information security concerns. For instance, if we consider that an organization utilizes a strong firewall, but its employees do not feel comfortable with this technology or resist to use it the information security cannot be assured in that organization. It is clear that focusing on advance security technologies should be alongside the focusing on individuals and other organizational parameters like environment. So obviously organizations should consider multi-perspective methods to protect their valuable IS assets and address information security problems (T. Herath, 2009).

Organizations often invest heavily just on technological or technical aspects of information security solutions. However, failures related to the information security breaches and incidents are still the most important problem for them (Ifinedo P. , 2012) (B.-Y. Ng, A. Kankanhalli, Y.C. Xu, 2009). The most important reason for this issue is that employees are the weakest link in the security chain and actually they are potential threats within the organization (J.M. Stanton, 2005). Figure 1 illustrates the potential threats to the sensitive organizational data.

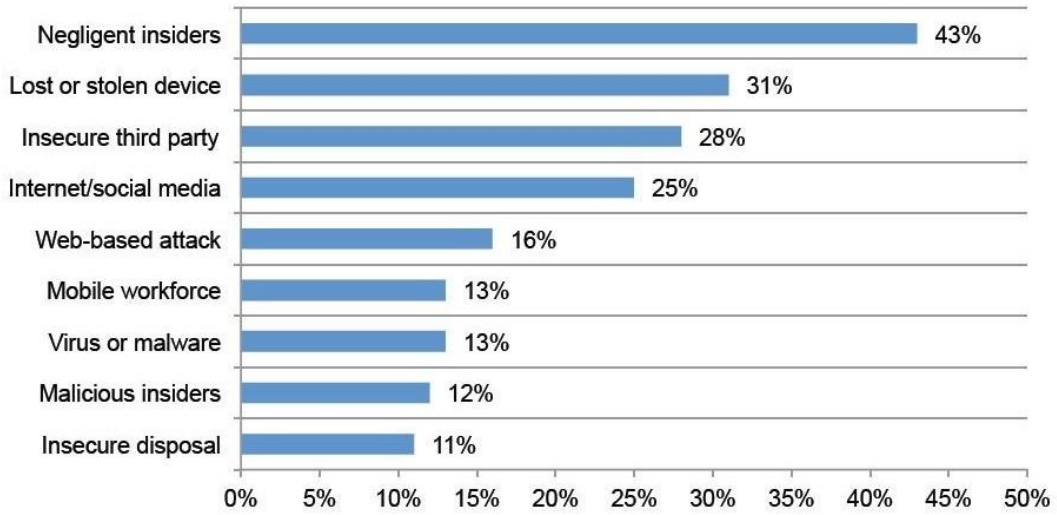

Figure 1-potential threats to the sensitive organizational data (IBM, 2012)

We can come to the conclusion that organizations must focus on the behavioral aspects of their employees and this is the inseparable part of information security management. Obviously, organizations need to design an approach or a function to influence the behavior of their employees. So it is necessary to have a comprehensive and multi-prospective framework that includes the behavioral aspects of employees alongside the technical aspects, resources, guidelines, requirements and rules for ensuring the security of IS assets. This framework is IS security policy (ISSP). A well-established ISSP usually contains sections like security goals, security strategy, rules and responsibilities, classification and control of assets, access control and continuity planning. On the other hand, there are well-established security standards like BS7799 or GASSP that specify uniform methods, rules and actives to implement policies.

For achieve success from ISSP it is important to study the behavior of employees because without their compliance the ISSP will not be fruitful. There are several studies in IS filed that investigate the employee's compliance behavior with the ISSP (e.g. (Bulgurcu et al., 2010) (T. Herath, 2009) (Ifinedo P. , 2012) (A. Vance, 2012). These studies help to know how the intention to comply with ISSP or intention to resist with ISSP can be generated in employees. It is obvious that deploying new IS/IT in organization just as new ISSP should be with the anticipation of its potential users' behavior. It means that if an organization deploys a new information system and if the potential users resist using it or after initial

acceptance they discontinue using it, the new IS will be unfruitful for that organization. From the adoption perspective studies are divided in to two stages including pre adoption or initial acceptance of new IS/IT and post adoption or continuance usage of IS/IT.

This study uses the IS continuance model for investigating the continuous compliance intention of employees. This model examines the continuous intention of IS/IT users and indicates the main constructs that make such intention in the users (Bhattacherjee, 2001). Figure 1 illustrates the IS continuance model.

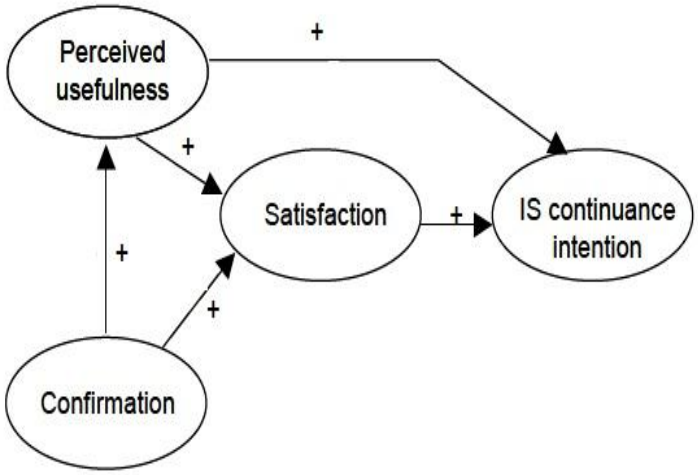

Figure 2- IS continuance model

As you can see in figure 1 the constructs of the IS continuance model are Perceived Usefulness, Confirmation of Expectations, Satisfaction and finally, IS continuance intention. This model integrates technology acceptance model (TAM) and expectation confirmation theory (Bhattacherjee, 2001). TAM is related to the initial acceptance of IT/IS, but has some constructs like Perceived Usefulness that can predict the continuance usage of information systems (Davis, 1989). The expectation confirmation theory is related to consumer repurchase behavior in marketing field (Oliver, 1980). After proposing this model, different studies by utilizing it, have examined the individual's post adoption behavior in different contexts like e-government, healthcare, e-learning and etc. This model is widely used among IS researchers and its usage is expanding over the last years (Islam, A.K.M. Najmul and Mantymaki, Matti).

Perceived Usefulness conveys the user conception that the information system will be useful for him/her and involves consideration like job performance. Confirmation means that the IS user feels that his/her expectation from new IS are confirmed during the usage stage. Both of Perceived Usefulness and Confirmation positively influence user satisfaction from the IS usage. Positive influence means that if perceived usefulness or confirmation increases increase, user satisfaction from IS usage will increase too. Furthermore, Confirmation of pre-adoption expectation positively influences Perceived Usefulness. Finally, according to the IS continuance

model Perceived Usefulness and Satisfaction positively influence the IS continuance intention. It means that determinants of continuance intention to use information systems are Perceived Usefulness and User Satisfaction (Bhattacherjee, 2001) .

The initial acceptance of IS/IT is very important toward IS/IT success, however, the continuous usage determines the long term success of IS (Bhattacherjee, 2001). So promoting continuous IS usage and preventing the stoppage of IS usage is a key point in IS success. Furthermore, it is important to mention that users beliefs and attitudes change during the usage period (Bhattacherjee, A. & Premkumar, G, 2004). Regarding that IS continuance model investigates users post adoption behavior and determines the main constructs those lead to continuance intention to use information system or information technology, we can utilize this model to investigate continuance employee's intention to comply with ISSP. Just as IS usage, compliance intention can be changed over the time and should be continuous for ensuring about IS success. Prior researchers have focused just on utilizing IS pre adoption theories, but investigating the continuous compliance intention is unclear.

1.2 Study Objectives

Understanding that how employees continue to comply with ISSP and investigating the continuous intention by utilizing the IS continuance model, is the primary objective of this study. This research aims to find major determinants of continuous compliance intention by accomplishing an empirical study.

1.3 Research Questions

This study tries to answer following questions:

1. Does confirmation of initial compliance expectations affect Perceived Usefulness of employees and is there a relationship between confirmation and perceived usefulness?

2. Does confirmation of initial compliance expectations affect satisfaction of employees from complying with ISSP and is there a relationship between confirmation and satisfaction?

3. Does perceived usefulness affect satisfaction of employees from ISSP compliance and is there any relationship between perceived usefulness and satisfaction of employees?

4. Does Perceived usefulness affect continuance intention to comply with ISSP and is there any relationship between perceived usefulness and continuance intention to comply with ISSP?

5. Does satisfaction of employees from compliance with ISSP affect continuance intention to comply with ISSP and is there any relationship between satisfaction and

continuance intention?

6. Is the IS continuance model a good predictor of employees continuous compliance behavior?

1.4 Scope

Although there are several theories for exploring IS continuance, this study, uses the widely used theory for exploring the employees continuous intention to comply with ISSP and it is limited to constructs of IS continuance model. Data is collected for examining the proposed model, further investigation and analysis from 270 employees of several banking organizations in Iran.

1.5 Significance of the study

A review of prior research in the security compliance field reveals that different studies have conducted to explore initial ISSP compliance; however, there is no study in post compliance behavior of employees. This means that this study can initiate a new trend in security compliance research.

The importance of the IS security policy for protecting sensitive and critical IS assets and ensuring the information security is obvious, but, the functionality of policy completely depends on compliance of employees. This study helps to gain success from security policies and ensuring about functionality of information systems security policies.

1.6 Structure of the Research

Figure 3 illustrates the research progression from the beginning (literature review) to the end (Conclusion).

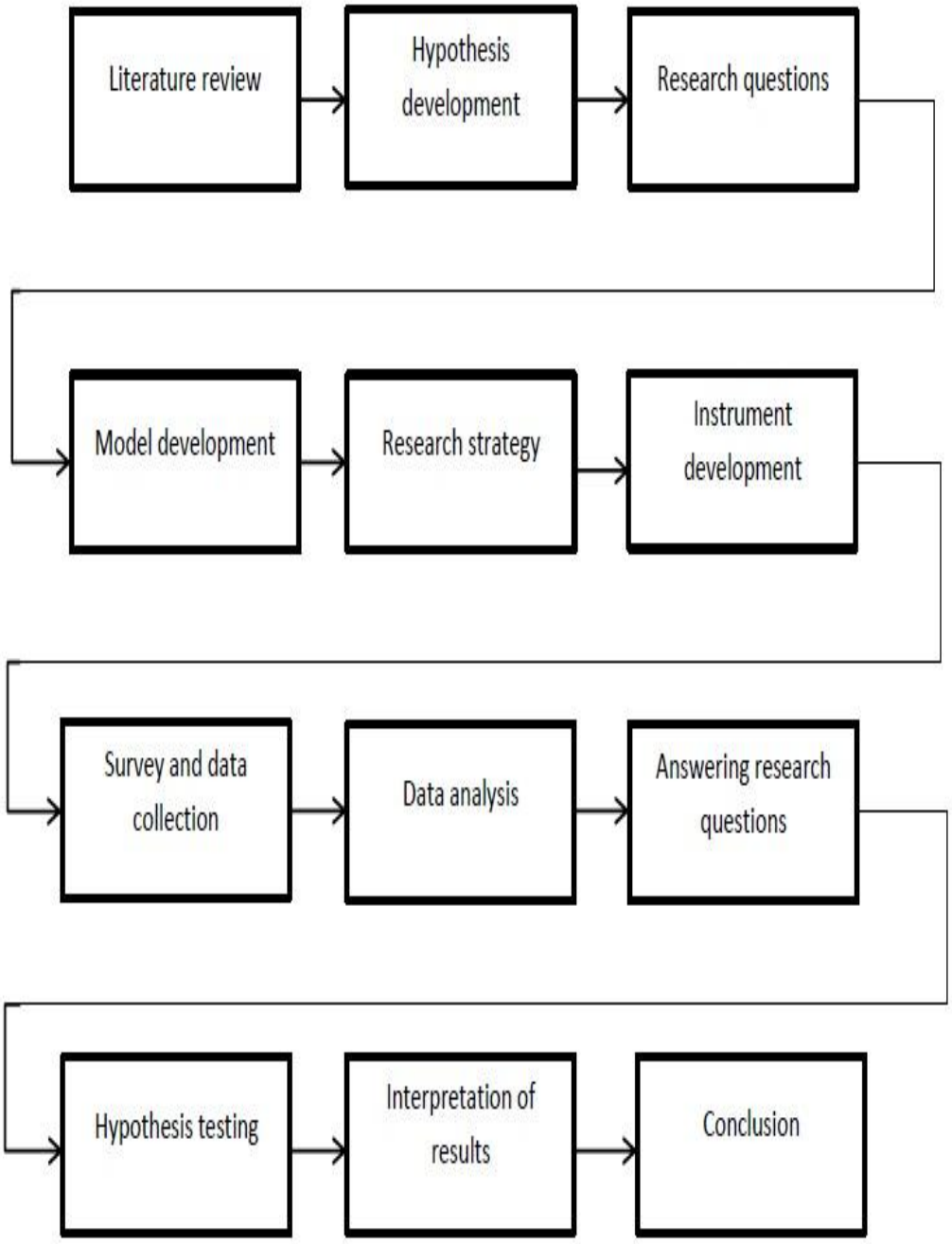

Figure 3- Study progression

1.7 Overview of Contents

This study contains six chapters. Chapter 1 includes a brief introduction to the ISSP compliance as well as IS continuance behavior and IS continuance model. It also includes research objectives, research questions, scope of the thesis, research significance and finally, the overall structure of the research.

Chapter 2 reviews the prior research in IS security compliance field. The common types of conceptual models for studying security compliance are discussed in this chapter.

