Factors Affecting Individual Information Security Practices

Santos M. Galvez
Trident University
577 Plaza Drive
Cypress, CA 90630
1-714-816-0366
santos.galvez@my.trident.edu

Joshua D. Shackman
Trident University
577 Plaza Drive
Cypress, CA 90630
1-714-816-0366
joshua.shackman@trident.edu

Indira R. Guzman
Trident University
577 Plaza Drive
Cypress, CA 90630
1-714-816-0366
indira.guzman@trident.edu

Shuyuan Mary Ho
Florida State University
142 Collegiate Loop
Tallahassee, FL 32306
1-850-645-0406
smho@fsu.edu

ABSTRACT

Data and information within organizations have become important assets that can create a significant competitive advantage and therefore need to be given careful attention. Research from industry has reported that the majority of security-related problems are indirectly caused by employees who disobey the information security policies of their organizations. This study proposes a model to evaluate the factors that influence the individual's information security practices (IISP) at work. Drawing on social cognitive and control theories, the proposed model includes cognitive, environmental, and control factors as antecedents of ISSP. The findings of this study could be used to develop effective security policies and training. They could also be used to develop effective security audits and further recommendations for organizations that are looking to make significant improvements in their information security profiles.

Categories and Subject Descriptors

K.6.5 Security and Protection

General Terms

Security, Human Factor, Standardization.

Keywords

Information Security Behavior; Mandatoriness; Social Cognitive Theory; Control Theory; Information Security Practices; Self-Efficacy; Security Standards; ISO27002.

1. INTRODUCTION

Researchers have realized that the majority of the problems in regards to information security are indirectly caused by employees' disobeying the information security policies of their organizations (Warkentin, Shropshire & Johnston, 2007; Whitman & Mattord, 2008). As security threats have grown, the need to protect organizational data has become a corporate crucial need. Although some of these attacks originate externally, most of them are intentionally or unintentionally originated by internal employees (Dhillon & Backhouse, 2000).

Stanton et al., (2003) pointed out that information security research has focused more on technical aspects of information security while ignoring its human factors. According to Mackenzie (2006) "… more than half of all security breaches are due to social engineering and end users' careless behavior". This means that, even if the technical layer is efficient, the security position of organizations depends on users' behavior. Even though information security has been seen as a technical issue, its members are formed only with technicians (Collete & Gentile, 2006). In focusing on the technical side, information security has overlooked the human factor which is frequently called the weakest point of a security chain (Angel, 1993). Human errors can cause severe security breaches in organizations. Hence, human factors are important and have been picked up by both the research community, and Information Systems security practitioners (Parker, 1998, 1999; Peltier, 2000, Siponen, 2000a, 2000b; Straub 1990). For example, Hinson (2003) points out that simple configuration mistakes by humans in the area of information security can leave networks ports open, firewalls vulnerable and information systems completely unprotected. Many organizations evaluate their technology for security risks, evaluating new products and testing the systems. But very few assess risks in regards to their employees (Hinson, 2003).

2. SIGNIFICANCE OF THE STUDY

The problem is how to encourage good individual security practices at work. There are many naive user behaviors that can cause negative effects on information security unintentionally. To design and prepare a more efficient security program for individuals, it is necessary to understand the factors that encourage good individual behavior (Rhee, Kim & Ryu, 2009). Siponen et al. (2009) point out that if individuals understand how vulnerable their organization is to security threats, they are more likely to comply with information security policies. Individuals' compliance with information security policies is a psychological

SIGMIS-CPR'15, June 4–6, 2015, Newport Beach, CA, USA.

http://dx.doi.org/10.1145/2751957.2751966

phenomenon, the theoretical model of this research was developed from behavioral theories such as social cognitive and control theory. These theories may shed light on factors influencing individual information security practices (IISP) at work.

In contrast to previous studies about information security that applied socio cognitive theory (SCT) using only one variable for Self Efficacy (Rhee et al., 2009), this study adopts the Compeau and Higgins (1995) model used in an information systems context. Compeau and Higgins (1995) took into consideration different factors of Social Cognitive Theory (SCT) such as "the encouragement of use by others", "the actual use of computers by others", and "the organizational support for computer use" that influence self-efficacy and outcome expectations. In this study, the researcher adopts the variables that were used by Compeau and Higgins (1995) and used in the information security practices model.

S. Boss, Kirsh, Angermeier, Shingler, and R. Boss (2009) used Control Theory in Information Systems to predict "precautions taken in information security" using items developed from professional security standards and from general information security best practices published by the National Cyber Security Alliance (2005). I include the variables used by Boss et al. (2009) for use in the information security practices model in addition to the ones used by Compeau and Higgins (1995) applied in computer usage.

In this research paper uses the well-known international standards in information security (ISO17799/27002) to measure the construct of individual information security practices (IISP) at work. By following the recognized and tested ISO17799/27002 standard, organizations will improve the efficiency of managing their information security endeavors. ISO17799/27002 has a group of published documents that offers guides to manage better information security. By referencing ISO 17799/27002, financial institutions will have access to a group of library controls that can be included in the development of security architecture. That architecture can be integrated with other technology processes in order to create policies, standards, and procedures that can be used as a part of the governance structure that need to be done in organizations (FFIEC, 2014).

This study will be beneficial for all kinds of organizations that want to develop better information security procedures with a more standard approach. Therefore, this study can explain security practices as expected by all companies whose security policies are based on ISO17799/27002.

3. BACKGROUND LITERATURE, MODEL, HYPOTHESES

The current model integrates Compeau and Higgins (1995) and Boss et al. (2009) models into one model by adapting some variables from both studies within the information security context to see the impact on the dependent variable, individual information security practices (IISP) at work based on ISO17799/27002.

