FACTORS AFFECTING COMPUTER CRIME PROTECTION BEHAVIOR

Sirirat Srisawang, Thammasat Business School, Thammasat University, Bangkok, