Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives

Quynh N. Nguyen
University of North Texas
Quynh.Nguyen@unt.edu

Dan J. Kim
University of North Texas
Dan.Kim@unt.edu

Abstract

Effective information security (InfoSec) management cannot be achieved through only technology; people are the weakest point in security and their behaviors such as inappropriate use of computer and network resources, file sharing habits etc. cannot be controlled by security technologies. Although the importance of individuals' InfoSec behaviors has been widely recognized, there is limited understanding of what impact individual users InfoSec protection behavior. Thus, focusing on the relationships among risk propensity, InfoSec self-efficacy, InfoSec protection efforts from several theoretical lenses, the study proposes a research model to explain individuals' intention to reinforce their InfoSec protection and empirically validates the proposed model. The results of the study are expected to provide a deeper understanding of the relationships among risk propensity, self-efficacy, risk perception, InfoSec protection efforts, and InfoSec reinforcement intention.

1. Introduction

With the increase of computer and Internet usage, information security (InfoSec) has become an important issue. In the US, the total average cost of cyber-crime in 2015 was $15 million [23]. Previous studies have been focused on using security technologies to enhance InfoSec in organizations. However, InfoSec cannot be achieved through technology alone; effective organizational InfoSec depends on all three components: people, processes, and technology. People present a weak point in security and their behaviors such as inappropriate use of computer and network resources, file sharing habits etc. cannot be controlled by security technologies [14]. Careless computing habits and improper online behaviors can threaten not only the security and privacy of their own personal data but also the safety of organization information system structure.

Although the importance of individual InfoSec behavior has been recognized, there is limited understanding of what impact computer users' InfoSec behavior [3]. There is a need for a sociotechnical approach to InfoSec research. Therefore, this study identifies the factors that impact on computer users' protection intention. Focusing on the relationships among risk propensity, InfoSec self-efficacy, InfoSec risk perception, and InfoSec protection efforts from several theoretical lenses, the study proposes a research model to explain individuals' intention to protect their InfoSec and validates the proposed model using empirical data. The results of the study are expected to provide a deeper understanding of what factors impact on InfoSec protection efforts and InfoSec reinforcement intention.

More specifically, the study mainly focuses on two research questions: 1) How does risk propensity associate with InfoSec risk perception, InfoSec protection effort and InfoSec reinforcement intention? 2) How does InfoSec self-efficacy associate with InfoSec risk perception, InfoSec protection effort and InfoSec reinforcement intention?

The paper is organized as follows: First, it begins with literature review of InfoSec and theoretical foundations. Next, we propose the research model and hypotheses. Third, we present the research methodology. Then, we analyze data and come up with the results. This lead to explanation in discussion part. The paper concludes with a discussion about the limitations and future research opportunities.

2. Theoretical background

2.1 Information security

The term "Information Security" has many definition covering technical, behavioral, managerial, philosophical, and/or organizational approaches [31]. For the purpose of this research, we focus on the behavioral aspect on an individual level, because the human factor is a key component of InfoSec. In 2013, according to US census bureau, 83.8 percent of US

URI: http://hdl.handle.net/10125/41763
ISBN: 978-0-9981331-0-2

households owned a computer (desktop, laptop and handheld computer), and 74.4 percent of US household had internet access. Personal computers and internet access are now necessary parts of daily life and have become an important virtual setting for everyday living and work. Individual computer users are more vulnerable to InfoSec threats, because in the home environment, individual computer users are not required to comply with strict InfoSec policies, trained to conduct safe computing, or protected by InfoSec staffs like in a corporate environment. Therefore, home computers are more exposed to security threats like computer viruses, data loss, identity theft, etc.

The majority of InfoSec research focus on employees' security behavior in organization [29], which is understandable since employee security behavior significantly impact on organization. With the increase of internet usage and technologies, more people work at home or continue their work outside the office. So personal computer becomes the work computer but with less security protection, thus behavioral InfoSec research has given more attention to home computer users. Many studies conducted with both employees and home users suggest that preventive behavior are influenced by threat and coping appraisal, which a key tenant of protection motivation theory (PMT). When an individual is aware of security threats, he or she will form beliefs about the perceived severity and probability of the threat, which are then evaluated against the beliefs formed about the efficacy of potential response [3]. However, these factors are not sufficient to explain what drives InfoSec protection intention.

Previous study indicates that a home computer user's intentions are formed by a combination of cognitive, social, and psychological components [3]. They suggest that the most effective messages in the context of online security behavior may be the messages that focus on the positive outcomes of performing security behavior, not the ones focus on potential negative outcomes of not following the security procedures. Other research by Ifinedo [16] show that factors such as self-efficacy, attitude toward compliance, subjective norms, response efficacy, and perceived vulnerability positively influence information systems security policy behavioral compliance intentions of employees. Previous research has found that personality constructs can be used to explain even more variance in behavior, providing understanding of user behavior. Therefore, it is important to identify what type of personality that affect security behavior and protection intention.

2.2 Theory of reasoned action and theory of planned behavior

Our research model is based on the Theory of Reasoned Action (TRA) by Ajzen and Fishbein (1969) [1] and the Theory of Planned Behavior (TPB) [2], the two best known theoretical models of behavior. The TRA proposes that human intention to perform or not to perform an action (behavioral intention) is the immediate antecedent of the actual behavior. The TRA states there are two factors that affect behavioral intention: attitude toward the behavior and subjective norms. Attitude is defined as a person's positive or negative feelings toward performing the behavior. Subjective norms is defined as a person's perception of what people important to them think about performing a behavior.