This model should be examined to evaluate the weight and importance of each of the components of the model. Given that, an individual's compliance with information security policies is a psychological phenomenon. Hence, the theoretical model of this research was developed from behavioral theories such as social cognitive and control theory. These theories are important in understanding factors influencing individual information security practices (IISP) at work based on ISO17799/27002

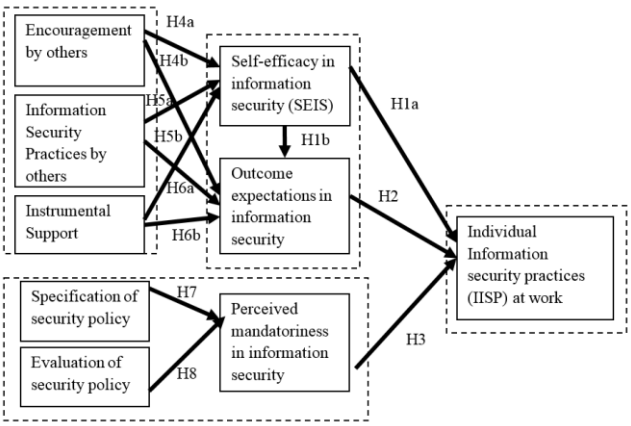

Figure 1 Research model.

3.1 Individual Information Security Practices (IISP) at work

Individual information security practices can be defined as preventive security behaviors (Straub, 1990) associated with desktop computer management, virus protection, and local-area-network security issues (Ryan, 2006). The repetition of an information security issue can show the way to regularity, structure, and knowledge transfer (Bartoli, Hermel &Ramis-Pujol, 2003) (As cited in Ryan, 2006, p.68). This results in a learned information security practice. In other words, IISP at work is the individual practices/behaviors that make the organizational information more secure.

Individual Information Security Practices (IISP) at work is related to guidelines and standards suggested by professionals in order to protect the assets of organizations (Ma & Pearson, 2005). The ISO27002 is the new name for ISO17799 standard and is the code of practice for information security (ISO, 2013). One of the best international standards well known in information security is ISO17799/27002. This standard provides good knowledge on information security in order to accomplish information security in organizations. According to Ma and Pearson (2005, p.4), information security professionals define best practices as guidelines, frameworks or checklists to protect the elements of the Information Systems. In addition, Theoharidou et al. (2005) point out that ISO17799/27002 is based on risk management which is accomplished via appropriate control measures to stop security threats. Given the flexibility and comprehensiveness of Information Security International Standard ISO17799/27002, it is taken as the basis of individual information security practices (IISP) at work.

3.2 Self-Efficacy in Information Security (SEIS)

There are different ways for individuals to show their efficacy. One of the effective ways that individuals expand to a more robust significance of efficacy is through experiences. Their performance accomplishments make them believe that they have the ability to perform a specific task well. Conversely, failures create self-doubts. To gain a sense of self-efficacy, individuals must overcome obstacles through effort. After individuals realize their capabilities through recurring successes, they can manage failures by being less negatively affected by them. Another way to strengthen self-belief is through modeling in which individuals

partially judge their capabilities in comparison with others (Bandura, 1994).

Rhee et al. (2009) suggested that SEIS might help explain current security practices and the intention to persevere in that effort. They define security practice as an "individual's information security risk management behavior involving two aspects: the adoption of security technology and security conscious care behavior related to computer and Internet usage". One is related to the use of security tools and features such as anti-virus software, anti-spyware, pop-up blocking function etc., and the other is in reference to security compliance behavior in using a computer and the Internet. Rhee et al. (2009) conclude that people who practice security care behavior and adopt security tools lower the vulnerability of information security. Based on the discussion above, there is a relationship between self-efficacy and the use of security tools. In this research, the construct of individual information security practices (IISP) at work will be based on the standard ISO 17799/27002 particularly in the areas of access control, compliance and information security policy with the objective of creating better security policies in organizations.
Therefore we predict that:

H1a: Individual's self-efficacy in information security (SEIS) is positively associated with individual information security practices (IISP) at work.

According to SCT, an outcome expectation is related to reward systems (Bartol & Srivastava, 2002) and is an important construct that can be used to explain and predict human behavior. It has three major forms: physical effects (i.e., pleasure, pain, and discomfort), social effects (i.e., social recognition, monetary rewards, power, and applause) and self-evaluation effects (i.e., self-satisfaction, self-devaluation). Therefore, human behaviors can be regulated by one of these different forms of effect (Bandura, 1997; Compeau & Higgins, 1995a). There are two types of outcome expectations (performance-related outcome expectations and personal outcome expectations) that deal with an individual's belief and reaction about the ability to proficiently use computers. Therefore we predict that:

H1b: Individual's self-efficacy in information security (SEIS) is positively associated with an individual's outcome expectations in information security.

3.3 Outcome Expectations in Information Security (OEIS)

An outcome expectation is an important construct that is used to explain and predict human behavior (Albion, 2001; Davis, 1989; Delcourt & Kinzie, 1993). Hence, it motivates individuals to carry on behaviors over extended periods of time if they believe their actions will generate desired results. According to Lent, Brown & Hackett (1994), outcome expectations are related to the anticipated outcomes of an action. For example, "If I regularly use my security tools, I will have more secure systems". In the context of information security, outcome expectations can motivate individuals to keep up information security behaviors if they believe their actions will generate a desired result. Thus,

H2: An individual's outcome expectations in information security is positively associated with individual information security practices (IISP) at work.