Chapter 3 contains hypothesis development and proposing conceptual model for ISSP continuous compliance.

Research methodology is given in Chapter 4. In addition, chapter 4 consists of developing measurements and survey items, testing the measurements and data collection.

Chapter 5 includes choosing data analysis method of this research and analysis of data with an appropriate statistical method. This chapter also contains the results of data analysis.

The discussion of data analysis results, implications for future research and for managers and finally, conclusion of this study are in Chapter 6.

CHAPTER II

Literature Review

2.1 Methodology

For literature review of this study it is necessary to overview all of the related previous research works. For this purpose, a pool of candidate literature is collected without limitation to any specific academic databases. So in the first step a search was done in all of the available academic databases including Business Source Premier, Springer Link, Scopus, IEEE Explore, ACM Portal and ISI Web of Science. In addition, Google Scholar search engine is used to ensuring comprehensive retrieval of research works. The keywords that are used in searching candidate research work are: "IS continuance model"; "Continuance intention"; "Information Security Policy"; "Information Systems Security Policy"; "Security compliance"; "ISSP" and "security policy compliance". The results indicated that there is no research work related to continuous compliance.

The resulting research works were chosen for review if they were completely relevant to the ISSP and compliance. On the other hand, for refining the research poll, studies that could help our understanding about integration of conceptual models with intention to ISSP compliance were chosen. The other criteria for choosing the candidate articles were their scientific significance. This means that they should include complete research work including well-described research methodology, conceptual model, data analysis, results of analysis(correlation matrix and reliability values) and finally, the confirmation of the majority of the hypothesis that were newly developed by them. Figure 3 illustrates the literature review methodology.

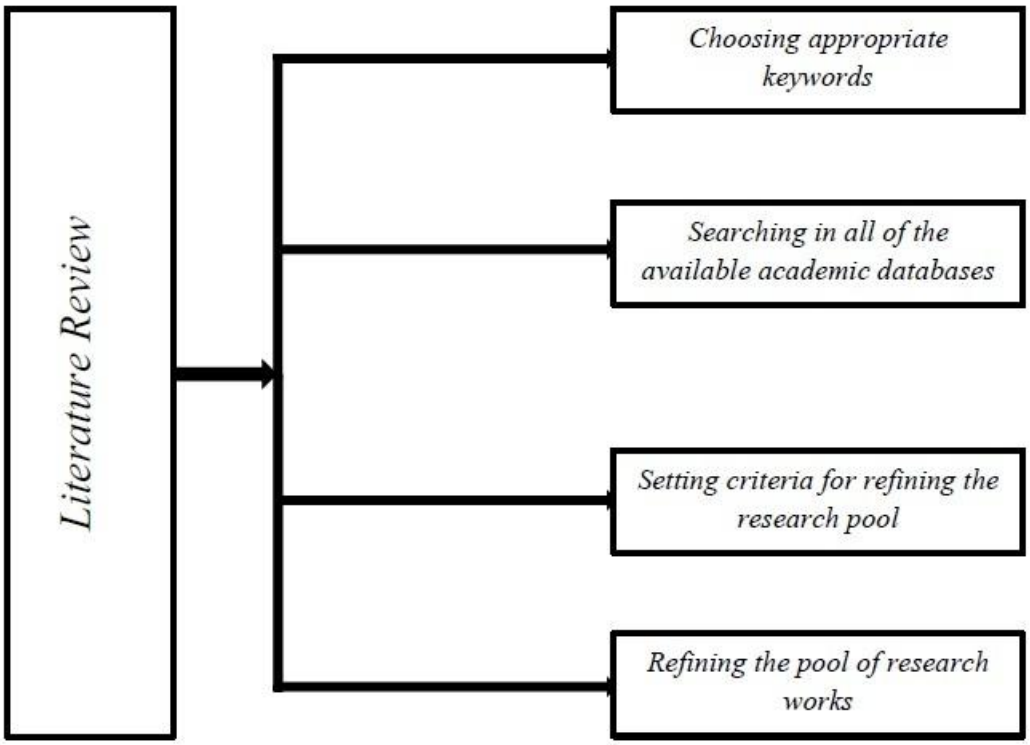

Figure 4- Methodology of review

2.2 Review of Acquired Research Works

Criminals usually try to attack IS assets through denial of service, fraud, web hacking and other attacks for the personal, political or financial purposes (Smith et al., 2010). So this motivates organizations to utilize information security standards for assuring about IS assets' security. In majority the of the government organizations, employees are mandates to comply with the information security standards. Smith et al. in their study investigate the mandated compliance in small, medium and large government agencies with Canonical action research. They have used Clegg's Circuits of power framework (Clegg, 1989) to understand power, resistance, norms and cultural relationships during the compliance. Smith et al. show that government organizations should have a strategy based on the size of organizations' sub-units in order to mandate standard compliance (Smith et al., 2010). In addition, insufficient resource allocation and lack of senior management input prohibit mandated standard accreditation and cultural biases and norms lead employees to resist with the security standard. We can extract an important point from Smith et al. study that in government organizations, employees who decide to comply with security standard or policy maybe because of cultural biases and norms can discontinue to compliance.

Employees' violation of the information security policies is a key problem in organizations (Ernst & Young, 2008). The most important reason of this violation is the negligence or ignorance of IS security policies in employees' part (Stanton et al., 2005). For overcoming this problem use of sanctions that are derived from

deterrence theory are widely used by IS scholars (M. Siponen & A. vance, 2010) (Kankanhalli, 2003) (Tudor J. K., 2000). These sanctions can be formal or informal. The informal sanctions consist of specifying punishments or penalties for violators of security policies. Informal sanctions are related to the social consequences of security policy violation. For instance, if an employee violates the security policy he or she would face with the disapproval of friends or co-workers. Several studies indicate that using sanctions are useful for IS security policy compliance and sanctions decrease the policy violence (Straub D. W., 1990) (Kankanhalli, 2003). The important point in using sanctions is that there should be a clear statement of penalties and punishments. In addition, the severity of punishments should be specified explicitly based on the factors such as the education level of employees. Siponen & Vance in their study mention that sanctions are not enough for ensuring about the security compliance (M. Siponen & A. vance, 2010). Fear of sanctions cannot always interpret as a reason of compliance. Employees may use neutralization techniques in order to comply with the ISSP (Piquero et al., 2005) (Sykes, G., and Matza, D., 1957).

Figure 4 illustrates the proposed model of Siponen and Vance. This model integrates neutralization technics with sanctions.

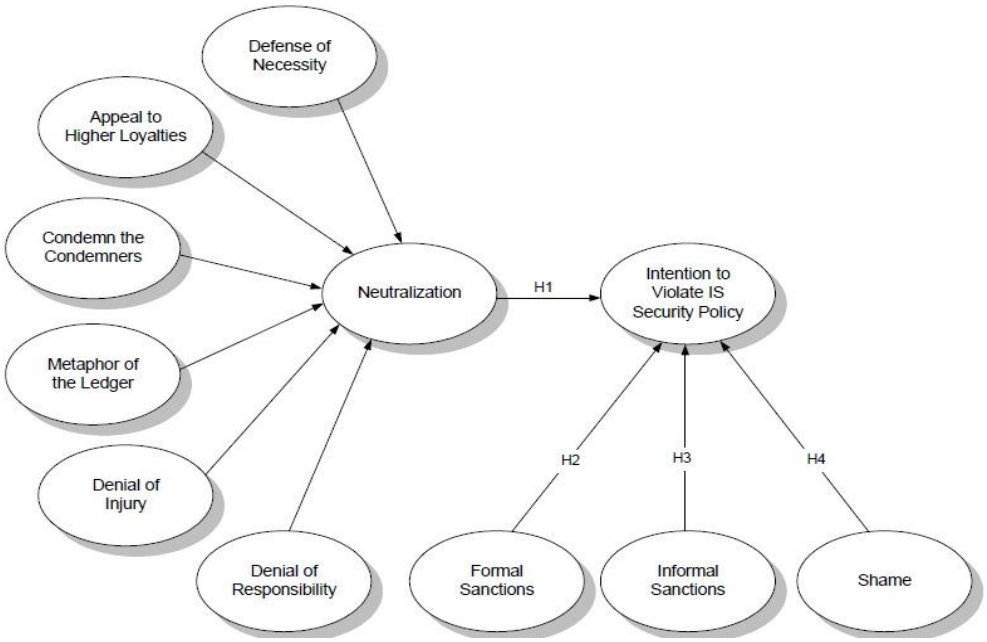

Figure 5- Integration of sanctions and neutralization techniques (M. Siponen & A. vance, 2010)

The explanations for each of neutralization techniques are given below:

Defense of necessity: This technique refers to a situation that an employee violates the security policy but, after that he or she does not feel guilty because he or she believes that breaking the rule and policy violation is necessary and there is no other choice (Piquero et al., 2005) (Minor W. W., 1981). For example, some employees claim that the time is not enough for compliance in specific deadlines and they have to violate or resist security policies.

Appeal to higher loyalties: In organizations, some employees might justify the violation of the security policy by arguing that he or she can get higher order or much value by policy violation. For instance, in competition with other employees and in competitive environment some employees violate the policy in order to get his or her work done (Siponen M., and Iivari J., 2006).

Condemn the condemners: In this case an employee breaks the policy law and believes that the law is unjust or unfair. For instance, in an organization part that security consideration is higher than some other parts, employees may think that security laws are unfair (Parker D. B., 1998).

Metaphor of the ledger: An employee may feel that he or she has done many good acts and after that he or she has a right to do some bad acts (Piquero et al., 2005). It means that for instance, in an organization an employee has complied with security rules for several years but, he or she believes that some policy violation are justified and reasonable.

Denial of injury: In this case, an employee thinks that violation of some policies does not harm organizations and he or she can break some rules without damage to the company (M. Siponen & A. vance, 2010) .

Denial of responsibility: Some employees justify the policy violation by arguing that the policy rules are out of their control or responsibility. This means that they believe some rules are under responsibility of other employees.

In the Siponen & Vance model there is another construct as shame. This construct refers to a situation that inhibits employees from violating the security policy. When friends or co-workers of an employee who has violated the ISSP know about the violation, this causes the shame feeling in that employee (Eliason, S. L. and Dodder R. A., 1999).

Regarding that fear of sanctions are not only indicators of ISSP, generally based on Siponen & Vance model, It can be understood that neutralization techniques that are explained above alongside with shame are the main reasons or indicators of policy violation behavior in organizations.

Persuasive communication is one of the other effective methods for the security compliance within organizations. Persuasive communication can affect employees' attitudes, intentions and behavior (Fishbein M. and Ajzen I., 1975). For instance, organizations can use persuasive messages within them to help to the compliance of end users and this can be effective in security training, awareness programs and other communication materials (Warkentin & Johnston, 2010). These messages should contain some kinds of threat because they should inform employees about the potential damage to organization and employees in case of security policy violation. These elements of threat are known as fear appeals (Warkentin & Johnston, 2010). Fear appeals should comprise factors that employees by using them can be sure that can overcome threats and do just as recommended manner. Figure 6 illustrates the Warkentin & Johnston's model that indicates threat, efficacy and social influence as determinants of behavioral intention to comply with ISSP.

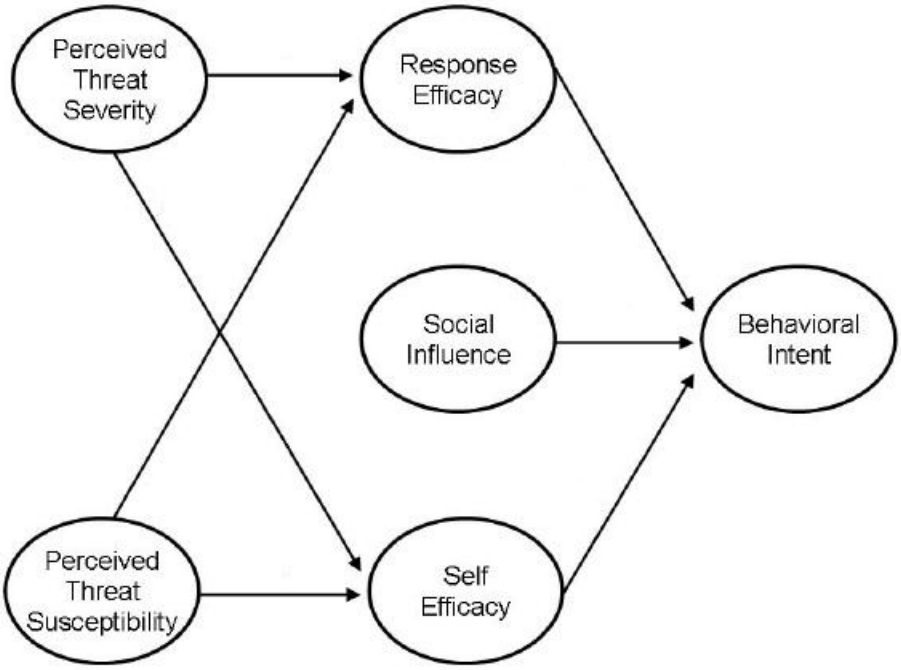

Figure 6- Fear appeals and IS security compliance intention (Warkentin & Johnston, 2010)

Threat is divided in to two perceptions. When an individual becomes aware of potential threats, he or she specifies a severity to that threat and on the other hand, specifies a possibility degree to that threat (Witte et al., 1996) (Witte, 1992). The efficacy is also divided in to two perceptions as efficacy of the pervasive massage contents and the recommendations and the efficacy of the employee to act similar to the recommendations. We can see that threat perceptions and can affect efficacy perceptions and consequently efficacy perceptions can affect behavioral intention to security compliance. Social influence which is the degree that an individual emphasizes the influential peoples' conception about the outcome of the policy violation, directly affects the intention to comply with ISSP. Another approach for investigating the employees' behavior in security compliance field is considering that their attitudes can affect the compliance intention (Bulgurcu et al., 2010).