The TPB extends the TRA developed by Ajzen and Fishbein. This theory adds perceived behavioral control as a factor that influences behavioral intention. Perceived behavioral control is the perception of how easy or difficult it would be to perform the behavior. According to TPB, human behavioral intention is affected by subjective norms, attitude towards the behavior, and perceived behavioral control [2], and each reveals a different aspect of the behavior and can be used in attempts to change it. People are expected to follow their intentions when they have motivation and some actual control over the behavior in question. Therefore, behavioral intentions are assumed to be the immediate antecedent of actual behavior [2]. The TPB is a useful conceptual framework for explaining the complexity of human social behavior. It has been widely used across differing domains.

The efficacy of the TRA model and the TPB model is supported by many empirical research studies, reviews [20] and meta-analyses [4]. In InfoSec security domain, previous studies have supported that a person's intention to comply with an information system security procedure is influenced by his or her attitude, subjective norms, and perceived behavioral control [13]. Therefore, numerous information system security studies have used the TPB to examine InfoSec behavior and individual's behavioral compliance with InfoSec policies [6].

2.3 Self-efficacy in information security

According to social cognitive theory, individuals actively seek and interpret information, and use that information to guide subsequent behaviors [22]. Self-efficacy is an important aspect of social cognitive theory. Bendura [10] explains self-efficacy as a form of self-evaluation which is determinant of individual behavior, self-efficacy refers to one's belief about his

or her own capabilities to organize and execute the actions successfully. In other word, self-efficacy is what an individual believes he or she can achieve using his or her knowledge, and skills. Self-efficacy influences human motivation, the amount of effort, self-regulation, and persistence of human efforts when they face specific circumstances or obstacles [8].

Self-efficacy theory proposes that people are more likely to engage in activities in which they have a high level of self-efficacy [11]. In other words, people's motivation and courses of action are determined by how people believe they can do the work effectively [8]. Previous research on self-efficacy indicates that judgments of self-efficacy can be measured along three basic scales: magnitude, strength, and generality. Self-efficacy magnitude measures the difficulty level of the task [11]. Self-efficacy strength measures the amount of conviction an individual has about performing a specific task [11]. Generality of self-efficacy refers to the extent to which self-efficacy on one task generalizes to other tasks in similar situations [19].

In the information systems context, Compeau and Higgins define computer self-efficacy as an individual judgment of one's capability to use a computer [15]. Previous research on computer end-user behavior has examined the role of computer self-efficacy [28]. Researchers in InfoSec have adapted the general term computer self-efficacy to a specific construct: InfoSec self-efficacy. InfoSec self-efficacy can be defined as one's belief in his or her capability to protect information and information systems from security threats, loss, unauthorized access, etc. [24]. Findings from previous research indicate that people with a high level of InfoSec self-efficacy use more security software, set stronger passwords, and conduct InfoSec practices frequently. In sum, InfoSec self-efficacy is an important factor that impacts on users' InfoSec practices [16].

3. Research model and hypotheses

General technology awareness is defined as an individual's perception about the technological abilities to control InfoSec in general. InfoSec self-technical controllability can be defined as an individual's perception of his or her own technical ability to control InfoSec threats. When individuals notice that existing technologies are able to detect, control, and prevent an InfoSec attack, they are more likely to believe in the usefulness of the technologies. In other words, having access to technologies and knowing the effectiveness of technologies, individuals will perceive that they have higher technical-control of InfoSec threats. Thus, we hypothesize:

Hypothesis 1a: General technology awareness is positively associated with InfoSec self-technical controllability.

We define InfoSec self-efficacy as individuals' beliefs about their ability to protect their information and computer systems from InfoSec threats. Previous research in the InfoSec domain has proved that individuals who have a high level of perception in technology's abilities to control threats to InfoSec in general will have stronger belief in their own abilities to control InfoSec threats and protect their computers at a personal level [24]. Thus, hypothesis H1b is proposed as follows:

Hypothesis 1b: General technology awareness is positively associated with InfoSec self-efficacy.

Because InfoSec self-technical controllability measures how people perceive their technical abilities to execute security practices to avoid InfoSec threats, it would have an effect on individuals' self-efficacy in InfoSec. When people perceive that they have technical abilities to conduct security practices, they will believe more in their own abilities to control InfoSec threats. People become more confident in themselves and their abilities to handle InfoSec issues when they perceive they have high technical controllability. Thus, we hypothesize:

Hypothesis 2: InfoSec self-technical controllability is positively associated with InfoSec self-efficacy.

Information security protection effort is defined as a set of current practices of computer users to defend their valuable information from unauthorized access, use, disclosure, etc. It includes InfoSec practices such as installing and updating anti-virus software on a personal computer, using a firewall on a home network, using complicated passwords and different passwords for different websites, making back-up copies of important files frequently, etc. The influence of self-efficacy on InfoSec protection practice has been demonstrated in prior studies. Self-efficacy was found to be a significant predictor of the decision of home wireless network users to implement security features on their networks [30]. People with higher self-efficacy in InfoSec are more likely to use security protection software, they also demonstrate a high level of security conscious care behavior [24]. Therefore, the following hypothesis is proposed:

Hypothesis 3a: InfoSec self-efficacy is positively associated with InfoSec protection effort.