3.4 Perceived Mandatoriness in Information Security (PMIS)

According to Venkatesh and Davis (2000), mandatoriness is based on the individual's perceptions of forced use of technology. A major amount of studies in Information Systems describe mandate in different ways; as a black box where individuals decide whether to react positively or negatively to the mandate, as a one- time decision to obey or reject the mandate, and finally as orders that come from management (Chae & Poole, 2005).Markus (1983) explains how some users accepted and some resisted the implementation of a financial system whose use was mandated by management. Other authors such as Sussman and Siegal (2003) analyze the use of e-mail which is not directly mandated by management. They propose that the acceptance of email services is not voluntary for individuals at any modern organization. According to Brown et al. (2002), individuals respond accordingly to a continuous mandate when they consider a policy mandatory or voluntary. Boss et al. (2009) in their study describe mandatoriness as the "degree to which individuals perceive that compliance with existing security policies and procedures is compulsory or expected by organizational management".

Based on Ouchi (1977, 1979) (As cited in Boss et al., 2009, p.5), a control system needs to be implemented to observe and evaluate individual behavior against some standard. A mandate from management in regards to policy can persuade individuals to follow the code of practice for information security. According to D'Aquila (2001), management expectations play a big role on individual behavior. Therefore, if individuals perceive that the code of practice for information security ISO17799/27002 is mandatory, they are more likely to have a better individual information security practices (IISP) at work.

H3: The higher the individual's perceived mandatoriness of compliance with existing information security policies and procedures, the higher the individual information security practices (IISP) at work.

3.5 Encouragement by others (ENCO)

Keyvani and Mozafari (2009, p.4) state that encouragement is "a process that focuses on the individual's resources and potentials to enhance self-esteem and self-acceptance". In addition, encouragement focuses on any resource that can be turned into an asset or strength (Keyvani & Mozafari, 2009). According to Dreikurs (1981), people need encouragement in a way that plants need water.

The encouragement of others has to do with situations where an individual looks to find guidance on behavioral expectations. This might influence both self-efficacy and outcome expectations (Compeau & Higgins, 1995).

Compeau and Higgins (1995) found out that encouragement by others (family, friends and subordinates) to use computers did not represent an important source of persuasion as when persuasion came from peers and superiors.

Similarly, it is expected that encouragement by others (peers and superiors) may influence self-efficacy in information security (SEIS) and personal outcome expectations in information security related to the use of information security tools as hypothesized in this study.

H4a: High encouragements by others in the use of information security tools positively affects an individual's self-efficacy in information security (SEIS).

H4b: High encouragements by others in the use of information security tools positively affect individual's outcome expectations in information security.

3.6 Information Security Practices by Others (ISPO)

Compeau and Higgins (1995) point out that the use of technology by others can be applied as a foundation of information in forming self-efficacy and outcome expectations. From a psychological perspective, behavior acquisition is done through learning by observation (Latham & Saari 1979; Manz & Sims 1986; Schunk 1981). Bandura (1977) points out that an individual learns new information and behavior by watching other individuals. That process is called observational learning which is mainly based on live and verbal instruction. Live model has to do with the actual individual showing the behavior to others, and a verbal instruction model describes and explains the behavior. According to Bandura et al. (1977), learning by observation influences behaviors through the influence on self–efficacy, i.e. the more frequent the use of information security practices by others, the higher the individual self-efficacy in information security. And it also influences outcome expectations by revealing the possible consequences of the behavior (Bandura, 1971).

In the context of information security, it is expected that others' practice (peers and superiors) may influence SEIS and outcome expectations in information security with regards to the use of information security tools, which is hypothesized in this study.

H5a: The more frequent the Information Security Practices by others in one's reference group is, the higher the individual's Self-efficacy in information security (SEIS) will become.

H5b: The higher the Information Security Practices by others in one's reference group, the higher the individual's outcome expectations in information security.

3.7 Instrumental Support (ISUP)

Social Cognitive Theory (SCT) conceives support as one of the factors that positively affect self-efficacy (Compeau & Higgins, 1995). Organizations give computer support to individuals who need it. Therefore, individuals are supposed to enhance their ability and their perceptions of their ability to manage a specific task (i.e. computer use). Support can also influence outcome expectations meaning that the organization's posture toward individuals' behavior might answer questions about the possible consequences of computer use (Compeau & Higgins, 1995).

In terms of information security, the availability of assistance as a type of support improves the user's security behaviors that could significantly reduce the organization's size of security related overhead and drive down the level of severity of security incidents. Therefore we predict that:

H6a: The higher the instrumental support to individuals for information security in the organization, the higher the individual's self-efficacy in information security (SEIS).

H6b: The higher the instrumental support for information security in the organization, the higher the individual's outcome expectations in information security.

3.8 Specification of security policy (SOSP)

One of the features of practicing control is the specification of desired behaviors or outcomes that come regularly in the form of formal documented procedures (Eisenhardt, 1985; Kirsch, 2004). These policies give controllers flexibility to align desired behavior with organizational goals with the purpose of achieving a particular objective (Lorange & Scott-Morton, 1974; Kirsch, 2004). Understandable policies give a clear path to the individual with the target of achieving the desired behavior. For example, a security policy might say, "Employees are to log off their computers when not at their desks." Another well- specified information security policy could be "Report/forward any suspicious e-mails (ones that request personal or organizational data, called 'phishing') that are not caught by the organizations' spam filter to the IS security workers for assessment" (S. Boss, Kirsch, Angermeier, Shingler, &R. Boss, 2009). Schneider et al. (2005) point out that the action of specifying a desired behavior shows the way to perceptions of mandatoriness on the part of individuals. Based on the above discussion, I propose that the specification of the existence of corporate information security policy might be seen by individuals as a mandatory.

H7: The higher the specification of security policy is, the higher the perceived mandatoriness in information security will be.

3.9 Evaluation of security policy (EVSP)

Evaluation is an essential part of control that can be described as the analysis of collected data with the intention of evaluating individual's compliance with specific behaviors or outcomes (Jaworski, 1988; Kirsch, 2004). If management never evaluates compliance, policies will be disregarded by employees (Boss et al., 2009).