Beliefs about the results of compliance can influence employees' attitudes toward ISSP compliance. These beliefs can also be about the benefits of ISSP compliance. For instance, employee always evaluate the cost of compliance and non-compliance or outcomes of the compliance like job performance, safety and satisfaction or non-compliance outcomes like sanctions and vulnerabilities (Bulgurcu et al., 2010). On the other hand, persuasive messages that are mentioned earlier can be as part of the awareness program. Awareness which generally contains different parts like training, can also affect the beliefs and attitudes of employees. There is also another type of awareness such as awareness that is obtained from the outside of the organization or general awareness. Bulgurcu et al. in their study indicate that beliefs about outcomes affect beliefs about overall assessment of consequences. They also mention that these beliefs influence the attitude of employees and consequently the

attitudes toward ISSP compliance alongside with normative beliefs (social influence) and self-efficacy affect intention to comply with ISSP (Bulgurcu et al., 2010). On the other hand, information security awareness (ISA) directly affects the employees' attitudes toward ISSP compliance. Generally we can say that security awareness affects beliefs, beliefs affect attitudes and finally, attitudes affect intention to comply with ISSP. Figure 7 presents the model proposed by Bulgurcu et al.

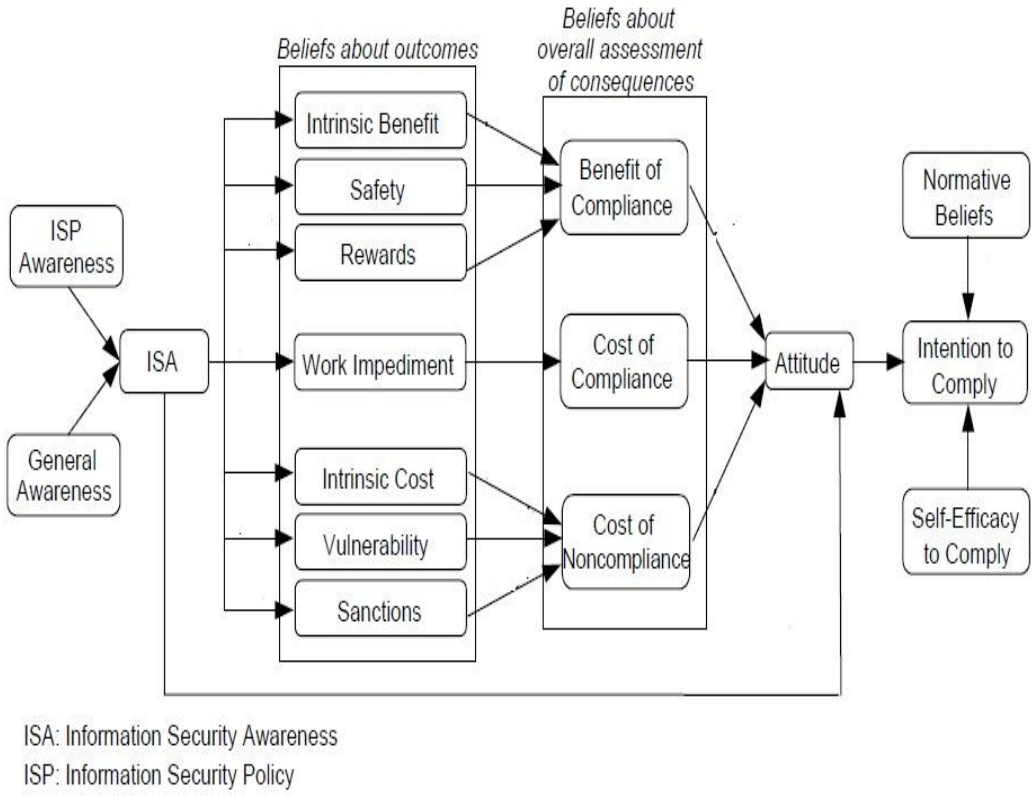

Figure 7-Beliefs, attitudes and ISSP compliance (Bulgurcu et al., 2010)

In some kind of organizations such as the government organization that compliance with ISSP is mandated, punishment is the key point in success of ISSP. It is important to know that the punishment should be managed based on the several factors, including justice and behavior of the employees (Y. Xue et al., 2011). Furthermore, there may be a difference between claimed punishment and actual punishment in organizations. For instance, in punishment statement there might be a claim that if an employee does a certain act, he or she will be fired, however, if he or she actually does that certain act the organization does not want to fire him or her. On the other hand, as it is mentioned earlier employees justify punishments for ISSP violation. If in their view punishments are reasonable the chance of compliance will increase. If they believe that the punishments are not reasonable, they would use a neutralization technique (Condemn the Condemners) ISSP violation. Over the several years, IS scholars have studied adoption behavior of IS/IT users and The TAM model is widely used for this purpose and there are several integrations and

extensions to this model. Xue et al. in their study also have used TAM model in order to explain the ISSP compliance behavior. This model is the most similar to the proposed model of this thesis because it uses satisfaction construct to explore compliance intention. However, this model does not consider the continuous intention and it just focus on initial compliance. In addition, it has perceived ease of use construction that generally influences initial intention. As you can see in Figure 8 actual punishment constructs alongside with Perceived usefulness, perceived ease of use and satisfaction directly affect intention.

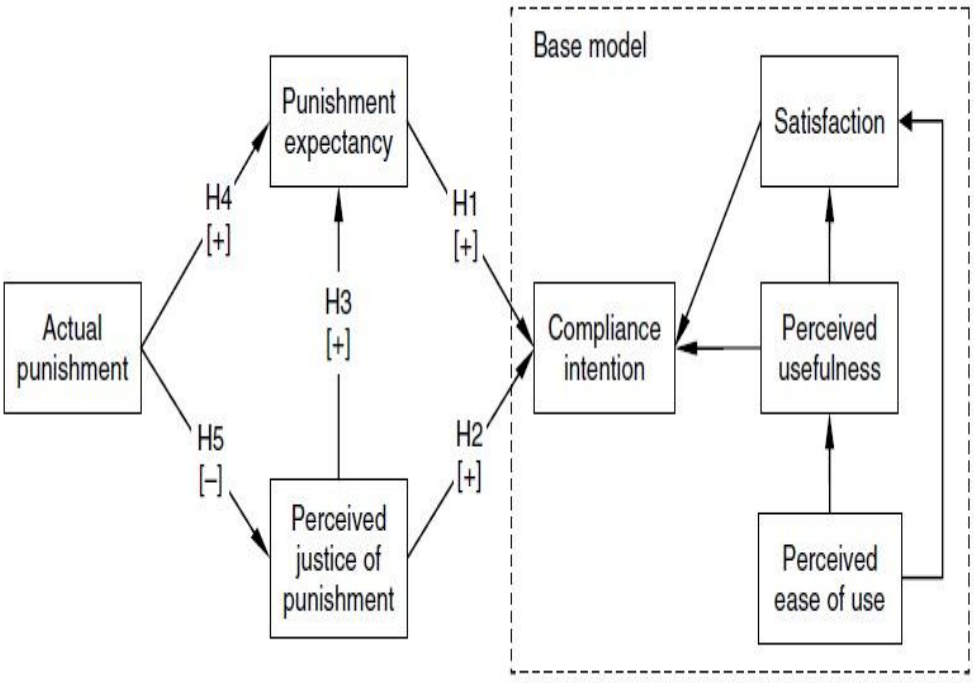

Figure 8- Integrating TAM and Punishment constructs (Y. Xue et al., 2011)

One of the useful models for studying the security behavior of the employees is the protection motivation theory. This model is extended form the health related beliefs' model in psychology filed and is developed by Rogers (R. Rogers, 1983). PMT is a powerful model for understanding the fear appeals. It means that PMT helps to the investigation employees' behaviors that are related to protecting themselves from potential threats (Anderson & Agarwal, 2010). As we saw previously threat consists of two conceptions namely as severity and susceptibility.

Also there are two constructs those refer to the efficacy. Combining the PMT and theory of planned behavior can be a good indicator of compliance behavior (Ifinedo P. , 2012). In addition, this can also be the indicator of none compliance behavior that is a different aspect of security compliance.

Theory of planned behavior (TPB) like TAM is widely utilized by IS scholars in order to explore IS usage behavior. TPB includes three parts including: attitudes, behavioral control and subjective norms (Ajzen, 1991). Attitudes refer to the feelings that might be positive or negative about the behavior. Behavioral control

describes user perception of difficulty of behavior and finally, subjective norms explain the perception of user about the other people's feeling about the behavior. So this model also can be used in the field of security behavior. Obviously the behavioral control, attitudes and subjective norms Influence the compliance intention and security behavior of the employees. Ifinedo in his study integrates the TPB and PMT and shows that the constructs of these two models are strong indicators of security behavior. Figure 9 illustrates the TPB and PMT integration for studying ISSP compliance intention.

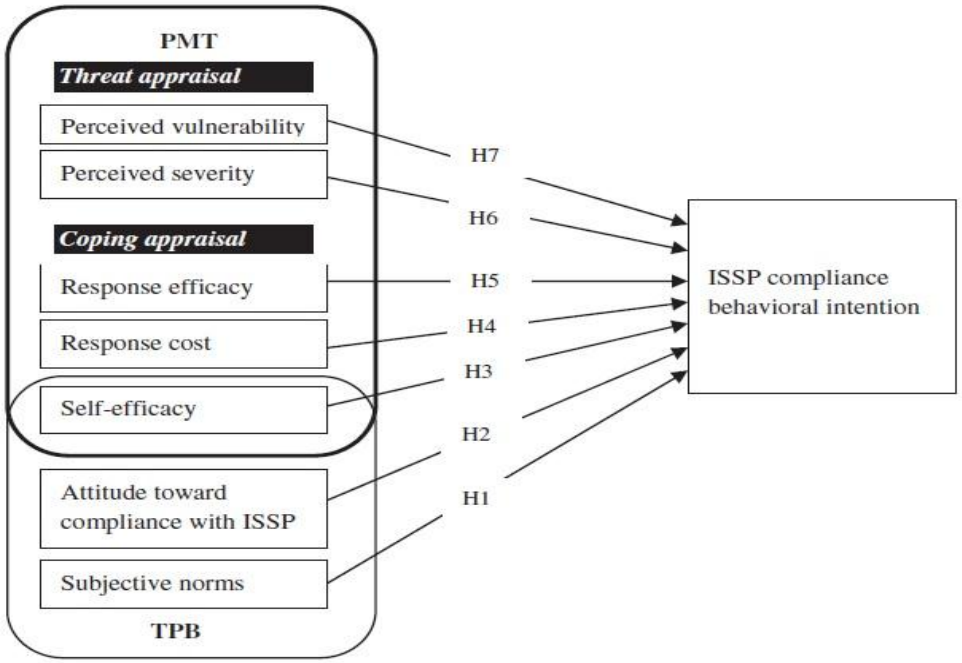

Figure 9- TPB and PMT integration (Ifinedo P. , 2012)

A different prospective that we can consider in order to describe the behavior of employees, is that personalities play an important role in shaping behaviors. Indeed, each of employees has special and different personality and this causes to shape special attitudes and behaviors. So considering the personalities is crucial for successful ISSP compliance. Beside personalities, organization culture strongly affects employees' behavior (Furnel & Rajendarn, 2012). For instance, employees of an organization may completely comply with the ISSP policy; however, in another organization that has a different culture employees may violate the policies. So we should not neglect the prominent effect of organization culture and personalities of employees.

An individual might have a variety of interactions in his or her workplace including interaction with managers, co-workers, colleagues and groups (Furnel & Rajendarn, 2012). Each of these factors can influence security behavior of employees. For instance, in different groups, various values or cultures may exist. In addition, an employee can have personal benefits or can consider group benefits. In figure 10, we can see all of the stated factors as indicators of security behavior.

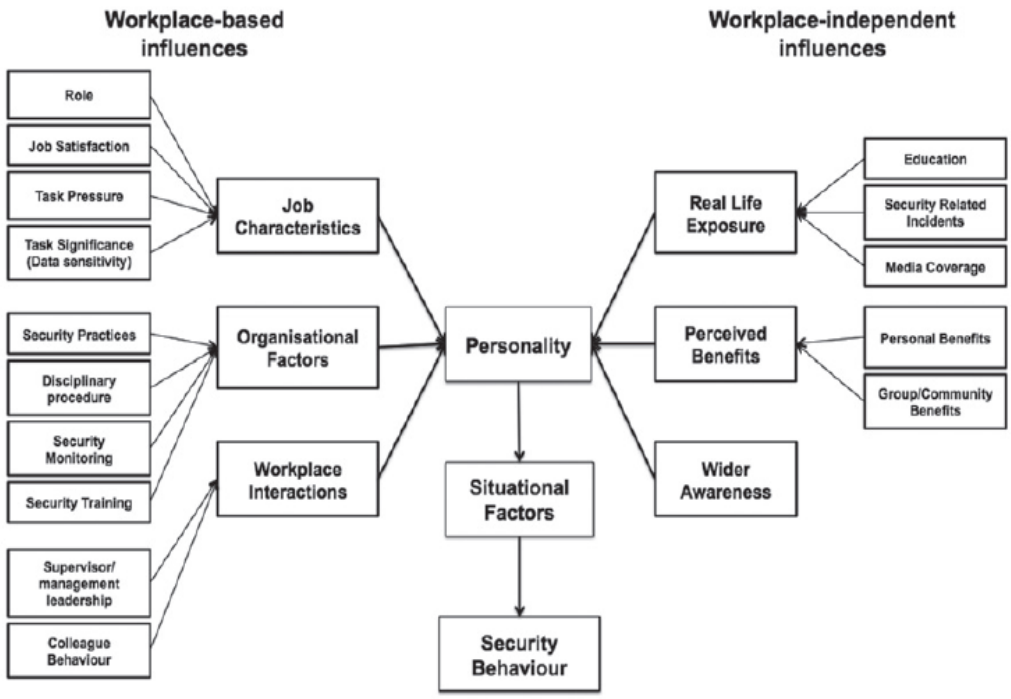

Figure 10- Security behavior indicators (Furnel & Rajendarn, 2012)

This model uses factors those are related to the workplaces and factors those related to the outside of workplaces. All of these constructs influence the personality of employees. Consequently, personalities affect factors that always don't exist. It means that there might be a situation that an individual with the same attitudes and personality acts differently. Finally, situational factors can be determinants of security behavior.