Information security risk perception is defined as an individual's belief about the chance of the occurrence of an InfoSec risk to his or her computer system. It's about how individuals perceive the chance

that their computer will face InfoSec breaches or how vulnerable their computer systems are. Risk compensation theory explains why people take risks. It states that individuals adjust their level of risk-taking behavior based on their sense of security [26]. Prior research on transportation safety argues that adding safety features to cars (such as air bags, seatbelts system, etc.) will encourage people to abandon their defensive driving skills; for example, they will increase their speed. The explanation is that they feel protected by the vehicle and safety systems [5]. While there is a debate about the support for risk compensation theory, the theory is still valid in predicting risk behavior in some situations. We argue that when people feel protected, they perceive that negative occurrences are less likely happen to them, thus they are more willing to take that risky action. So there is a relationship between people's perception of safety and their risk perception. We propose that when individuals have high InfoSec self-efficacy, they believe more in their abilities to control the InfoSec threats. Thus, they feel safer when using their computer systems. In other words, their perception of an InfoSec risk to their computer systems decreases. To conclude, we expect that individuals who have high InfoSec self-efficacy are likely to have lower InfoSec risk perception. Hypothesis 3b states this relationship:

Hypothesis 3b: InfoSec self-efficacy is negatively associated with InfoSec risk perception.

Information security reinforcement intention refers to individuals' future intention to strengthen their InfoSec protection practice. It implies that individuals will implement stronger security procedures, such as buying more software to protect their computers from InfoSec breaches, learning more about protection techniques, etc. Bandura [9] states that self-efficacy is one of the most important preconditions for behavior change because it determines coping behavior. Prior studies show that people's behavior is strongly influenced by their confidence in their abilities to perform certain behaviors [7]. In the TPB, the concept of perceived behavioral control is adapted from self-efficacy theory. Thus, self-efficacy is one of the determinants for future intention. In the computer use context, researchers indicate that computer self-efficacy has an effect on people's intentions to use computers in the future [21]. Rhee et al. [24] argue that intention to exert effort is an indicator of future behavior, and their findings support that individuals who have higher InfoSec self-efficacy will have stronger intentions to strengthen their InfoSec practices. Bulgurcu et al. [13] state that there is a significant relationship between an employee's self-efficacy in complying with the organization's InfoSec policy and his or her intention to comply. Consistent with their findings, we propose the following hypothesis:

Hypothesis 3c: InfoSec self-efficacy is positively associated with InfoSec reinforcement intention.

Research on risk has been conducted in various disciplines. In the information systems discipline, e-commerce area has studied how trust and risk affect consumer's intention and decision in online transaction [24]. Online consumer perceived risk is a consumer's belief about the potential uncertain negative outcomes from the online transaction [18]. Consumers' belief plays an important factor in their behavior. Previous research shows that consumer's trust and perceived risk have strong impacts on purchasing decisions. For this study, we look at risk in different aspect, by studying computer users' risky personality (risk propensity). For the purpose of this study, we define risk propensity as an individual current tendency to take risk; it is an individual trait that can change over time and is an emergent property of the decision maker. People who have high-risk

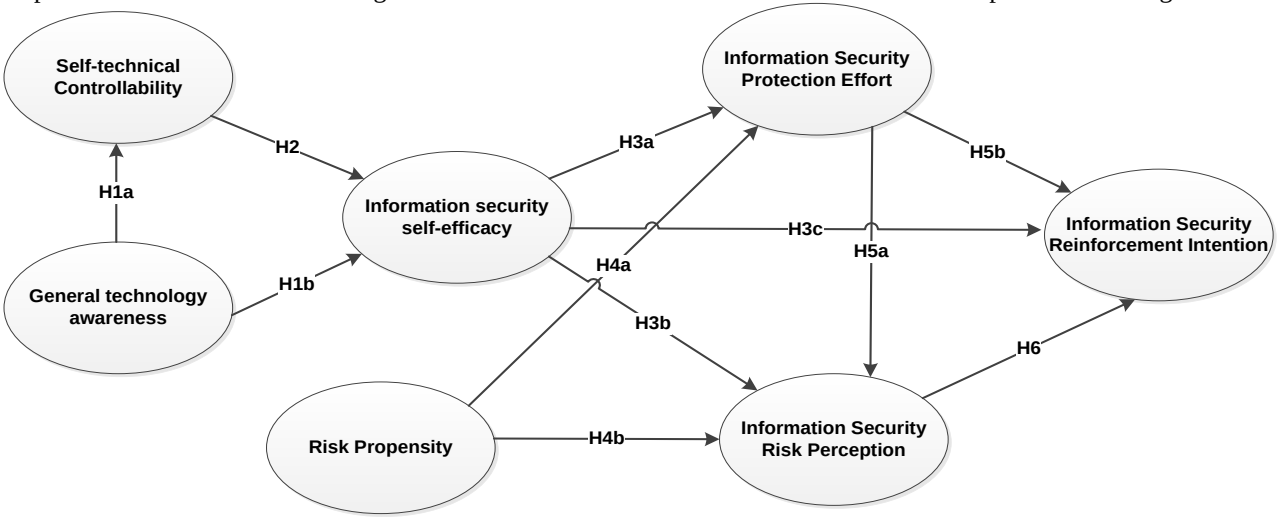

Figure 1. Research Model

propensity are more willing to do things that involve risk in order to achieve their goals. The effect of risk propensity on risky decision making were found to be mediated by perception of risk [25]. While using the Internet involves security threats like malware, data loss, unauthorized access, etc. users can protect themselves by using InfoSec protection solution. High-risk propensity person would less likely to use antivirus or malware prevention to prevent malicious threats from executing. To state in other way, an InfoSec protection practice would be viewed less favorably by people who have high-risk propensity. Thus, we hypothesize:

Hypothesis 4a: Risk propensity is negatively associated with InfoSec protection effort.