People in charge of evaluation decide if the result has been accomplished or whether the individual has demonstrated desired behaviors by following written policies. Evaluation is based on formal documentation that measures current status and makes modifications accordingly. Auditors usually evaluate individual's behavior based on the log file. Another type of evaluation is hands-on where personnel of the organization evaluate the individual's machine to check for compliance. The requirement is for individuals to perceive compliance with existing policies as crucial to management. In addition, management needs to show all individuals in the organization that they view compliance with the policy as mandatory (S. Boss, Kirsch, Angermeier, Shingler, & R. Boss, 2009).

H8: The higher the individual's evaluation of security policy, the higher the perceived mandatoriness of compliance with existing security policies and procedures.

4. RESEARCH DESIGN METHODOLOGY

4.1 Data Collection Procedure

The link of the online survey was distributed via e-mail to individuals who have experience working with Information Systems as end users.

4.2 Reliability and Validity

The measurement items suggested in this research study were selected from previous research studies, some items were used in their original form and others adapted for the information security context of this study. It is critical for each reflective measurement instrument that its reliability and validity Cronbach alpha coefficients were used to determine the internal consistency reliability of each instrument composed of multiple items. Content validity refers to whether the selected items capture the total scope of the construct as described by the construct's domain (Straub et al., 2000). Construct validity will be assured through literature review related to construct's domain (Peter et al., 2007).

The construct individual information security practices (IISP) at work was adapted from Ma and Pearson (2005) study of "best practices" with ISO17799. Ma and Pearson covered ten ISO17799/27002 security dimensions composing of 36 security practices for self-assessment, reassessing the information security practices of business partners, and the independent evaluation of information security management within the business organization. To my knowledge, no studies were done at the individual level using ISO17799/27002. After analyzing each question of the sections of ISO11799/27002, I managed to adapt twenty five questions covering five different security areas applied to the individual level. The reliability of the constructs in the categories of information security policy, asset classification and control, system access control, systems development and maintenance, communications and operations management was above .8.These five categories are part of the ISO17799/27002 standard but each section has its own group of questions that are part of the individual information security practices (IISP) at work.

Assessing reliability of the construct self-efficacy in information security (SEIS), the authors Rhee, Kim and Ryu (2009) calculated Cronbach's alpha with a result value of .965 and the factor loadings for SEIS were greater than .8. The rest of the constructs' reliability of this research was above .7. According to Nunnally (1978), .7 is acceptable for Cronbach's Alpha. The factor loadings were greater than .7. The survey items that measured SEIS construct included questions developed by Rhee, Kim and Ryu (2009) for the protection of the information.

Outcome expectations have been considered by many researchers including Davis (1989) and Davis et al. (1989) who used the term "usefulness" to reflect beliefs (or expectations).The authors measured perceived usefulness in regards to using IBM-PC based graphic system (Chart Master). All of the items were taken and adapted to information security context. For example the question "Using Chart Master in my job would enable me to accomplish tasks more quickly" was changed to "Information Security systems enable me to accomplish tasks more quickly". The reliability of the construct "perceived usefulness" was .97.

Perceived mandatoriness in information security was taken from the study of Boss, Kirsch, Angermeier, Shingler, & Boss (2009). The reliability of this construct was above .8.

The effects of encouragement by others, was taken from the study of Compeau and Higgins (1995) who studied if the use of computers was encouraged by others. This construct was adapted in the context of information security to evaluate if the use of information security tools was encouraged by others. The study shows that the reliability of this construct was above .7.

Compeau and Higgins (1995) pointed out that the behavior of others with regard to the use of technology was the basis of information used to develop individual's self-efficacy and outcome expectation. They used a 5-point likert -type scale to evaluate the items. These items were taken as they are and applied to the information security context in order to evaluate information security practices by others. This construct's reliability was above .7

In this study, all the items were measured with a 7-point likert-type scale to become more reliable varying from "Strongly Disagree" to "Strongly Agree".

4.3 Structural Model Analysis

This research model was evaluated using a SEM (structural equation modeling) method to test the research hypotheses. SEM was performed in Smart PLS which is a predictive technique that can handle multiple independent, mediating and dependent variables even when predictors display multicollinearity like in the present research study. In addition, it simultaneously models the structural paths (i.e., theoretical relationships among latent variables) and measurement paths (i.e., relationships between a latent variable and its indicators) (Chin, Marcolin, & Newsted, 1996). SEM can concurrently test the convergent validity and discriminant validity of the scales used to measure theoretical constructs and the proposed related links between theoretical constructs like in the present research study (Lowry, & Gaskin, 2014).

5. PRESENTATION OF RESULTS

5.1 Hypothesis Testing Results

The results of t-values and path coefficients are shown in table 1 (t>1.65; *p<0.1, t >1.96;**p < .05, t>2.57;***p<0.01). Path coefficients values and the significance of the relationships are shown in figure 2.Those values describe how strong the effect of one variable is on another variable. Most of the paths coefficients are significant except the paths between ENCO->SEIS and ISPO->OEIS. When the size of the outcome t-value is above 1.96, it is assumed that the path coefficient is meaningfully different from 0 at a significance level of 5 percent. The critical t-values for significance levels of 1 percent and 10 percent probability of error are 2.57 and 1.65 respectively (Noppa, 2010). According to (Hair, Hult, Ringle and Sarstedt, 2013) the rule of thumb for sample sizes of up to about 1000 observations, the path coefficients with values above 0.20 are usually significant and those with values below 0.10 are usually not significant.