Control elements are critical for determining behavior aspects. For understanding controls it is useful to know formal and informal controls. As it is discussed earlier subjective norm or social influences can directly affect the intention of employees. These factors are the informal type of the controls (Cheng et al., 2013). Social influence can be divided into two categories namely as social pressures and social bonds. Social pressures refer to the influence of the co-workers or other influential people's view on the employees' beliefs. Social bond is originated from social bond theory in criminology field (Hirschi T, 1969).

Based on (Hirschi T, 1969) study people are most reluctant to comply with the rules of their groups. So in ISSP context, we can conclude that employees those have strong links with their groups can violate ISSP due to the rules of groups. Furthermore, based on this model we can conclude that employees that have dependencies in their relationships with co-workers, managers and groups may have different type of attitudes or intentions. Figure 11 shows the relationship of the all factors that are mentioned above.

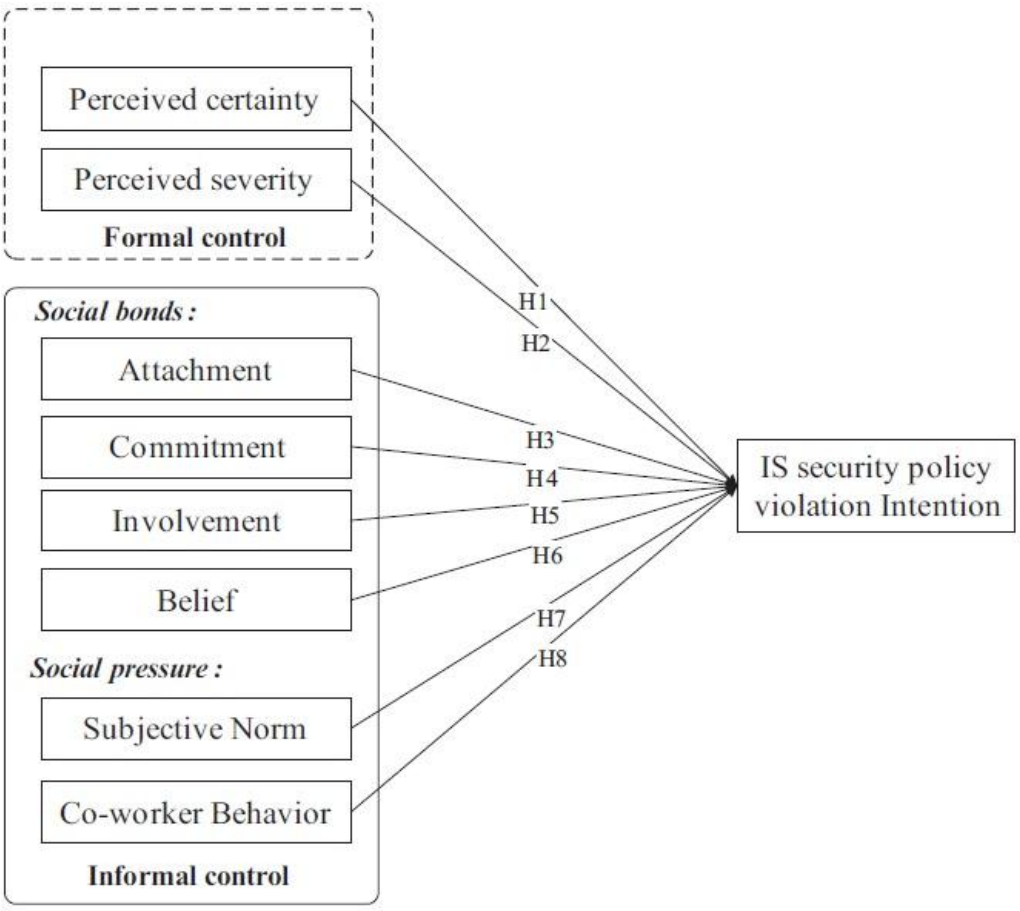

Figure 11- Controls and violence intention (Cheng et al., 2013)

Figure 11 illustrates that all of the control factors, including formal and informal types, can directly persuade employees to violate ISSP.

Internet usage policies are the important part of ISSP because organizations might face with serious attacks through internet. In this contest new elements such as identification and risk can play important role in security behavior (Li et al., 2010).

Organizations should assess potential risks in internet usage and then they should utilize an appropriate method for awareness of employees. By regarding the internet security risks, employees may consider some benefits from violation of internet usage policies. So these benefits may overcome risks. In this case employees believe that they can neglect risks for achieving benefits (Li et al., 2010).

We can infer that organizations must explicitly analyze both of the risks and profits for the purpose of investigating employees' ISSP compliance behavior. Cost-benefit analysis can help organizations to assess potential risks and benefits of the internet usage. Furthermore, risks include both of potential threats of internet usage and detection or sanction threats. It means that violating acts of the policy may have detection or sanction consequences. Figure 12 depicts the relationships among risks, benefits, personal norms and intention.

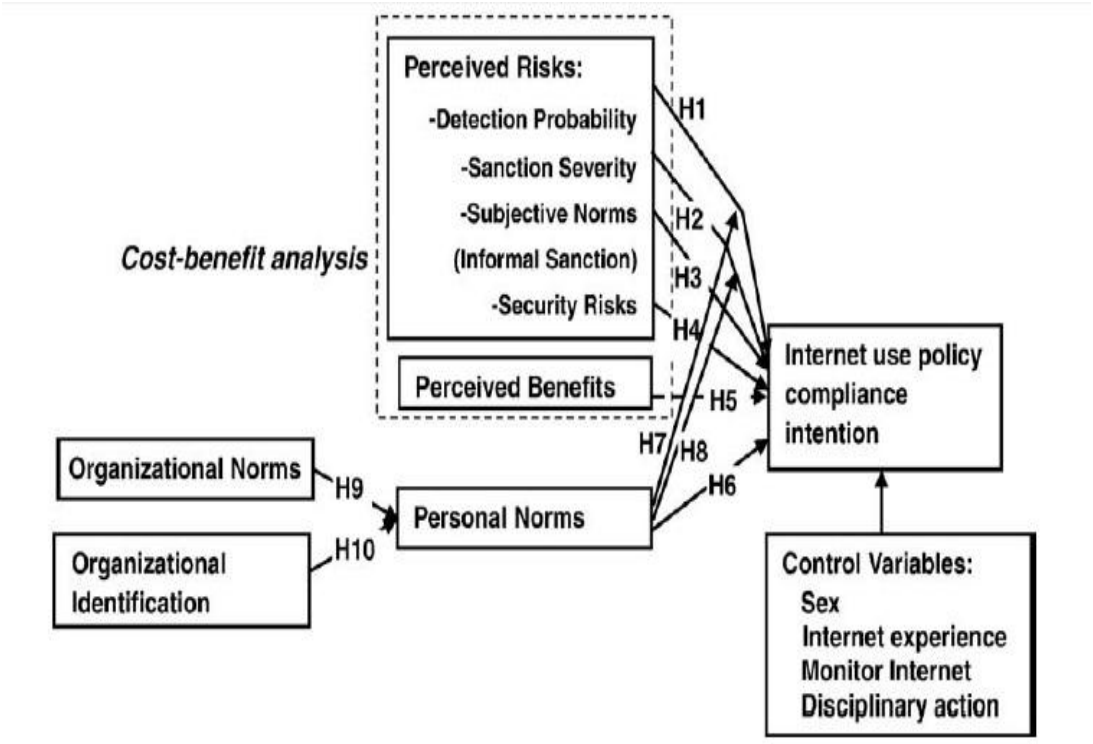

Figure 12- Risks, controls and control variables (Li et al., 2010)

This model is proposed for internet security compliance and we can see that personal norms alongside with the risks, benefits and control variables directly affect intention to comply with the internet use policy. In addition, sanctions and detection risks can be affected by personal norms and (Li et al., 2010). This also confirms the importance of cost benefit analysis in order to analyze risks and benefits.

Exploring the behavior of the employees is very complex. There are several studies and research works those have described the security behavior and intention from different views. This is because of complexity of the human behavior and variety of human behavior perspectives is still a mystery. This study has stated several conceptual models and factors that investigate the ISSP compliance intention however; there are also other important factors like habit.

Every employee has special habits. Habits include routine and repetitive behaviors. These behaviors are usually constant in a remarkable period of time and they can influence other behavior. So habits can be good indicators of ISSP violation or compliance behavior (Vance et al., 2012).For instance, assume that an employee has a habit of password changing frequently. Thus, this employee can easily comply with the password security policy. In addition, habits can influence perception of employees about threats or efficacies. For example, if an employee breaks the policy rules repeatedly and this becomes a habit for him or her, the threat severity or fear appeal will decrease subsequently. The following figure illustrates a model proposed by Vance et al. for describing the effect of habit in ISSP compliance.

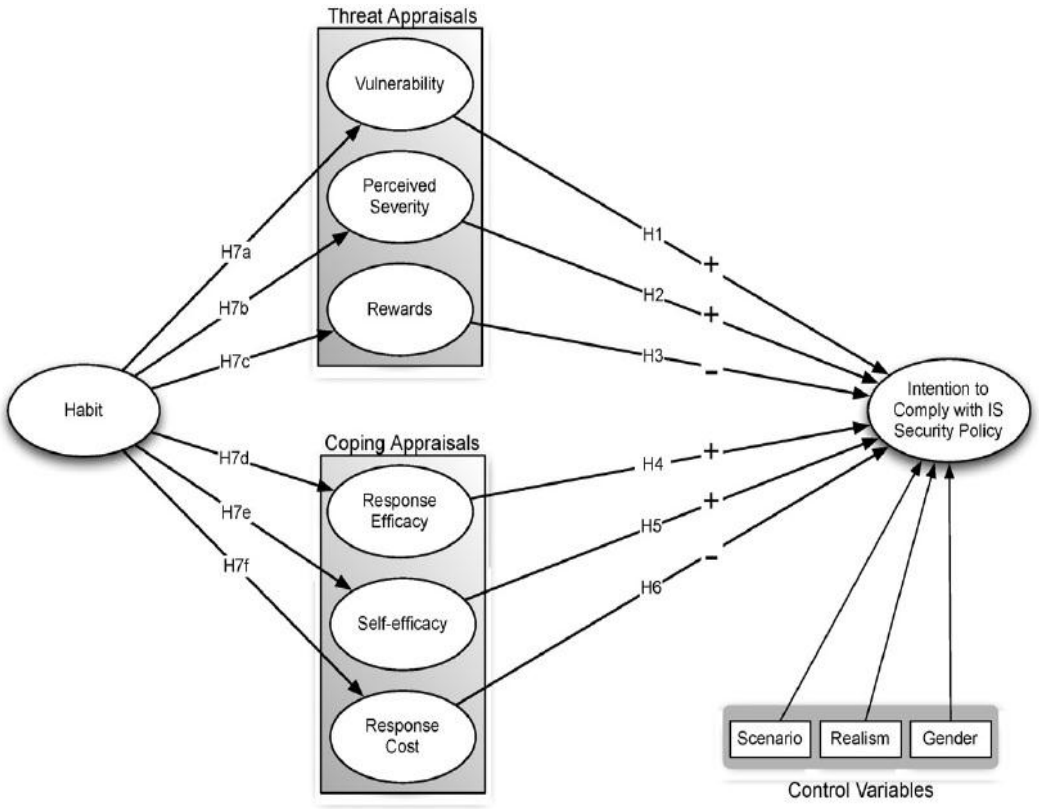

Figure 13- Habit and ISSP Compliance (Vance et al., 2012)

Habit influences all constructs of PMT model including threat appraisals and coping appraisals. Control variables directly influence ISSP compliance intention.

Among the different studies in compliance behavior field, some have used a general framework for studying the employees' intention. These frameworks consist of the majority of constructs that were used in previous studies. For instance, Ifinedo has proposed a conceptual model that includes several other theories and models such as TPB, SBT and SCT (Ifinedo P. , 2014). He also has added control variables such as job tenure or position in to previous control variables. Figure 14 shows the integration of three models in order to explore ISSP compliance intention.