Some studies in risk literature support that people's risk perception in a specific situation is influenced by their propensity to take or avoid risks [12]. It means people who have risk-seeking propensity will perceive less risk than who have risk-averse propensity. They tend to recognize positive outcomes, overestimate the probability of gains, and underestimate the probability of loss, so it leads to lowering their risk perception. In other words, there is a significant negative relationship between risk propensity and risk perception [25]. However, other studies found that there is no significant effect of risk propensity on risk perception in decision making situation [17]. In the InfoSec context, we argue that people who have higher risk propensity level will perceive less InfoSec risk. They are more likely to underestimate InfoSec threats to their computers. The next hypothesis posits this relationship:

Hypothesis 4b: Risk propensity is negatively associated with InfoSec risk perception.

We propose that when individuals conduct strong InfoSec procedures, they will perceive less security threats toward their information systems. When people have anti-virus software on their computers, use wireless encryption feature in their wireless connection, check and apply security updates frequently, they will more likely to think that their computer systems are well secured. Knowing that they are being protected by different protection methods, they would feel safer when using their computers. They overlook the probability of risk, and they feel that security breaches are less likely happen to them. Thus, we hypothesize:

Hypothesis 5a: InfoSec protection effort is negatively associated with InfoSec risk perception.

When people have practiced InfoSec protection, it means they already have positive attitude toward the protection behavior and have knowledge about how to protect their computers. They have certain belief that their protection effort can help them to secure their computers from security threats. According to the TRA & the TPB, their belief and positive attitude will impact on their intention to have InfoSec protection in future. Because they already know how to conduct InfoSec protection, they probably will continue enforcing security procedure. At this point, they are familiar with InfoSec procedure, they have more knowledge about security techniques, so they probably have stronger intention to continue InfoSec protection in order to protect their computer better. They will not only continue protect their computers but also put more effort into protecting their information systems. The more effort they put on current InfoSec protection, the more likely they will strengthen their InfoSec protection intention in future. Thus, we hypothesize:

Hypothesis 5b: InfoSec protection effort is positively associated with InfoSec reinforcement intention.

When people perceive risk, they want to reduce risk. People who have weak InfoSec risk perception will be less willing to conduct InfoSec protection procedures. On the other hand, people who have strong InfoSec risk perception are more likely to protect their information systems. Thus, they have stronger intention to conduct one or more InfoSec protection procedures. We assume that when people perceive more risk about their computer systems, they are more likely to conduct stronger protection procedures to protect their computers. Thus, we propose that InfoSec risk perception has a positive relationship with InfoSec reinforcement intention. Hypothesis 6 states this relationship:

Hypothesis 6: InfoSec risk perception is positively associated with InfoSec reinforcement intention.

The model summarizes the proposed research hypotheses is presented in Figure 1.

4. Research method

4.1. Research design

To validate the propose research model, we had collected data using a questionnaire from students in a public university in the U.S. A total 248 respondents completed the survey. After removing incomplete and invalid responses, we have 244 usable responses. For analysis tool, we use Partial Least Squares (PLS), which utilizes a principle component-based for estimation.

4.2. Measures

We use multi-item scales to improve reliability and validity of measurement. InfoSec protection effort

construct was operationalized using formative scale items. Other constructs were operationalized using reflective scale items. This survey was conducted at the individual level. We captured demographic variables including age, gender, major, and employment status. Other control variables are computer experience, internet experience, computer ownership, computing literacy level, and internet literacy level.

5. Data analysis and results

The research model is validated through two-step analysis using SmartPLS 2.0. First, we test a measurement model to ensure the validity and reliability of measures before testing the proposed hypotheses (i.e., structure model testing). Then we conduct tests of significance for all paths using the bootstrapping method.

Table 1. Construct correlations, consistency and reliability of reflective constructs

Construct	CR	Alpha	AVE	Construct					
				GTA	RI	RPE	SE	RP	SC
General Technology Awareness (GTA)	0.783	0.582	0.548	**0.740**					
InfoSec Reinforcement intention (RI)	0.917	0.878	0.735	0.100	**0.857**				
InfoSec Risk Perception (RPE)	0.942	0.916	0.801	-0.169	0.203	**0.895**			
InfoSec Self-efficacy (SE)	0.947	0.938	0.620	0.443	0.152	-0.318	**0.788**		
Risk Propensity (RP)	0.752	0.358	0.605	-0.064	0.024	0.131	-0.066	**0.778**	
Self-technical Controllability (SC)	0.925	0.892	0.755	0.391	0.098	-0.255	0.567	-0.096	**0.869**

Note: 1) Composite reliability (CR), Cronbach's Alpha (Alpha), Average valance extracted (AVE); 2) Bold numbers on the diagonal are the square root of the AVE; 3) Off-diagonal elements are correlations among constructs.