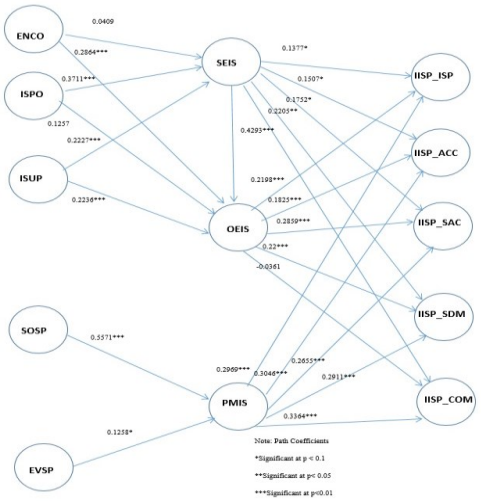

Figure 2 Path coefficients

Hypothesis 1, which predicts that Individual's self-efficacy in information security (SEIS) is positively associated with individual information security practices (IISP) at work, was supported. SEIS affected individual information security practices (IISP) at work in regards to IISP_ISP (1.679>1.65; *p<.10; significant), IISP_ACC (1.793 >1.65; p<.10; significant), IISP_SAC (1.947> 1.65; *p<.10, significant), IISP_SDM (2.360>1.96; **p< .05; significant) and IISP_COM (5.119> 2.57;***p< .01; significant). In addition, it affected positively

individual's outcome expectations in information security (OEIS) (2.577>2.57; ***p<.01; significant). Hypotheses that had low effect size (coefficient less than .2) were the following SEIS-> IISP_ACC, SEIS->IISP_ISP, and SEIS->IISP_SAC. This means that self-efficacy had low effect size on individual information security practices (IISP) at work in regards to communications and operations management, information security policy and system access control.

Hypothesis 2, which predicts that Individual's outcome expectations in information security is positively associated with individual information security practices (IISP) at work was supported. OEIS predicted IISP at work in regards to IISP_ISP (3.028>2.57; ***p<.01; significant), IISP_ACC (2.981>2.57; ***<.01; significant), IISP_SAC (3.537>2.57;***p<.01; significant), IISP_SDM (2.416>1.96;**p<.05; significant), but it did not affect IISP_COM (0.538>1.96, not significant).

Hypothesis 3, which predicts individual's perceived mandatoriness of compliance with existing information security policies and procedures, is positively associated with individual information security practices (IISP) at work was supported. PMIS predicted IISP at work in regards to IISP_ISP (3.509>2.57;***p< .01; significant), IISP_ACC (3.899>2.57; ***p< .01; significant), IISP_SAC (3.266>2.57;***p< .01; significant), IISP_SDM (3.050>2.57;***p< .01; significant), IISP_COM (4.755>2.57;***p< .01; significant).

Hypothesis 4, which predicts high encouragements by others in the use of information security tools is positively associated with individual's outcome expectations in information security was supported except the relationship with SEIS.ENCO predicted OEIS (2.937>2.57; ***p<.01 significant) but did not affect SEIS (0.479>1.96;**p< .05; not significant).This result supports the work of Compeau and Higgins (1995) which pointed out that encouragement of use of computing technology from family, friends and subordinates did not represent an important source of persuasion.

Hypothesis 5, which predicts that Information Security Practices by others (ISPO) in one's reference group is positively associated with individual's Self-efficacy in information security (SEIS) was supported except the relationship with OEIS. ISPO predicted SEIS (4.131>2.57; ***p< .01; significant).

Hypothesis 6, which predicts that instrumental support (ISUP) to individuals for information security in the organization, is positively associated with individual's self-efficacy in information security (SEIS) was supported. In addition, the relationship with OEIS was supported. ISUP predicted SEIS (2.681> 2.57; ***p< .01; significant) and OEIS (2.732> 2.57; ***p< .01; significant).

Hypothesis 7, which predicts that the specification of security policy (SOSP), is positively associated with perceived mandatoriness in information security (PMIS) was supported. SOSP predicted PMIS (7.666>2.57; ***p< .01; significant).

Hypothesis 8, which predicts that individual's evaluation of security policy (EVSP) is positively associated with perceived mandatoriness of compliance with existing security policies and procedures was supported (1.689>1.65; *p<.10; significant) but had low effect size (coefficient less than .2).

Hypotheses	Relationship	Path Coefficient	T-statistic	Hypothesis Support
H1a	SEIS -> IISP_ACC	0.1507	1.793	Yes *p<.10
H1a	SEIS -> IISP_COM	0.4285	5.119	Yes ***p<.01
H1a	SEIS -> IISP_ISP	0.1377	1.679	Yes *p<.10
H1a	SEIS -> IISP_SAC	0.1752	1.947	Yes *p<.10
H1a	SEIS -> IISP_SDM	0.2205	2.36	Yes **p<.05
H1b	SEIS -> OEIS	0.1912	2.377	Yes ***p<.01
H2	OEIS -> IISP_ACC	0.1825	2.981	Yes ***p<.01
H2	OEIS -> IISP_COM	-0.0361	0.538	No
H2	OEIS -> IISP_ISP	0.2198	3.028	Yes ***p<.01
H2	OEIS -> IISP_SAC	0.2859	3.537	Yes ***p<.01
H2	OEIS -> IISP_SDM	0.22	2.416	Yes **p<.05
H3	PMIS -> IISP_ACC	0.3046	3.899	Yes ***p<.01
H3	PMIS -> IISP_COM	0.3364	4.755	Yes ***p<.01
H3	PMIS -> IISP_ISP	0.2949	3.509	Yes ***p<.01
H3	PMIS -> IISP_SAC	0.2655	3.266	Yes ***p<.01
H3	PMIS -> IISP_SDM	0.2911	3.05	Yes ***p<.01
H4a	ENCO -> SEIS	0.0409	0.479	No
H4b	ENCO -> OEIS	0.2864	2.937	Yes ***p<.01
H5a	ISPO -> SEIS	0.3711	4.131	Yes ***p<.01
H5b	ISPO -> OEIS	0.1257	1.477	No
H6a	ISUP -> SEIS	0.2227	2.681	Yes ***p<.01
H6b	ISUP -> OEIS	0.2236	2.732	Yes ***p<.01
H7	SOSP -> PMIS	0.5571	7.666	Yes ***p<.01
H8	EVSP -> PMIS	0.1218	1.689	Yes *p<.10

Table 1 Results Summary of tested hypotheses

6. DISCUSSION OF FINDINGS

The outcomes of this study provide support for all of the research questions regarding Social Cognitive Theory and Control Theory assessment on Individual Information Security Practices (IISP) at work using ISO17799/27002.The following research questions were examined.