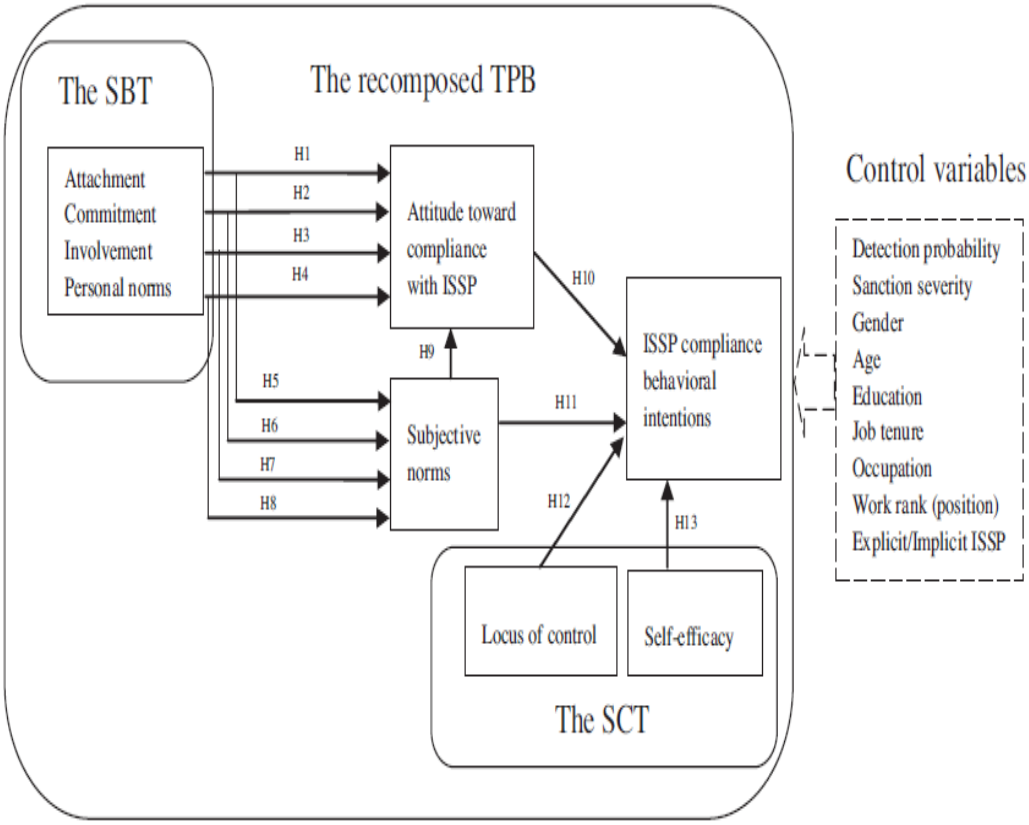

Figure 14-SBT, TPB and SCT integration (Ifinedo P. , 2014)

SCT or social cognitive theory states that individuals usually have a specific conception about their development (Bandura, 1997). Individuals always consider the degree which they can control events that can directly or indirectly affect their behavior (Ifinedo P. , 2014). The SBT and TPB are explained previously in this study. Bandura's model indicates that constructs of SBT influence the constructs of TPB. Furthermore, constructs of SCT and TPB directly influence the intention to comply. Deterrence or control variables also affect the ISSP compliance. This model gives a multi-perspective framework with several constructs that helps to the better understanding of security behavior, but some other important constructs like habit, personality and risks are missing. Actually, integrating all of the related theories and models is not possible and makes the research so complex.

Aurigemma & Panko in their study of security behavior propose a composite framework for a comprehensive exploring of ISSP compliance (Aurigemma & Panko, 2012). Figure 15 illustrates this framework that integrates several conceptual theories in order to a multi-perspective study.

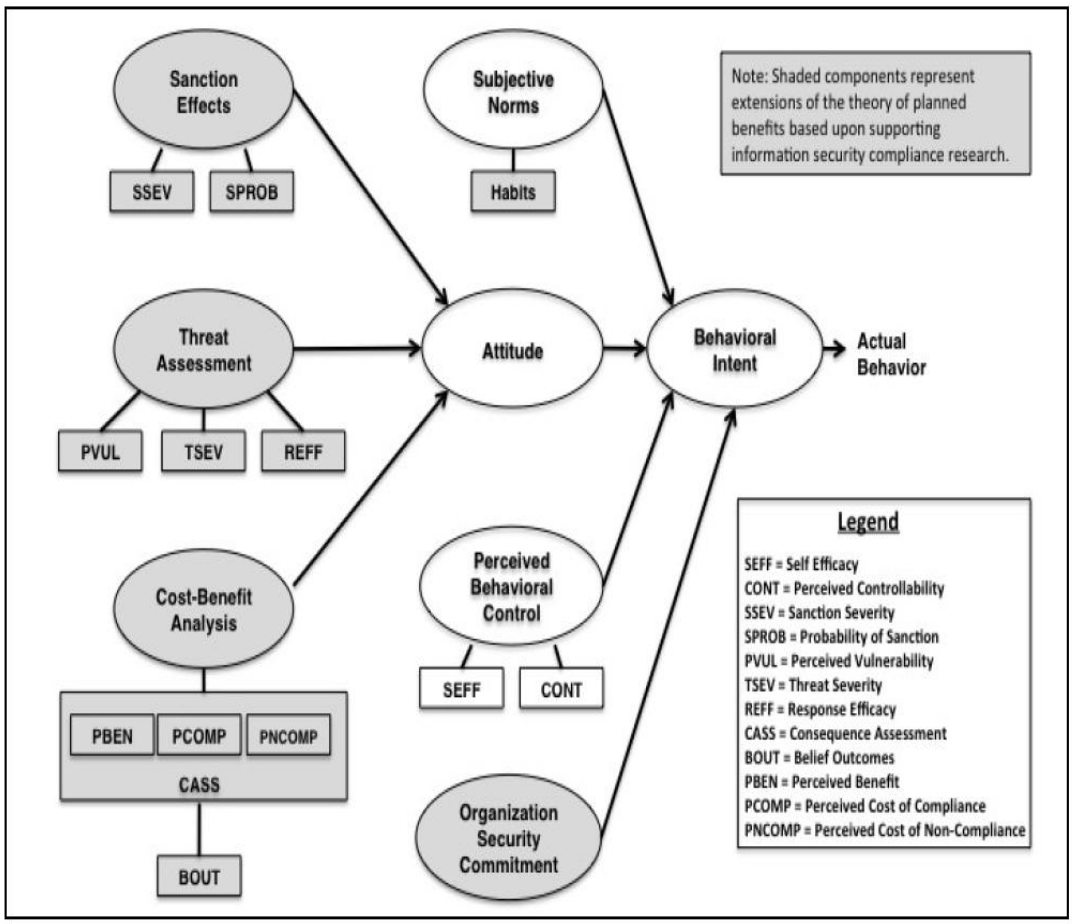

Figure 15- Composite framework for compliance study (Aurigemma & Panko, 2012)

This framework contains constructs of TPB, deterrence, PMT, fear appeals and habit. In addition, Aurigemma & Panko have considered the TPB as the base model and they have expanded it with constructs that are proposed in the ISSP compliance field. So determinants of intention to comply with ISSP are the main constructs of the TPB model. As you can see subjective norms, behavioral control and attitude directly affect the compliance intention. Organization commitment also directly influences the intention. Regarding this framework it can be concluded that the constructs of TPB are the main determinants of compliance intention and other constructs indirectly influence the intention. However, according to the other theories that are mentioned in this study control variables, habit, risks, benefits and other constructs also can directly influence the intention. So there are various studies investigating the different aspects of the employees' behavior and each of them is not absolute and depends on the context of the study.

Organizational power absolutely has a certain relationship with the IS compliance behavior (Kolkowska & Dhillon, 2013). Based on the Hardy's theory organizational power has different facets including resources, meanings, process and systems (Hardy, 1996). Describing the relationship of the organizational power and ISSP compliance from these dimensions can help to better understanding the employee's behavior.

Resources: Every employee may have specific control on the creation resources of the organization. So the degree of control can influence the behavior of the employees (Kolkowska & Dhillon, 2013). Alongside the control of resources there might be punishments, sanctions or rewards from the managers' side in order to control this authority.

Process: Business process within the organization allocates some responsibilities or power for different employees. So maintaining the position and power originated from the processes are important for employees. So this can affect their security behavior because they know that violation of the ISSP may endanger their positions and power.

Meaning: Organizations usually have a hierarchy of the power within them. So indoctrinating the power hierarchies and responsibilities should be appropriate. Different symbols, languages or icons can be used for this purpose (Kolkowska & Dhillon, 2013). These icons or languages make different meanings and by using them, changing the norms and values can be shown legitimate and desirable (Kolkowska & Dhillon, 2013). We can use this process to explain the violation or compliance behavior of the employees.

System: This dimension of power is related to the previous three dimensions and without them cannot exist. System power is critical for the decision making process in organization through the whole organization. It certainly influences the behavior of employees because it can motivate or inhibit the employees to comply with the ISSP.

From the different power perspectives, we can investigate violation or compliance behavior of the employees. For example, if an employee has not control authority of some IS assets, he or she may be reluctant to comply with policies that are related to those assets. Contrarily, an employee who has control authority of some IS assets, may has some responsibilities that persuade him or her to be more compliant with ISSP. Regarding the process perspective an employee who has responsibilities related to the specific processes may be more reluctant to the ISSP compliance. On the other hand, power can persuade employees to violate ISSP for several reasons, including competitions and getting more privileges. It means that power could influence both of the compliance or violation intention.

There are also other facets of security behavior that can be valuable indicators of ISSP compliance. Because of the complexity of the human behavior variety of factors can deal with behaviors and affect them. Guo has proposed a framework of security related behaviors (K. H. Guo, 2013). In this framework several possible behaviors related to the security are listed. Information about security related behaviors are given in the Table 1.

Table 1- Security related behaviors (K. H. Guo, 2013)

Security-related behavior	Security assurance behavior (SAB)	Security compliant behavior (SCB)	Security risk-taking behavior (SRB)	Security damaging behavior (SDB)
Definition	Active behaviors by an individual who has clear motive to protect the organization's IS	Behaviors that are in line with organizational security policies	Behavior that may put the organization's IS at risk	Behaviors that will cause direct damage to the organization's IS
Example	Take precaution; report incidents	Refrain from prohibited behavior	Password write-down; copy sensitive data to mobile devices	Crack password; data theft
Intentionality	Intentional	Intentional or unintentional	Intentional	Intentional
Motive (from the security perspective)	Beneficial	Neutral	Neutral	Malicious
Expertise	High	Low to high	Low to high	High
Role	End users and IS people	End users and IS people	End users and IS people	More likely IS people
Job relatedness	No	No	Yes	No
Consequence	Improve security	(Not applicable)	Risk	Direct damage
Action vs. inaction	Action	Action or Inaction	Action	Action
Rule	(Not applicable)	Organizational policy	Organizational policy	Laws and organizational. Policy
Other characteristics	Do what one is not expected to do	Do not do what one is expected not to do	Do what one is expected not to do	Do what one is prohibited from doing

Security compliant behavior and other behaviors are explained in the table 1. All of these behaviors can influence each other. Furthermore, each of these security behaviors has its own characteristics. Compliant behavior can be intentional or unintentional. For instance, an employee may deliberately violate the ISSP for different purposes. On the other hand, an employee may be unaware when he or she violates the ISSP. Another characteristic of the compliant behavior is that in some cases a specific action should be done for ISSP compliance. However, in some other cases if an employee does not do any action he or she is in line with the ISSP (K. H. Guo, 2013).

Overview of the ISSP compliance research can show that several studies try to study And explain the intention to comply with ISSP. They have used different conceptual theories and models to investigate several aspects of compliance behavior. Some of them have integrated various models for a multi-perspective study.

Among these research works those which have used IS adoption theories are very important for this thesis because the goal of this study is to pursue the ISSP

compliance behavior by utilizing a post adoption theory. Indeed, there is no conceptual model or theory explaining the continuous intention to comply with the ISSP and it is necessary to fill this gap in IS research.

CHAPTER III

Hypothesis Development and Research Model

This chapter develops necessary hypothesis for proposing the research model by utilizing the constructs of IS continuance model. The main objective of this chapter is to exploring the continuous compliance behavior of the employees based on IS post adoption research.

3.1 Research Model

For further investigating the employees' compliance behavior, studying the continuous intention to comply with ISSP is compulsory. As it is mentioned earlier initial security compliance is not enough for assuring about the successful implementation of ISSP. Previous research about IS adoption confirms that new IS/IT success completely depends of the initial acceptance of its users as well as continuance intention to use. Modern organizations are increasing their investment in new information systems because of competitive advantage and better management of information. Thus, organizations should utilize methods for predicting or increasing adoption of new IS/IT users in order to predict or increase the IS success. Literature review in the ISSP compliance field reveals that several studies utilize usage adoption theories or models for explaining employee's compliance behavior. They also confirm that these models and theories are suitable for ISSP compliance study because adoption to new information systems and comply with new ISSP are very close conceptions. However, previous studies just have used the pre-adoption theories or model and they have not focus on continuance theories. So this study utilizes one of the widely used models in order to explore continuous compliance. Figure 16 illustrates the research model.

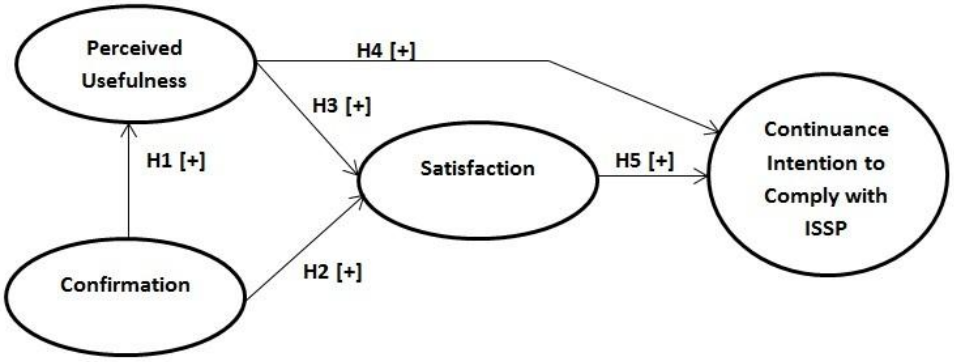

Figure 16- Research model

3.2 Research Hypothesis

In the research model, based on IS continuance model and ISSP compliance behavior five hypothesis are developed. These hypotheses explain relationship among four constructs of the model including perceived usefulness of ISSP, confirmation of expectation about ISSP, overall satisfaction with ISSP and finally, continuance intention to comply with ISSP.