Table 2. Loadings and cross-loadings

	General Technology Awareness (GTA)	InfoSec Reinforcement intention (RI)	InfoSec Risk Perception (RPE)	InfoSec Self-efficacy (SE)	Risk Propensity (RP)	Self-technical Controllability (SC)
GTA_01	**0.6588**	0.1288	-0.1549	0.3108	-0.0369	0.3122
GTA_02	**0.7664**	0.0736	-0.1581	0.3408	-0.0941	0.2592
GTA_03	**0.7887**	0.0205	-0.0622	0.3288	-0.0123	0.2927
RI_01	0.1046	**0.8925**	0.1699	0.1446	0.0560	0.1443
RI_02	0.0555	**0.9200**	0.1734	0.1350	0.0333	0.0977
RI_03	0.0337	**0.7831**	0.2291	0.0776	-0.0549	0.0641
RI_04	0.1475	**0.8260**	0.1308	0.1595	0.0395	0.0227
RPE_01	-0.0862	0.2147	**0.8249**	-0.2336	0.1692	-0.2158
RPE_02	-0.1724	0.1516	**0.9153**	-0.3159	0.1106	-0.2297
RPE_03	-0.1964	0.2307	**0.9359**	-0.2802	0.0656	-0.2127
RPE_04	-0.1463	0.1291	**0.9008**	-0.3083	0.1296	-0.2566
SE_01	0.3053	0.0250	-0.2263	**0.6860**	-0.1079	0.4270
SE_02	0.2700	0.0243	-0.2746	**0.7448**	-0.0480	0.4509
SE_03	0.3227	0.1620	-0.2754	**0.7883**	-0.0350	0.5025
SE_04	0.4001	0.1384	-0.2898	**0.8030**	-0.0155	0.4688
SE_05	0.3546	0.0852	-0.2843	**0.8284**	-0.0065	0.4733
SE_06	0.3501	0.1300	-0.3390	**0.8494**	-0.0112	0.4717
SE_07	0.3716	0.1622	-0.2176	**0.8222**	-0.1089	0.4333
SE_08	0.3693	0.2629	-0.2136	**0.8128**	-0.0536	0.3779
SE_09	0.3056	0.0741	-0.2234	**0.7475**	-0.0515	0.4566
SE_10	0.3821	0.1215	-0.2227	**0.8189**	-0.0491	0.4097
SE_11	0.3957	0.1111	-0.1784	**0.7468**	-0.0906	0.4320
RP_01	-0.0789	0.0147	0.0727	-0.0726	**0.8538**	-0.0620
RP_02	-0.0111	0.0244	0.1462	-0.0225	**0.6944**	-0.0951
SC_01	0.4124	0.0758	-0.2154	0.4810	-0.0726	**0.8673**
SC_02	0.3519	0.0575	-0.2268	0.5048	-0.0918	**0.9045**
SC_03	0.2664	0.1212	-0.2571	0.5118	-0.0914	**0.8310**
SC_04	0.3199	0.0841	-0.1882	0.4729	-0.0801	**0.8713**

5.1 Measurement model

The reliability and validity of the scales and measurements items are evaluated. For reflective constructs, the convergent validity is assessed by examining individual item reliability and construct reliability. The reliability of the scales is examined by two indicators: composite reliability (CR) and Cronbach's alpha. The composite reliabilities for each of the reflective constructs are all above the recommended 0.7 level to indicate internal consistency of the data. The Average Variance Extracted (AVE) is a measure of convergent validity and all AVE values in Table 1 are above the recommend minimum of 0.50, which mean at least 50% of measurement variance is captured by the latent construct.

Table 3. Error term, T-statistic, and VIF scores for formative items

	Weight	Standard Error	T-Statistics	VIF
PE_01	-0.0533	0.0632	0.8421 NS	1.6710
PE_02	0.1872	0.1061	1.7639 **	1.5520
PE_03	0.0924	0.0904	1.0224 NS	1.2780
PE_04	0.1797	0.0818	2.1976 **	1.1980
PE_05	0.2883	0.1026	2.8090 **	1.3620
PE_06	0.4175	0.0989	4.2211 ***	1.3340
PE_07	-0.0075	0.0972	0.0775 NS	1.2580
PE_08	0.1627	0.0971	1.6758 **	1.0650
PE_09	0.3092	0.0867	3.5663 ***	1.1000

Note: InfoSec protection effort (PE)
NS: not significant, * p < 0.1, ** p < 0.05, *** p < 0.001

The table of loadings and cross-loadings (table 2) shows each item loading highest on its assigned latent construct will all loadings above 0.5 (adequate value), those with values lower than 0.5 were deleted from the scales accordingly. In conclusion, the results show the study's measures are psychometrically adequate for this study.

For formative construct, the validity is examined by considering the results of a principal components analysis (PCA) and item weightings. Items are assumed to be valid if their weightings are significant.

We remove items that have no significant weightings. Reliability is examined by considering multi-collinearity among scale items by using variance inflation factor (VIF). As shown in table 3, all of the indicators' VIF values are lower than 5. VIF analysis indicates that the items are sufficiently reliable. In conclusion, the formative construct is valid and reliable.