RQ1. How do encouragement by others, information security practices by others, and instrumental support affect self-efficacy in information security and outcome expectations in information security?

Encouragement by others (ENCO) was shown to have a positive effect on outcome expectations in information security (OEIS) that is statistically significant. The result of the analysis showed that encouragement by others in the use of information security tools affected individual's outcome expectations in information security (OEIS). The result is consistent with the predictions of the original hypothesis. This supports the work of Albion (2001), Davis (1989) and Delcourt & Kinzie (1993) in which they point out that outcome expectations motivates individuals to keep up with behaviors over extended periods of time if they believe their actions generate desired results. Hence, information security tasks are accomplished quickly and job productivity is increase if individuals are encouraged to use information security tools by peers, family, friends, and managers.

Information security practices by others (ISPO) was shown to have a positive effect on SEIS that is statistically significant but not on individual's OEIS. This result was intuitive to the original hypothesis; however given observational learning nature of ISPO in its social cognitive theory context, the positive influence is explained. Individual's SEIS is high when Information Security Practices are being followed by peers, family, friends, and managers. Individuals feel confident in handling different information security threats such as viruses and spywares. They are more confident in using different programs and applying security patches to the servers in order to protect the information against intruders. In addition, they are confident in learning advanced skills and using user's guide when help is needed to protect the information. This supports the work of Bandura (1977) in which he states that self-efficacy assumes, that different modes of influence change individual behavior in a way of generating self-perceptions of efficacy.

Instrumental support (ISUP) was shown to have a positive effect on SEIS and OEIS that is statistically significant. This result was

intuitive to the original hypothesis; however given the assistance nature of ISUP in its social cognitive theory context, the positive influence is explained. Individuals feel more confident in handling information security issues such as viruses, spywares and security patches, when individuals have guidance in the selection of information security tools. In addition, they have a specific person or a group available for assistance.

RQ2. How do cognitive factors such as self-efficacy in information security and outcome expectations in information security affect individual information security practices at work?

SEIS was shown to have a positive effect on IISP at work based on ISO17799/27002 that is statistically significant. This result was intuitive to the original hypothesis; however given the belief nature of SEIS in its social cognitive theory context, the positive influence is explained. SEIS directly affects Individual Information Security Practices (IISP) at work based on ISO17799/27002 in regards to information security policy, asset classification and control, system access control, system development and maintenance, and communications and operations management. Individuals are more effective in following information security policy, providing feedback to individuals responsible with the update and maintenance of the information security policy, and finally following management's intention to support information security programs. In addition, they are able to protect the information when they feel confident handling viruses, spywares, terms related to information security, web browsers to different security levels.

SEIS was shown to have a positive effect on OEIS and is statistically significant. This result was innate to the original hypothesis; however knowing the belief nature of SEIS in its social cognitive theory context, the positive influence is explained. Individuals are able to protect the information when they feel confident handling viruses, spywares, terms related to information security, web browsers to different security levels, and advanced skills.

OEIS was shown to have a positive effect on IISP at work based on ISO17799/27002 that is statistically significant. This result was innate to the original hypothesis; however knowing the motivation nature of OEIS in its social cognitive theory context, the positive influence is explained. OEIS directly affects Individual Information Security Practices (IISP) at work based on ISO17799/27002 in regards to information security policy, asset classification and control, system access control, system development and maintenance, but it does not affect communications and operations management. Individuals are more effective in following information security policies, providing feedback to individuals responsible with the update and maintenance of the information security policy, and following management's intention to support information security programs when information security systems support critical aspect of their job.

RQ3. How do individual perceptions about mandatoriness in information security influence individual information security practices at work?

Perceived mandatoriness in information security (PMIS) was shown to have a positive effect on IISP at work based on ISO17799/27002 that is statistically significant. This result was innate to the original hypothesis; however knowing the mandate nature of PMIS in its control theory context, the positive influence is explained. PMIS directly affects Individual Information Security Practices (IISP) at work based on ISO17799/27002 in regards to information security policy, asset classification and control, system access control, system development and maintenance, and communications and operations management. Individuals are more effective in following information security policies, providing feedback to individuals responsible with the update and maintenance of the information security policies, and following management's intention to support information security programs, when they comply with organization's security policies and procedures.

RQ4. How do specification and evaluation influence perceived mandatoriness in information security?

Specification of security policy (SOSP) was shown to have a positive effect on PMIS that is statistically significant. This result was innate to the original hypothesis; however knowing the specify nature of SOSP in its control theory context, the positive influence is explained. Individuals understand and comply with organization's security policies and procedures when they are familiar with organization's IT security policies, procedures and guidelines. This study extends the work of Schneider et al. (2005) who found out that the action of specifying a desired behavior shows the way to perceptions of mandatoriness. In addition, this study extends the work of S. Boss, Kirsch, Angermeier, Shingler, & R. Boss, (2009) who found out that policies give a clear path to individuals with the objective of achieving desired behaviors.

6.1 Limitations of the study

This study had to rely on self-reported data about individual information security practices at work. We do not know their practices for sure at work so we have to rely on self-reporting data. This could be problematic and could lead to common method bias.