Confirmation & Perceived usefulness

The initial conception of users about usefulness might be low because they may have not explicit expectation about the new IS (Bhattacherjee, 2001). Users may accept to use a new information system just because they want to gain concrete perception about the usefulness of IS. So through the confirmation of the initial or subsequent expectations about information system, users may develop a higher degree of usefulness perception.

Based on cognitive dissonance theory (Festinger L. A., 1957) users may experience psychological tension when their expectations about usefulness of information systems do not be confirmed during the actual usage of information system. Thus, the increase of confirmation perception causes the increase of perceived usefulness and the decrease of confirmation causes the decrease of usefulness. So there is a causal relationship between confirmation of expectation and perceived usefulness.

We can describe the compliance behavior based on conceptions of usage adoption because perceived usefulness and confirmation of expectation is applicable in

security behavior of the employees. For example, an employee has initial expectation about the ISSP compliance including job performance, rewards or degree of usefulness. So after actual compliance behavior confirmation of expectation may cause the increase of the perceived usefulness. Contrarily if expectation about ISSP is disconfirmed during the actual compliance, the degree of perceived usefulness of ISSP compliance will decrease. Furthermore, it is important to know that employees' initial usefulness perception is one of the expectations that should be confirmed during the actual compliance.

According to the information above this study develops first hypothesis:

Hypothesis 1: Confirmation of compliance expectations has a positive relationship with perceived usefulness of employees.

Confirmation & satisfaction

Based on the ECT (Oliver, 1980) confirmation of expectations is determinant of users' satisfaction with actual usage. Confirmation is related to the expected IS usage benefits and therefore influences the evaluative response of the employees. Bhattachejee argues that confirmation directly influences the overall satisfaction of IS users during the post adoption period (Bhattacherjee, 2001). For instance, every user has his or her own expectation about the new information systems and if these expectations are confirmed, overall satisfaction with IS usage will be increased. On the other hand, if expectations of users are disconfirmed, the degree of satisfaction will be decreased during the actual IS usage. So there is a casual relationship between confirmation and satisfaction and confirmation is positively related to the overall satisfaction of IS users.

In chapter 2 we found that IS adoption hypothesis can be utilized through ISSP compliance study. So the relation between confirmation and satisfaction that is related to the post adoption field also can be described in security compliance study. In the initial stage, employees have some expectation about the ISSP compliance. If these expectations would be confirmed during the actual compliance, their overall satisfaction with ISSP will be increased. On the other hand, if their expectations would be disconfirmed, their degree of satisfaction will be decreased.

We can come to the conclusion that confirmation of compliance expectation directly influences the overall satisfaction with ISSP and the relationship between these constructs is positive. The expectations of an employee about ISSP compliance may include usefulness, ease of use, job performance and etc.

Based on the discussion above this study develops second hypothesis:

Hypothesis 2: Confirmation of expectation has a positive relationship with overall satisfaction of employees with ISSP.

Perceived usefulness & satisfaction

Drawing from the technology acceptance model, perceived usefulness is one of the determinants of technology acceptance (Davis, 1989). This has been confirmed through several studies and through different contexts (Davis, 1989) (K. Mathieson, 1991) (Taylor & Todd, 1995). According to the IS continuance theory, perceived usefulness alongside the confirmation is another determinant of users satisfaction. For instance, if a user believes that using information system is useful for him or her, he or she will be satisfied with IS usage. The higher degree of usefulness causes the higher degree of satisfaction. On the other hand, if an employee feels that information system is not useful, he or she will resist using it. Briefly, there is a casual relationship between usefulness and satisfaction of the users.

In the ISSP compliance field, relationship between usefulness and satisfaction can be utilized. If an employee believes that complying with ISSP is useful, he or she will be satisfied with complying. Contrarily, if an employee thinks that complying with ISSP is not useful he or she will not be satisfied with complying. So we can conclude that there is a casual relationship between usefulness and satisfaction and perceived usefulness of ISSP compliance positively affects overall satisfaction with ISSP compliance.

Therefore the following hypothesis can be proposed:

Hypothesis 3: Perceived usefulness has a positive relationship with overall satisfaction with ISSP compliance.

Perceived usefulness & continuance intention to comply with ISSP

According to the TAM, perceived usefulness is one of the direct determinants of technology acceptance (Davis, 1989). Perceived usefulness is related to the instrumentally consideration and plays an important role in motivating intentions. Bhattacherjee confirms that perceived usefulness can be used in continuance usage context and he believes that usefulness can also determine the continuance intention If an employee feels that using the information system is useful he or she will continue to use it (Bhattacherjee, 2001). So perceived usefulness directly influences the user's intention to continue using information system.

The relation above is also applicable in ISSP compliance context. Assume an employee who is in actual compliance stage. If the employee believes that compliance is useful for him or her, he or she will continue to ISSP compliance. So perceived usefulness of ISSP compliance directly affects continuance intention to comply with ISSP. The higher degree of usefulness perception results in a higher degree of the continuous complying.

Thus, based on the discussion above this study develops following hypothesis:

Hypothesis 4: Perceived usefulness has a positive relationship with continuance intention to comply with ISSP.

Satisfaction & continuance intention to comply with ISSP

Drawing from the expectation confirmation theory (ECT) satisfaction is the primary determinant of the continuance intention to use information system (Bhattacherjee, 2001). Satisfaction includes positive feeling, but it can be changed to dissatisfaction that includes negative feeling. If an employee is dissatisfied with using information system (because of a low degree of usefulness or disconfirmation of expectations), he or she will not continue to use it. It means that if employees have a high degree of satisfaction they will be more motivated to continuance usage. Briefly overall satisfaction with information system directly influences intention to continue it (Bhattacherjee, 2001).

Based on the information above, we can utilize the relationship between satisfaction and continuance intention in ISSP compliance context. Overall satisfaction with ISSP compliance results in continuance intention to comply with ISSP. For example, if an employee is dissatisfied with ISSP compliance, most probably he or she will not continue to comply with ISSP and he or she will break some rules and guidelines. Therefore it can be deduced that overall satisfaction with ISSP directly affects continuance intention to comply with ISSP.

According to the information above the following hypothesis is proposed:

Hypothesis 5: Overall satisfaction with ISSP compliance has a positive relationship with continuance intention to comply with ISSP.

In summary, this study hypothesis that constructs of IS continuance model can be utilized in ISSP compliance contexts in order to investigate continuous intention of employees to complying with ISSP. This study suggests that compliance behavior contains two stages namely as initial compliance and continuous compliance. Initial compliance with ISSP is investigated through several studies, but it is a need to analyze the next stage for assuring about the success of the ISSP and IS security.

CHAPTER IV

Research Methodology

This chapter contains methodology of this study for testing research model and hypothesis. It includes scenario design, measurement item development, pre-testing and refinement of items, sample, data collection, and finally, choosing an appropriate method for analyzing collected data.

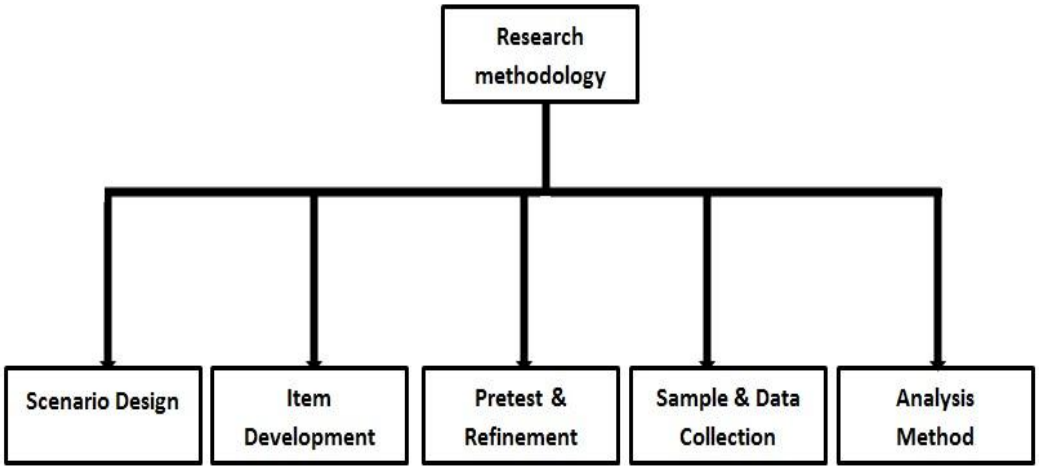

Figure 17- Research Methodology

For designing an appropriate research methodology, this study utilizes several accredited references and top MIS journals, including MIS Quarterly and Information Systems Research (Bulgurcu et al., 2010) (Bhattacherjee, 2001) (A. Vance, 2012). This research methodology is widely used by IS scholars and it can help this study in analyzing and testing the research model and hypothesis through an appropriate and trusted way.

4.1 Scenario design

The first step for conducting research is to design a framework in order to listing all of the necessary functions and works. In other word, for doing efficient research an explicit plan is compulsory. After proposing the research model and developing the hypothesis, next stages should be designed very carefully for appropriate and trustable testing. The general plan is given below:

Step 1: Method of data collection

Survey method is appropriate for testing the hypothesis of this study. Furthermore, an online survey helps to saving time and to have more respondents. For getting more accurate responses and motivation respondents some incentives should be considered. Getting high percent of valuable response is the primary purpose in this stage.

Step 2: Measurements

Designing measurement items and survey contents is very crucial for this research since data should be collected based on these measurement items. Thus, all of these items should be extracted from previous research and literature review. In addition, demographic information should be considered among the survey items.

Step 3: Testing and refining the measurement items

For assuring about the validity of the survey items a pilot test should be done. Items should be refined based on feedback of several faculty members and professionals. A card sorting test (Moore & Benbasat, 1991) is appropriate for getting feedback a card sorting test (Moore & Benbasat, 1991) is appropriate for getting feedback and refining the measurement items.

Step 4: Choosing sample for data collection

Subjects should be employees of organizations and because this study investigates the post compliance behavior, employees should be in the actual compliance stage. After choosing appropriate sample survey items should be sent by email for each of employees. The reminder emails also should be sent after due date. Finally, incentives should be considered through online environment because physical incentives and rewards are not possible.

Step 5: Choosing statistical analysis method

The final step is choosing an appropriate software or mechanism for statistical analysis. Literature review and professional recommendation are important in order to choosing valid methods. Hypothesis should be examined carefully through statistical analysis.

4.2 Item development

Four constructs should be measured for further analysis. All constructs of the research model are related to the IS continuance model. So this study, by using feedback from IS professionals tries to refining two measurement items of IS continuance model (confirmation and Continuance intention) and adopting them in ISSP compliance context. Table 2 illustrates the measurement references.

Table 2- References of Measurement Items

Measurement Items	References
Perceived Usefulness	(Davis, 1989) (Bhattacherjee, 2001)
Confirmation	(Bhattacherjee, 2001)
Satisfaction	(Bhattacherjee, 2001)
Continuance Intention	(Bhattacherjee, 2001)

Measurement of perceived usefulness and satisfaction consist of four items for each. Measurement of confirmation and continuance intention to comply with ISSP, consist of three items for each. All of the constructs are measured in multiple items based on the five point Likert scale. In Likert scale items are scored from strongly disagree (1) to strongly disagree (5). So if a respondent chooses 1, it means that he or she is completely disagree with the statement. On the other hand, if he or she chooses 5, it means that he or she completely agrees with that statement. All of the measurement items are mentioned in Appendix A.

4.3 Testing and Refining the Measurement Items

As it is mentioned earlier that it is compulsory to test contents of measurement items and refining them based on the ISSP field. Before testing the measurement items, 6 IS professionals skilled in statistical analysis and quantitative research methods reviewed the measurement items. After two rounds of refining and reviewing all of the professionals accepted that measurement items are relevant and accurate. Next measurement items were proposed to 10 other IS professionals for card sorting process (Moore & Benbasat, 1991). Results of card sorting test revealed some other factors related to ISSP compliance and helped to appropriate classification. The measurement items were refined again based on card sorting test and factors related to ISSP compliance.

Pilot survey

After translating the measurement items from English to Persian, survey is conducted among 30 employees of banking organizations. All of the survey items were similar to the main survey items of this study. After distributing the questionnaires, 25 of the respondent participated in the survey and completed the questionnaires. So the response rate was 83%. In addition, the respondents remarked about the wording and length of the survey items and they recommended their concerns about the structure of the survey. Based on the respondents' comments, survey items were further modified.

Reliability of measurement scales

The reliability of measurement items were tested by Cronbach's α. In the alpha test, factor loadings greater than 0.7 are acceptable. Factor loadings between 0.7 and 0.8 are indicator of good reliability and internal consistency. Factor loadings greater than 0.8, mean the excellent reliability and internal consistency. Alpha test of measurement items based on the pilot data shows that factor loadings for all of the measures are greater than 0.8 which indicates excellent reliability and excellent internal consistency for measurement items of this study.

Convergent Validity

All of the measurement items were tested through convergent validity. In convergent validity test, factor loadings greater than 0.6 are acceptable (Chin et al., 1997). All of the loadings for pilot test were greater than 0.8 and this indicates convergent validity of the measurements. Results are given in appendix B.