5.2 Structural model

The structural model shows results about the path significance of hypothesized relationships using the path coefficients (β) and the squared R (R^2). The SmartPLS results for path coefficients and the R^2 are showed in figure 2. The path significance levels (t-values) are calculated by bootstrapping method. Table 4 summarizes the βs, t-value, and the results of hypothesis test. The results support hypotheses (H1a)

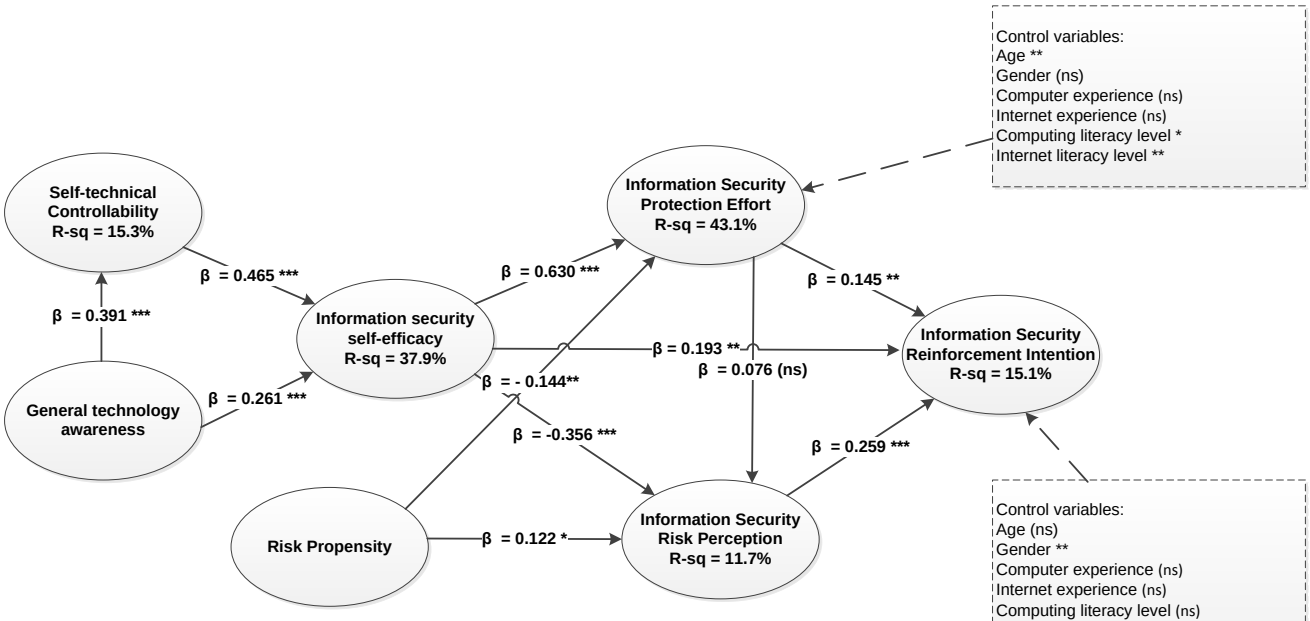

Figure 2. PLS Model

Note: NS: not significant, * p < 0.1, ** p < 0.05, *** p < 0.001

and (H1b) which suggest the positive relationship between general technology awareness with self-technical controllability and InfoSec self-efficacy. Hypothesis (H2) is supported to affirm that self-technical controllability is positively associated with InfoSec self-efficacy. Hypotheses (H3a, b, c) are supported to affirm the prediction indicating that InfoSec self-efficacy is associated with InfoSec protection effort, InfoSec risk perception, and future intention to reinforce protection.

Hypothesis (H4a) is also supported, which predicted that risk propensity is positively associated with InfoSec protection effort. Contrary to hypothesis (H4b), risk propensity has positive relationship with InfoSec risk perception. Hypothesis (H5a) is not supported, means there is no significant relationship between current protection effort and InfoSec risk perception. The result supports hypothesis (H5b), which indicates that current protection effort is positively associated with future reinforcement intention. Finally, the result indicates that InfoSec risk perception is positively associated with InfoSec reinforcement intention. Overall, the model explains 43.1% of the variance in respondents' InfoSec protection effort, and 15.1% of the variance in respondents' InfoSec reinforcement intention.

Table 4. Summary of the results

Hypotheses	β	t-value	Results
H1a: GTA -> SC	0.391 ***	5.594	Supported
H1b: GTA -> SE	0.261 ***	7.384	Supported
H2: SC -> SE	0.465 ***	5.661	Supported
H3a: SE -> PE	0.630 ***	11.898	Supported
H3b: SE -> RPE	-0.356 ***	4.622	Supported
H3c: SE -> RI	0.193 **	2.522	Supported
H4a: RP -> PE	-0.144 **	1.970	Supported
H4b: RP -> RPE	0.122 *	1.433	Contrary
H5a: PE -> RPE	0.076 NS	0.929	Not supported
H5b: PE -> RI	0.145 **	1.724	Supported
H6: RPE -> RI	0.259 ***	4.068	Supported
Note: NS: not significant, * $p < 0.1$, ** $p < 0.05$, *** $p < 0.001$			

Control variables (age, gender, computer experience, internet experience, computer ownership, computing literacy level, internet literacy level) are included in the model. Age, computing literacy level, and internet literacy level are found to have significant effects on InfoSec protection effort. Gender, and internet literacy level are found to have significant effects on InfoSec reinforcement intention. Computer experience, and internet experience have no significant effect on InfoSec protection effort and InfoSec reinforcement intention.