A major limitation of this study is that 71% of the sample is younger than 29 years old, 70% does not have a bachelor's degree and 76% has less than five years of experience working with Information Systems. Hence, the sample is skewed towards younger individuals, less educated, and less experienced.

The survey of Individual Information Security Practices (IISP) at work was based on ISO 17799/27002. Since Information Security is a developing area that changes constantly, the latest ISO 27002:2013 standard has some improvements to maintain an adequate information security management system (Disterer, 2013). These improvements should be included in future research of IISP at work.

7. CONCLUSION

This research study concluded that cognitive forces of the social cognitive theory such as self-efficacy and outcome expectations applied to information security played an important role on individual information security practices (IISP) at work based on ISO17799/27002. In addition, self-efficacy and outcome expectations in information security were found to be positively influenced by encouragement by others, information security practices by others or instrumental support. Other findings were that elements of control such as specification and evaluating behaviors of security policy affected positively on perceived mandatoriness in information security. In addition, perceived mandatoriness in information security was effective in motivating individuals to follow information security practices at work based on ISO17799/27002. .

8. REFERENCES

[1] Albion, P. R. (2001). Some factors in the development of self-efficacy beliefs for computer use among teacher education students. Journal of Technology and Teacher Education, 9(3), 321-347.

[2] Angel, I. (1993, October, 1993). Computer security in these uncertain times: the need for a new approach. Paper presented at the Proceedings of the 10th international conferences on computer security, audit and control (CompSec), London.

[3] Bandura, A. (1965). Influence of models' reinforcement contingencies on the acquisition of imitative responses. Journal of Personality and Social Psychology, 1(6), 589-595.

[4] Bandura, A. (1971). Influence of Models' Reinforcement Contingencies on the Acquisition of Imitative Responses. In A. Bandura (Ed.), Psychological Modeling: Conflicting Theories (pp. 112-127). Chicago, IL.

[5] Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84, 191-215.

[6] Bandura, A. (1977). Social Learning Theory. Englewood Cliffs, New Jersey: Prentice Hall.

[7] Bandura, A. (1977). The self and mechanisms of agency. In J. Suls (Ed), Social psychological perspectives on the self. Hillsdale, N.J.: Erlbaum, in press.

[8] Bandura, A. (1978). Reflections on Self-Efficacy in Advances in Behavioral Research and therapy. Pergamon Press, 237-269.

[9] Bandura, A. (1982). Self-efficacy Meachism in Human Agency. American Psychologist, 37(2), 122-147.

[10] Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. NJ: Prentice Hall.

[11] Bandura, A. (1988). Self-Regulation of motivation and action through goal systems. Dordrecht, Netherlands: Kluwer Academic Publishers.

[12] Bandura, A. (1989). Human Agency in Social Cognitive Theory. American Psychological Association, 44(9), 1175-1184.

[13] Bandura, A. (1994). Self-efficacy. In Ramachaudran (Ed.), Encyclopedia of human behavior (Vol. 4, pp. 71-81). New York: Academic Press: Academic Press.

[14] Bandura, A. (1997). Self-efficacy: The exercise of control. New York: W.H. Freeman and Company.

[15] Bandura, A. (2002). Social Cognitive Theory in Cultural Context. Applied Psychology: An International Review, 51(2), 269-290.

[16] Bandura, A., Adams, N., & Beyer, J. (1977). Cognitive Processes Mediating Behavioral Change. Journal of Personality and Social Psychology, 35(3), 125-139.

[17] Bartol, K., & Srivastava, A. (2002). Encouraging knowledge sharing: the role of organizational reward systems. Journal of Leadership and Organizational Studies, 9(1).

[18] Bartoli, A., Hermel, P., & Ramis-Pujol, J. (2003). Innovation Assessment as a management information tool: a case study. Measuring Business Excellence, 7(2), 6-20.

[19] Boss, S., Kirsch, L., Angermeier, I., Shingler, R., & Boss, R. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151.

[20] Brown, S.A., Massey, A.P., Montoya-Weiss, M.M., Burkman, J.R. (2002). Do I really have to? User acceptance of mandated technology. European Journal of Information Systems112002;, 283–295.

[21] Chae, B., & Poole, M. (2005). Mandates and technology acceptance: a tale of two enterprise technologies. Journal of Strategic Information Systems, 14(2), 147-166.

[22] Chin, W. W., Marcolin, B. L., & Newsted, P. R. (1996). A Partial Least Squares Latent Variable Modeling Approach For Measuring Interaction Effects: Results From A Monte Carlo Simulation Study And Voice Mail Emotion/Adoption Study. Proceedings of The Seventeenth International Conference On Information Systems.

[23] Collete, R., & Gentile, M. (2006). The security architect: bridging the gap between business, technology and security. The Information Systems Security Association Journal, 42-44.

[24] Compeau, D. R. and C. A. Higgins (1995a). "Application of social cognitive theory to training for computer skills." Information Systems Research 6(2): 118-143.

[25] Compeau, D. R., & Higgins, C. A. (1995b). Computer self-efficacy: Development of a measure and initial test. MIS Quarterly, 19(2), 189-210.

[26] Compeau, D., Higgins, C. A., & Huff, S. (1999). Social Cognitive Theory and Individual Reactions to Computing Technology: A longitudinal study. MIS Quarterly, 23(2), 145-158.

[27] D'Aquila, J. M. (2001). Financial accountants' perceptions of management's ethical standards. Journal of Business Ethics, 31(3), 233-244.

[28] Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of information Technology. MIS Quarterly, 13(3), 319-340.

[29] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). USER ACCEPTANCE OF COMPUTER TECHNOLOGY: A COMPARISON OF TWO THEORETICAL MODELS. Management Science, 35(8), 982-1003.