Discriminant Validity

Finally, discriminant validity of measurement scales was examined. Discriminant validity can be tested by comparing the shared variance between items and average variance extracted (AVE) of individual items (Chin et al., 1997). For discriminant validity the AVE of all individual items should be greater that shared variance between items. Comparing the AVE and shared variance of items in pilot tests indicates the discriminant validity of all measurement items.

4.4. Sample and Data Collection

Subject selection criteria

There were two criteria for selecting sample and subjects for survey. First of all employees should directly deal with ISSP in their organizations. It means that there should be mandated compliance with ISSP in order to explicit investigating the

compliance behavior. Second, all of the employees should be in post compliance phase. They should be in a situation that ISSP has been established for a while and they are in actual compliance phase. So the target employees may have gotten trainings or education about security threats or compliance. They also may have some degree of security awareness during the ISSP establishment.

Survey

After searching among different organization it is confirmed that Data were collected for further analysis from employees of several private or public banking organizations in Iran. Because distributing the questionnaire among the employees and getting feedback from them were time consuming, a web-based questionnaire was conducted. Because all of target employees had access to internet they could easily reply to the questionnaire. An invitation that included original e-books as incentives to participation in survey was sent for 350 employees. Finally, after one month 287 employees participated in survey. Among the responses, 275 were valid and complete with the validity rate of 96%.

4.5 Data Analysis Method

In the research model there are three dependent constructs (usefulness, satisfaction & continuance intention to comply with ISSP) and there is one independent construct (confirmation). In order to research model analysis Structural equation modeling (SEM) is the most appropriate method because the research model is theatrically justified (Bhattacherjee, 2001). For testing an well-established and theoretically justified model LISREL method is more appropriated than PLS because PLS is suitable for analyzing and predicting second-ordered and multi-dimensional and constructs (Chin et al., 2003) (Gefen et al., 2005). In addition, PLS utilizes a component base approach for analyzing the complex research model and it is not highly dependent of sample size (Chin W. W., 1998). On the other hand, SEM helps to identifying unobservable constructs by using previous knowledge. SEM also applies measurement errors in the research model. This study uses two approaches of SEM namely as confirmatory factor analysis and analyzing the structural model. For this purpose LISREL 8.5 is used.

CHAPTER V

Data Analysis

This chapter presents the statistical analysis of research model and hypothesis based on the collected data from 270 employees.

5.1 Demographic Information

In this part demographic information is given. Table 3 illustrates descriptive information about subjects of sample.

Table 3- Demographic information

Demographic Items	Frequency	Percentage
Male	153	56.6
Female	117	43.3
Age (20-40)	182	67.4
Age (40-60)	88	32.5
Private Organization	144	53.3
Public Organization	126	46.6

Approximately 56.6% of final sample were males and 43.3% of sample were females. The age of sample ranged from 20 to 60 and 67.4% of subjects were in age between 20 and 40 and 32.5 % of them were in age between 40 and 60. Lastly, 144 of the subjects were employees of private organizations and 126 of them were working in public organizations. All of the respondents had computer experience and they could access to internet. Demographic items of survey are given in Appendix C.

5.2 Analysis of Hypothesis and Structural Model

First of all in order to test the hypothesis of research model the goodness of fit indices is estimated. According to Bentler and Bonnet (1980) Chi square/Degree of freedom ratio is a good indicator of the research model fit. If this ratio is lower or equal to 5, the research model is a good fit.

Table 4- Fit indices

Fit indices	Recommended Value	Actual Value
χ^2		347.218
df		127
χ^2 / df	≤5	2.734
RMSEA	≤0.8	0.057
P value	≤0.5	0.000
GFI	≥0.9	0.940
CFI	≥0.9	0.970

The chi square/ degree of freedom ratio for the research model is 2.734. So this is goodness of fit indicator of research model. The Structural equation with AMOS presents other goodness of fit factors including RMSEA, P value, GFI and CFI. RMSEA or root mean square error of approximate shows whether structural model with given estimate parameters is well fit to the matrix of population covariance or not (Byrne, 2001) (Hair et al., 2006). Results show that RMSEA of for research model is 0.057 and is lower than 0.8. According to the Hair et al. study parameter estimates of structural model is fit to matrix of population covariance. GFI or goodness of fit, estimates the proportion of the variance that is considered by the covariance of the estimated population (Tabachnick & Fidell, 2007). Regarding hair et al. study the GFI factor should be greater than 0.9 and therefor GFI factor of the research model is significant. Lastly, CFI or comparative fit indicates that whether hypothesis fits to the observed data. Hair et al. suggest that CFI should be greater than 0.9 and therefor CFI factor for research model is significant.

In the next step path significance and the R^2 value (Path coefficient) for all relationships are estimated. Figure 18 illustrates R^2 values and path significance for all of the relationships.

Figure 18- Path significance and coefficient values

Regarding figure 18, all of the hypothesis paths of research model are significant at $P \leq 0.001$. R^2 indicates that whether variation of the data has a good fit or not. For instance, $R^2=0.56$ shows that the fit explains the 56% of the variation in collected data. Among the constructs, continuance intention has the greatest R^2 value and satisfaction has the lowest R^2 value. The relationship between perceived usefulness and continuance intention to comply with ISSP compliance has the highest degree of significance and the relationship between confirmation and satisfaction has the lowest degree of significance among the other relationships.

For calculating regression weights confirmatory factor analysis is conducted. This analysis through maximum likelihood estimation, investigates values such as regression weight, standard deviation, and critical ratio. These values also help to find the significance of pairwise relationships of research model. Table 5 shows the regression weights (B) of relationships based on maximum likelihood estimation.

Table 5- Regression Weights

Paths	Standard Regression Weights (B)	Standard Error S.E.	Critical Ratio	P
H1:Confirmation-Usefulness	0.459	0.039	8.231	***
H2:Confirmation-Satisfaction	0.289	0.019	26.549	***
H3:Usefulness-Satisfaction	0.427	0.052	12.714	***
H4:Usefulness-Continuance Intention	0.527	0.064	9.517	***
H5:Satisfaction-Continuance Intention	0.490	0.027	18.816	***

B values range from 0.289 to 0.527. Regarding Table 5, all of the paths are significant at $P<0.001$ and therefore the entire hypothesis are supported. Critical ratios ranged from 26.549 to 8.231. According to the Hair et al. study critical ratios should be greater than 1.96 and results show that all of the critical ratios are acceptable (Hair et al., 2006). The greatest critical ratio is for the relationship between satisfaction and continuance intention. The lowest critical ratio is for relationship between confirmation and usefulness.

Standard error indicates the precision of likelihood estimation and the lower standard error shows the more precise estimation. Standard errors for all of the pairwise relationship are close to zero. It means that estimations are precise and errors are acceptable for all B values of relationships. Among the relationships confirmation-satisfaction has the lowest standard error and usefulness-continuance intention has the greatest standard error. In order to assuring about the reliability of constructs and getting the descriptive data a confirmatory factor analysis presents values such as Skewness, Kurtosis and alpha. Table 6 illustrates these values based on CFA.

Table 6- Reliability and descriptive information

	N	MIN	MAX	MEAN	SD	SKEW.	KURT.	ALPHA
PUSE	270	2.47	5.00	3.88	.62	-.24	-.07	8.34
SAT	270	2.86	5.00	3.14	.56	-.39	.05	8.9
CONF	270	1.34	5.00	3.90	.58	-.19	.12	9.14
INT	270	1.57	5.00	3.23	.69	-.43	.25	9.36

Note. PUSE: Perceived Usefulness, SAT: Satisfaction, CONF: Confirmation, INT: Continuance Intention to comply with ISSP

According to the Table 6, all of the alpha values are greater than 0.8 and this confirms that all of the coefficients are significant and acceptable. Alpha value for continuance intention to comply with ISSP is the greatest and alpha value for perceived usefulness is the lowest among other constructs. Skewness and kurtosis are related to the distribution of observed data and the values indicate that all of the observed data are distributed in normal form. Furthermore, negative skewness values indicate that data distributions are skewed in the same direction. Based on the Tabachnick & Fidell findings, negative values of skewness shows that linearity assumptions are confirmed (Tabachnick & Fidell, 2007).

In the next step correlation matrix of model constructs is calculated by CFA. Correlation between constructs and square roots of average variance extracted (AVE) are presented in Table 7.

Table 7- Correlation matrix

	Confirmation	Usefulness	Satisfaction	Continuance Intention
Confirmation	0.863			
Usefulness	0.413	0.847		
Satisfaction	0.217	0.326	0.849	
Continuance Intention	0.384	0.547	0.345	0.912

Correlations for all of the pair wise relationships are positive and greater than 0.2. An effect size of r =0.1 means that the effect size is small. A correlation of 0.3 means a medium effect size and lastly a correlation of r =0.5 shows a large effect size (Cohen J., 1988). Thus, Table 7 illustrates that the relationship between perceived usefulness and continuance intention to comply with ISSP has the largest effect size. In addition, results show that the average variance extracted for each of the constructs is greater than shared variance between relationships. This indicates that all of the constructs of the research have discriminant validity.

There are three criteria proposed by Fornell and Larcker for testing the convergent validity. First, all of the factor loading must be greater than 0.7. Second, reliability amounts for all of the constructs should be more than 0.8. Finally, AVE for every construct should be more than the variance caused by measurement error. Table 7 shows that all AVE values (Values in diagonal of the matrix) are more than 0.7 and these values are also more than variance of measurement error. In addition, values of reliabilities for all constructs are more than 0.8. It means that constructs of research model have convergent validity.

Direct and indirect effect

In the structural equation modeling there is a difference between direct and indirect effect (Jöreskog & Sörbom). A total effect size consists of direct plus indirect effect size. On the other hand, for investigating the moderator factors including gender and age it is useful to analyzing the direct and indirect effect sizes for each of the different groups. In this study subjects are divided to females and males groups from gender perspective. In addition, subjects are divided to under 40 years old and over 40 years old. Table 8 presents the direct and indirect effect sizes on the continuance intention to comply with ISSP for all of the constructs from gender perspective.

Table 8- Direct and Indirect effect from Gender Perspective

Constructs	INT (Females)			INT (Males)		
	Direct	Indirect	Total	Direct	Indirect	Total
PUSE	0.352	0.149	0.481	0.369	0.174	0.543
CONF	NA	0.167	0.167	NA	0.215	0.215
SAT	0.451	0.124	0.575	0.491	0.153	0.644
$R^2 = 0.671$						

Note. PUSE: Perceived usefulness, CONF: Confirmation, SAT: satisfaction, INT: continuance intention to comply with ISSP

Results of direct and indirect effects confirm that gender moderates the effects on the continuance intention. For both of the groups, satisfaction is more important than perceived usefulness in determining the continuance intention to comply with ISSP.

Results also indicate that satisfaction is the prominent determinant of continuance intention for males and females. In addition, indirect effect size of confirmation is greater in males. It means that confirmation of expectation in actual compliance stage is more important for males. Finally, total effect size of satisfaction is greatest among other constructs for males and females.

As discussed earlier, the subjects are divided into two groups from age perspective. Direct and indirect effect sizes of constructs are presented in Table 8.

Table 9- Direct and Indirect effects (Age Perspective)

Constructs	INT (Under 40)			INT (Over 40)		
	Direct	Indirect	Total	Direct	Indirect	Total
PUSE	0.426	0.171	0.597	0.287	0.158	0.443
CONF	NA	0.192	0.153	NA	0.211	0.211
SAT	0.413	0.181	0.594	0.539	0.184	0.723
$R^2 = 0.619$						

Note. PUSE: Perceived usefulness, CONF: Confirmation, SAT: satisfaction, INT: continuance intention to comply with ISSP

For the older group, satisfaction with ISSP compliance is more important than usefulness of ISSP. However, in younger group perceived usefulness is the prominent determinant of continuance intention. Furthermore, indirect effect size of confirmation is greater in older group. It means that confirmation of expectation during actual compliance stage is more important for subjects who are in 40-60 age. Finally, results confirm that age moderates the effects on continuance intention to comply with ISSP.

CHAPTER VI

Conclusion and Implications

This chapter aims to present discussion about the data analysis results. Conclusion, study limitations and implications are also given in this chapter.

6.1 Summary of results

Information security is one of the major issues for modern organizations. As discussed earlier organizations utilize several technical or behavioral techniques in order to solve security problems especially in information systems. Information systems play an important role for the success of the organizations. All of the modern organizations need information systems to process large volume of the information. On the other hand, information systems usually keep very important data and security problems in them can be very pernicious. One of the important approaches for ensuring information systems security is to provide a multi-perspective security policy that contains general rules, guidelines and techniques. So compliance with ISSP is very important because in case of ISSP violation, organization managers cannot handle the security issues. Regarding various studies that have investigated employees' intention to comply with ISSP, this study tried to continue this research trend by utilizing the IS continuance model. Obviously initial intention to comply with ISSP is not enough because in actual compliance stage employees may interrupt continuance behavior. So exploring the continuance intention is necessary for ISSP success.

This study utilizes reliable measurements for collecting data and statistical analysis. Results of measurement items indicate that all of them are reliable and valid. In order to assuring validity and reliability of survey and measurement items, several tests including alpha, convergent and discriminant are accomplished. Results of these tests confirm that items can be accurate indicators of employee's attitudes and behaviors and they have convergent and discriminant validity.

For testing the research hypothesis and conceptual model several methods including structural equations modeling and confirmatory factor analysis are utilized. Results confirm the entire research hypothesis and all of the SEM and CFM factors are significant and acceptable. Table 10 illustrates the summary of hypothesis testing.