6. Discussion

By integrating three theories TRA, TPB, and self-efficacy theory, this research contributes to both theory and practice in the examination of how self-efficacy and risk-related variables are related to InfoSec protection intention. This research proposes a model that aims to enhance understanding about computer user InfoSec protection behavior and reinforcement intention. The study's results show that the model's independent variables explain an adequate amount of variance in the proposed model's dependent variable. InfoSec self-efficacy, InfoSec protection effort, and InfoSec risk perception are found to have positive effect on InfoSec reinforcement intention. Computer users' general technology awareness and InfoSec self-technical controllability would impact on their InfoSec self-efficacy.

6.1 Theoretical contributions

This study offers implication for InfoSec researchers. First, this study proposes and validates a research model that using TRA, TPB and self-efficacy theory to examine computer users' InfoSec protection reinforcement intention. The findings indicate that InfoSec self-efficacy, current protection behavior, and InfoSec risk perception are predictors for user's InfoSec reinforcement intention. In fact, InfoSec risk perception is found to have the strongest effect on protection intention. Therefore, TRA, TPB, and self-efficacy theory provide a better understanding of the factor that impact on computer users' InfoSec reinforcement intention.

Second, the study examines the role of risk propensity, a user characteristic, on InfoSec current protection effort and InfoSec risk perception. The results indicate that risk propensity has negative impact on InfoSec current protection effort. Contrary to literature in risk propensity, risk propensity has positively impact on InfoSec risk perception. When an individual has high risk propensity (risk-taking propensity), he or she are more willing to take risk. But it doesn't mean that individual perceives less InfoSec risk than risk-averter person, in fact, they perceive more InfoSec risk to their computers. Thus, the effect of risk propensity on risk perception depends on the domain. These findings on risk propensity has important implication. People's propensity to take risk or avoid risk can explain their intention to perform protection behavior. The explanation is risk propensity impacts on people's perception on InfoSec risk and their attitudes toward InfoSec protection behavior. According to TRA and TPB, attitude is an important antecedent of behavior intention. So examining risk

propensity in the framework of TRA and TPB offers researchers a new direction in investigating behavior intention.

Third, this study provides further support to findings in the extant literature that InfoSec self-efficacy does have effects on computer users' InfoSec protection effort and InfoSec reinforcement intention. Especially, InfoSec self-efficacy has strong effect on InfoSec protection effort. In conclusion, the study helps to develop a new understanding of InfoSec protection behavior of computer users.

Fourth, the results indicate that computer experience and internet experience have no effect on InfoSec protection effort and reinforcement intention. In other words, there is indifference in InfoSec protection between long-term computer users and newbies. People who use the systems for a longer time are not more likely to protect their computers and information than people who are new users. While experience is not an indicator for InfoSec protection, computing literacy level and Internet level are significant predictors for InfoSec protection. When users have higher level of expertise and familiarity with computers and internet, they have enough knowledge and skills to protect their computers from InfoSec threats. Therefore, these users are more likely to conduct InfoSec protection procedures and reinforce them.

6.2 Practical implications

This study also provides several practical implications. First, this research suggests that when computer users perceive high InfoSec risk, they are more likely to reinforce their InfoSec protection procedures. Many computer users do not recognize that they may have security threat when using computers and the Internet, or do not know how to protect their computers from cyberattack. Companies can enhance employees' InfoSec protection intention by informing them what kind of computer usage behavior are risky. Companies can launch InfoSec awareness campaigns and training for their employees. By providing employees with necessary knowledge and skills, companies can make positive change in InfoSec protection intention, which lead to strengthen InfoSec protection behavior and improvement in organizations' information system security.

Second, the findings indicate that when people already act on InfoSec protection procedures, they are more likely not only continue doing that in the future and but also put more effort on that. This is a positive finding for companies. When companies motivate their employees to have InfoSec compliance, they are not only enhancing employee protection behavior but also training them to get a new habit. Previous studies indicate that habit has a significant role in the context of employee's compliances with company InfoSec policies [27]. When InfoSec protection becomes a habit, employees will continue following InfoSec policies without strong enforcement from managers. They are accustomed to perform protection behavior. In order to achieve that, companies have to build a culture that encourage InfoSec compliances. Also, they need to set clear, feasible InfoSec policies so employees can perform them easily and effectively.

6.3 Limitation and future research

The study is about computer and internet usage behavior which some questions related to risky-behaviors. Those questions may make participants provide socially desirable responses. Also there are some questions that used technical terms like "file-sharing software" or "Web installed mobile codes" that some computer users may not be familiar with, so those kind of question will also influence the results. The sample of the study has a limitation to represent general population because most participants are college students.

This study examines what factors influence computer users' InfoSec protection behavior. There are several directions of the future research. Future research could continue examine users' characteristics and their influence on users' protection behaviors. Another potential study can also focus on InfoSec risk exposure behaviors in more specific situation like online shopping or social network sites with different cultural perspectives. In mobile social networking environments, for example, it would be an interesting study to example users' risk propensity and their influence on InfoSec protection behavior in countries with high and low uncertainty avoidance. Computer users in high uncertainty avoidance countries have a tendency to avoid uncertainty or risk, while users from low uncertainty countries might be more prone to take risk.