[30] Delcourt, M. A., & Kinzie, M. B. (1993). Computer technologies in teacher education:The measurement of attitudes and self-efficacy. Journal of Research and Development in Education, 27(1), 35-41.

[31] Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. Communications of the ACM, 43(7), 125-128.

[32] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(2), 92-100. Retrieved from http://search.proquest.com/docview/1349963585?accountid=28844

[33] Dreikurs, R. (1981). Social Equality: The Challenge of today. Chicago: Alfred Adler Institute.

[34] Eisenhardt, K. M. (1985). Control: organizational and economic approaches. Management Science, 31(2), 134-149.

[35] FFIEC. (2014). Architecture Considerations. Retrieved from http://ithandbook.ffiec.gov/it-booklets/information-security/information-security-strategy/architecture-considerations.aspx?prev=1

[36] Hair, J., Hult, T., Ringle, C., & Sarstedt, M. (2013). A Primer on partial least Squares Structural Equation Modeling (PLS-SEM): SAGE Publications, Inc.

[37] Hinson, G. (2003). "Human factors in information security." Innovative information security awareness programs: 5.

[38] ISO. (2013). Introduction To ISO 27002 (ISO27002). Retrieved from http://www.27000.org/iso-27002.htm

[39] ISO-17799. (2000). Information technology, code of practice for information security management. Geneva: International Standards, Organisation.

[40] Jaworski, B. (1988). Toward a theory of marketing control: environmental context, control types, and consequences. Theory of Marketing Control, 52, 23-39.

[41] Keyvani, A., & Mozafari, M. (2009). Encouragement, Punishment, Offering New Solutions. International Journal of Management Perspectives, 1(4), 74-85.Lucie Press.

[42] Kirsch, L. (1996). Contextual influences on self-control of IS professional engaged in systems development. Accounting, Management, & Information Technology, 6(3), 191-219.

[43] Kirsch, L. J. (2004). Deploying common solutions globally: The dynamics of control. Information Systems Research, 15(4), 374-395.

[44] Latham, G. P., & Saari, U. M. (1979). Application of Social-Learning Theory to Training Supervisors through Behavioral Modeling. Journal of Applied Psychology, 64(3), 247-246.

[45] Lent, R., Brown, S., & Hackett, G. (1994). Toward a unifying social cognitive theory of career and academic interest, choice, and performance. Journal of Vocational Behavior, 45, 79-121.

[46] Lorange, P., & Scott-Morton, M. (1974). A framework for management control systems. Sloan Management Review, 16(1), 47-56.

[47] Lowry, P., & Gaskin, J. (2014). Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATION, 57(2), 36.

[48] Ma, Q., & Pearson, J. M. (2005). ISO 17799: "Best Practices" in information security management? Communications of the Association of Information Systems, 15, 577-591.

[49] MacKenzie, K. (2006). Employees may be opening doors to criminals. Retrieved from http://www.ft.com/cms/s/458807fe-efec-11da-b80e-0000779e234

[50] Manz, C. C., & Sims, H. P. (1986). Leading self-managed groups: A conceptual analysis of a paradox. Economic and Industrial Democracy, 7(141-165).

[51] Markus, M. L. (1983). Power, politics, and mis implementation. Communications of the ACM, 26(6), 430-444.

[52] NCSA. (2005). Top Ten Cybersecurity Tips. National Cyber Security Alliance, Washington DC.

[53] NIST. (1998). Information technology training requirements: A role and performance-based model. Washington D.C.: U.S. Department of Commerce.

[54] Noppa. (2010). How to Run SmartPLS. Retrieved from https://noppa.lut.fi/noppa/opintojakso/ab40aj200/luennot/instructions.docx

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

[56] Ouchi, W. (1979). A conceptual framework for the design of organizational control mechanisms. management Science, 25(9), 833-848.

[57] Peltier, T. (2000). How to build a comprehensive security awareness program. Computer Security Journal, 16(2), 23-32.

[58] Peter, S., Straub, D., & Rai, A. (2007). Specifying Formative Constructs in Information Systems Research. IS Research, 31(4), 623-656.

[59] Rhee, H., Kim, C., & Ryu, Y. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computer & Security, 28(8), 816-826.

[60] Ryan, James Emory (2006) A comparison of information security trends between formal and informal environments. Ph.D. dissertation, Auburn University, United States -- Alabama. Retrieved October 22, 2007, from ProQuest Digital Dissertations database. (Publication No. AAT 3225287).

[61] Schneider, F., Gruman, J., & Coutts, L. (2005). Applied Social Psychology: Understanding and Addressing Social and Practical Problems. Thousand Oaks, CA: Sage Publications.

[62] Schunk, D. (1981). Modeling and Attributional Effects on Children's Achievement: A self-efficacy analysis. Journal of Educational Psychology, 73(1), 93-105.

[63] Siponen, M. (2000a). A conceptual foundation for organizational IS security awareness. Information Management & Computer Security, 8(1), 31-41.

[64] Siponen, M. (2000b). Critical analysis of different approaches to minimizing user-related faults in information system security: implications for research and practice. Information Management & Computer Security, 8(5), 197-209.

[65] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31.

[66] Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270.

[67] Siponen, M., Mahmood, A., & Pahnila, S. (2009). Are Employees Putting Your Company At Risk By Not Following Information Security Policies? Communications of the ACM, 52(12), 145-147.

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

[69] Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 24(6), 472-484.

[70] Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. Management Science, 46(2), 186-204.

[71] Warkentin, M., Shropshire, J., & Johnston, A. (2007). The IT security adoption conundrum: an initial step towards validation of applicable measures. Proceedings of the 13th Americas Conference on Information Systems.

[72] Whitman, M., & Mattord, H. (2008). Management of Information Security (2nd ed.). Boston, Ma: Thompson Course Technology.