Table 10- Summary of results

Hypothesis	Results
Hypothesis 1: Confirmation of compliance expectations has a positive relationship with perceived usefulness of employees.	Confirmed
Hypothesis 2: Confirmation of expectation has a positive relationship with overall satisfaction of employees with ISSP.	Confirmed
Hypothesis 3: Perceived usefulness has a positive relationship with overall satisfaction with ISSP compliance.	Confirmed
Hypothesis 4: Perceived usefulness has a positive relationship with continuance intention to comply with ISSP.	Confirmed
Hypothesis 5: Overall satisfaction with ISSP compliance has a positive relationship with continuance intention to comply with ISSP.	Confirmed

All of the hypotheses are confirmed through SEM analysis. So the proposed conceptual model is valid and reliable.

This study also examined the moderator effects of gender and age on the continuance intention to comply with ISSP. Results confirm that gender and age affect the relationship between satisfaction and continuance intention. In addition, different results from gender and age perspective confirm that relationship between perceived usefulness and continuance intention is affected by moderator factors. This study also has investigated the direct and indirect effects of all constructs and results show that relationships have different effect sizes through different groups of employees.

6.2 Conclusion

First of all based on the measurement analysis results, the measurement items of this study can be utilized in future research of ISSP compliance field. We can conclude that the measurement items are reliable for further study and for exploring the

continuance behavior of employees.

Second, according to the SEM and CFA results this study confirms that IS continuance model is suitable and reliable framework for continuous compliance study. It means that by accurate measurement items this model can be used in ISSP compliance context.

Third, SEM and CFA results show that perceived usefulness and satisfaction of employees are determinants of continuance intention to comply with ISSP. So these factors can predict post adoption behavior as well as continuous compliance of employees. In addition, Confirmation of expectation positively affects perceived usefulness and satisfaction. It also indirectly affects continuance intention to comply with ISSP.

Fourth, according to the direct and indirect analysis different groups of employees have different behaviors and attitudes. So considering moderating factors like age and gender can moderate the effects on intentions.

6.3 Study Limitations

First of all this study just uses one of the well-known post adoption models for studying the continuous compliance. There are also other models or theories that can be utilized for this purpose. For instance, constructs of TAM and TPB including perceived ease of use, subjective norms and behavioral controls can be determinants of continuance intention. This study has not investigated the effect of these constructs and the constructs of research model are limited to IS continuance model.

Second, subjects of this study are limited to the employees of banking organizations however, employees of other kinds of organizations may have different behaviors.

Third, this study only investigates the age and gender of employees as moderator factors. However, there are also other moderator factors like culture and experience.

Lastly, initial intentions of employees are not examined in this study. However, compliance behavior can be investigated through longitudinal research. For instance, the research model proposed by Karhanna et al. can be utilized in order to exploring pre compliance and post compliance together.

6.4 Implications

Organization managers have to study the behavior of employees for designing security plans and frameworks. As discussed earlier success of information systems security policies depend on the compliance of employees. Thus, managers can analyze the employees, behavior in order to estimate and predict the ISSP success. They can utilize the proposed model of this study for assuring about contiguous compliance of employees. This is very important point to protecting the valuable IS assets because if employees continue to comply with ISSP, security incidents will

decrease remarkably. Managers also should consider demographic factors for implementing ISSP. They should treat females or males differently and they should specify special sanctions or rewards for different kind of groups. Awareness and motivation strategies also should be specified explicitly based on the various groups of employees.

This study also offers implications for researchers. Future research can use other conceptual models or theories including UTAUT and Bhattacherjee's two stage adoption model (Bhattacherjee & Premkumar, 2004) in order to explore other aspects of continuous compliance. Previous research in IS adoption field indicates that there are several studies that have extended the IS continuance model. Different researchers have added extra constructs like habit to this model (Kang et al., 2008) (Kim. B., 2010). Information systems' scholars can utilize these extensions and extra constructs for studying the security behavior. In addition actual usage behavior can be explored alongside the continuance intention in longitudinal study.

Other implication for researchers is that they can analyze other moderator factors including culture, experience and education. They can study the effects of these moderator factors on relationships of the proposed model.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior and human decision processes. *Organizational Behavior*, *50*(2), 179-211.

Anderson, CL., Agarwal R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-43.

Aurigemma, S., & Panko, R. (2012). A composite framework for behavioral compliance with information security policies. *45th Hawaii International Conference on System Sciences.*

Bandura, A. (1997). Self-Efficacy: toward a unifying theory of behavioral change. *Psychological Review, 82*(2), 191-215.

Bentler, P. M., Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin, 88*(3), 588-606.

Bhattacherjee, A. & Premkumar, G. (2004). Understanding changes in belief and attitude toward information technology usage: A theoretical model and longitudinal test. *MIS Quarterly, 28*(2), 229-254.

Bhattacherjee, A. (2001). Understanding information systems continuance. An expectation–confirmation model. *MIS Quarterly, 25*, 351-370.

Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). Information security policy compliance:an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*, 523-548.

Byrne, B. M. (2001). SEM with AMOS: Basic concepts, applications, and programming. Routledge.

Cheng, L., Li, Y., Li, W., Holm, E., Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & security*, *39*, 447-459.

Chin, W., Gopal, A., Slaisbury, W. D. (1997). Advancing the theory of adaptive structuration: The development of a scale to measure faithfulness of appropriation. *Information Systems Research, 8*(4), 342-367.

Chin W. W. (1998). The partial least square approach to structural equation modeling. *Lawrence Erlbaum Associates*.

Clegg, S. R. (1989). Frameworks of Power. *Sage Publications*.

Cohen J. (1988). Statistical power analysis for the behavioral. Hillsdale: *Routledge Academic*.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*, 319-340.

Eliason, S. L. and Dodder R. A. (1999). Techniques of neutralization used by deer poachers in the western united states: A research note. *Deviant Behavior, 20*(3), 233-252.

Ernst & Young. (2008). *Ernst & Young 2008 Global Information.* http://faisaldanka.wordpress.com/2008/10/.

Festinger L. A. (1957). A theory of cognitive dissonance. Evanston, IL: Row and Peterson.

Fishbein M. and Ajzen I. (1975). Belief, attitude, intention and behavior. *Reading, MA: Addison-Wesley.*

Furnel, S. & Rajendarn, R. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security*, 12-15.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242-251.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., Tatham, R. L. (2006). *Multivariate data analysis.* New Jersey: Prentice Hall.

Hardy, C. (1996). Understanding power: bringing about strategic change. *British Journal of Management*, 3-16.

Herath, T., Rao, H. R. (2009). Encouraging information security behaviors: role of penalties, pressures and perceived effectiveness. *Decision Support Systems* , 154-165.

Hirschi T. (1969). *Causes of delinquency.* Berkeley, CA: University of California Press.

IBM. (2012). *The source of greatest risk to sensitive data.*

Ifinedo, P. (2007). An empirical study of ERP success evaluations by business and IT managers. *Information management & computer security*, 270-282.

Ifinedo, P. (2012). Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Computer & Security, 31*, 83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*, 69-79.

Islam, A.K.M. Najmul and Mantymaki, M. (n.d.). Culture and student samples as moderators of continued IT usage. *PACIS 2011 Proceedings.*

Jöreskog, K. J. & Sörbom. D.(n.d.) (1996) *LISREL 8: User's reference guide.* Lincolnwood: Scientific Software International.

Kang, Y. S., Hong, S., Lee, H. (2008). Exploring continued online service usage behavior: The roles of self-image. *Computers in Human Behavior, 25*(1), 111-122.

Kankanhalli, A. T. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*, 139-154.

Kim. B. (2010). An empirical investigation of mobile data service continuance: Incorporating the theory of planned behavior into the expectation–confirmation model. *Expert Systems with Applications, 37*, 7033-7039.

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, 3-11.

Li, H., Zhang, J., Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*, 635–645.

Mathieson, K. (1991). Predicting User Intentions: Comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research, 2*(3), 173-191.

Minor W. W. (1981). Techniques of Neutralization: A reconceptualization and empirical examination. *Journal of Research in Crime and Delinquency, 18*(2), 295-318.

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

Ng, B.-Y., Kankanhalli, A., Xu, Y. (2009). Studying users' computer security behavior:a health belief perspective. *Decision Support Systems, 46*, 815-825.

Oliver, R. L. (1980). A cognitive model for the antecedents and consequences of satisfaction. *Journal of Marketing Research, 17*, 460-469.

Parker D. B. (1998). Fighting computer crime: A new framework for protecting information. *New York: John Wiley & Sons*.

Piquero, N. L., Tibbetts, S. G., Blankenship, M. B. (2005). Examining the role of differential association and techniques of neutralization in explaining corporate crime. *Deviant Behavior, 26*, 159-188.

Rogers, R. (1983). Cognitive and physiological processes in fear-based attitude change: a revised theory of protection motivation. In:. Guilford Press.

Siponen M., & Iivari J. (2006). IS security design theory framework and six approaches to the application of IS security policies and guidelines. *Journal of the Association for Information Systems, 7*(7), 445-472.

Siponen, M. & vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*, 487-502.

Siponen, M., Mahmood, M. A., Pahnila, S. (2013). Employees' adherence to information security policies: An exploratory field study. *Information*, In press.

Smith, S., Winchester, D., Bunker, D., Jaimeson, R. (2010). A study of mandated compliance to an information security De Jure standard in a government organization. *MIS Quarterly, 34*, 463-486.

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

Straub D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*, 255-276.

Sykes, G., and Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*, 664-670.

Tabachnick, B. G. & Fidell, L. S. (2007). Using multivariate statistics (5th Ed.). *Boston: Allyn & Bacon*.

Taylor, S. & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research, 6*(2), 144-176.

Tudor J. K. (2000). IS security architecture:An integrated approach to security in the organization. *Boca Raton, FL: CRC Press.*

Vance, A., Siponen, M., Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*, 190-198.

Warkentin, M., & Johnston, A. C. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566.

Witte, K. (1992). Putting the fear back into fear appeals:The extended parallel process model. *Communication Monographs, 59*, 329-349.

Witte. K., Cameron, KA., Mckeon, JK., Berkowits, JM. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication, 1*, 317-341.

Xue, Y., Liang, H., Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research, 22*(2), 400-414

APPENDICES

APPENDIX A-Measurement Items

Continuance intention to comply with ISSP:

CICI 1: I intend to continue complying with ISSP rather than discontinue Complying with ISSP.

CICI 2: My intentions are to continue complying with ISSP rather than using other security methods.

CICI 3: If I could, I would like to discontinue my compliance with ISSP (reverse coded).

Perceived usefulness:

U 1: Complying with ISSP helps me accomplish tasks more quickly.

U 2: Complying with ISSP helps me perform many tasks more conveniently.

U 3: Complying with ISSP increases my productivity.

U 4: Overall, Compliance with ISSP is useful in managing my tasks.

Confirmation:

C 1: My experience with ISSP compliance was better than what I expected.

C 2: The service level provided by ISSP was better than what I expected.

C 3: Overall, most of my expectations from ISSP compliance were confirmed.

Satisfaction:

S 1: I feel satisfied with ISSP compliance.

S 2: I feel pleased with ISSP compliance.

S 3: I feel contended with ISSP compliance.

S 4: I feel delighted with ISSP compliance.

APPENDIX B-Scale reliabilities

Constructs	Item	Mean	S. D.	Loading	Reliability	AVE
Perceived Usefulness	U 1	3.55	1.65	0.91	0.91	0.85
	U 2	3.64	1.74	0.84		
	U 3	4.18	1.66	0.86		
	U 4	4.29	1.79	0.99		
Satisfaction	S 1	3.98	1.23	0.93	0.94	0.72
	S 2	3.47	1.27	0.90		
	S 3	3.42	1.16	0.88		
	S 4	3.64	1.59	0.89		
Confirmation	C 1	4.15	1.76	0.83	0.89	0.87
	C 2	3.78	1.83	0.86		
	C 3	3.35	1.91	0.85		
Continuance intention to comply with ISSP	CICI 1	3.76	1.57	0.81	0.86	0.76
	CICI 2	3.87	1.69	0.84		
	CICI 3	4.11	1.74	0.82		

APPENDIX C- Demographic items in Survey

1) Name, Last name (Confidential):

……

2) Gender:

……

3) Age:

……

4) Organization (Confidential):

……

5) Position (Confidential):

……

6) Years of work experience:

……

7) ISSP compliance period:

……

8) Education (Degree):

……

9) Daily hours of work with internet:

……

10) Security training experience:

……

TEZ FOTOKOPİSİ İZİN FORMU

ENSTİTÜ

Fen Bilimleri Enstitüsü ☐
Sosyal Bilimler Enstitüsü ☐
Uygulamalı Matematik Enstitüsü ☐
Enformatik Enstitüsü ☐
Deniz Bilimleri Enstitüsü ☐
YAZARIN

Soyadı : Abed
Adı : Javad
Bölümü : Information Systems

TEZĠN ADI (İngilizce) : How employees intend to continue complying with information systems' security policies? : Insights from information systems' continuance model

TEZĠN TÜRÜ : Yüksek Lisans ■ Doktora ☐

1. Tezimin tamamından kaynak gösterilmek şartıyla fotokopi alınabilir. ☐

2. Tezimin içindekiler sayfası, özet, indeks sayfalarından ve/veya bir bölümünden kaynak gösterilmek şartıyla fotokopi alınabilir. ☐

3. Tezimden bir (1) yıl süreyle fotokopi alınamaz. ☐

TEZİN KÜTÜPHANEYE TESLİM TARİHİ : …….