7. Conclusion

With the increasing number of security threats and cybercrimes, there is a need to understanding what influence people intention in InfoSec protection. This research examined InfoSec protection intention and reinforcement intention by drawing from relevant behavioral intention theories TRA, TPB, and self-efficacy theory. A survey of computer users' behavior and risk characteristic was conducted. The results show that InfoSec reinforcement intention is influenced by InfoSec self-efficacy, InfoSec risk

perception, and InfoSec protection effort. The study contributes to our understanding of InfoSec protection behavior.

8. References

[1] Ajzen, I. and Fishbein, M. The prediction of behavioral intentions in a choice situation. *Journal of Experimental Social Psychology 5*, 4 (1969), 400–416.

[2] Ajzen, I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes 50*, 1991, 179–211.

[3] Anderson, C.L. and Agarwal, R. Practicing Safe Computing: a Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly 34*, 3 (2010), 613–A15.

[4] Armitage, C.J. and Conner, M. Efficacy of the Theory of Planned Behaviour: A meta-analytic review. *British Journal of Social Psychology 40*, (2001), 471–499.

[5] Aschenbrenner, K.M. and Biehl, B. Improved Safety through improved technical measures? *Challenges to accident prevention. The issue of risk compensation behaviour*, (1994).

[6] Aurigemma, S. A Composite Framework for Behavioral Compliance with Information Security Policies. *Journal of Organizational and End User Computing 25*, 3 (2013), 32–51.

[7] Bandura, A., Adams, N.E., Hardy, A.B., and Howells, G.N. Tests of the generality of self-efficacy theory. *Cognitive Therapy and Research 4*, 1 (1980), 39–66.

[8] Bandura, A. *Social foundations of thought and action: a social cognitive theory / Albert Bandura.* 1986.

[9] Bandura, A. Self-Efficacy. *Encyclopedia of human behavio 4*, (1994), 71–81.

[10] Bandura, A. Exercise of personal and collective efficacy in changing societies. In *Self-efficacy in changing societies.* 1995, 1–45.

[11] van der Bijl, J.J. and Shortridge-Baggett, L.M. The theory and measurement of the self-efficacy construct. *Scholarly inquiry for nursing practice 15*, 3 (2001), 189–207.

[12] Brockhaus, R.H. Risk taking propensity of entrepreneurs. *Academy of Management Journal 23*, 3 (1980), 509–520.

[13] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. Information Security Policy Compliance: An Empiracal Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly 34*, 3 (2010), 523–548.

[14] Herath, T. and Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems 47*, 2 (2009), 154–165.

[15] Higgins, C.A. and Compeau, D.R. Development of a Measure and Initial Test. *MIS Quarterly 19*, 2 (1995), 189–211.

[16] Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security 31*, 1 (2012), 83–95.

[17] Keil, M., Wallace, L., Turk, D., Dixon-Randall, G., and Nulden, U. Investigation of risk perception and risk propensity on the decision to continue a software development project. *Journal of Systems and Software 53*, 2 (2000), 145–157.

[18] Kim, D.J., Ferrin, D.L., and Rao, H.R. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems 44*, 2 (2008), 544–564.

[19] Lunenburg, F.C. Self-Efficacy in the workplace: Implications for motivation and performance. *International Journal of Management, Business and Administration 14*, 1 (2011), 1–6.

[20] Madden, T.J., Ellen, P.S., and Ajzen, I. A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action. *Personality and Social Psychology Bulletin 18*, 1 (1992), 3–9.

[21] Marakas, G.M., Yi, M.Y., and Johnson, R.D. The Multilevel and Multifaceted Character of Computer Self-Efficacy: Toward Clarification of the Construct and an Integrative Framework for Research. *Information Systems Research 9*, 2 (1998), 126–163.

[22] Nevid, J.S. Psychology: Concepts and applications, 2nd ed. *Psychology: Concepts and applications, 2nd ed.*, 2007. http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=psyc5&NEWS=N&AN=2006-03419-000.

[23] Ponemon Institute. 2015 Cost of Cyber Crime Study: Global. October (2015).

[24] Rhee, H.S., Kim, C., and Ryu, Y.U. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security 28*, 8 (2009), 816–826.

[25] Sitkin, S.B. and Weingart, L.R. Determinants of Risky Decision-Making Behavior: a Test of the Mediating Role of Risk Perceptions and Propensity. *Academy of Management Journal 38*, 6 (1995), 1573–1592.

[26] Trimpop, R. and Wilde, G.J.S. *Challenges to accident prevention: the issue of risk compensation behaviour*. Styx, 1994.

[27] Vance, A., Siponen, M., and Pahnila, S. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management 49*, 3-4 (2012), 190–198.

[28] Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly 27*, (2003), 425–478.

[29] Warkentin, M. and Willison, R. Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems 18*, 2 (2009), 101–105.

[30] Woon, I.M.Y., Tan, G.W., and Low, R.T. A protection motivation theory approach to home wireless security. *Twenty-Sixth International Conference on Information Systems*, (2005), 367–380.

[31] Zafar, H. and Clark, J.G. Current state of information security research in IS. *Communications of the Association for Information Systems 24*, 1 (2009), 557–596.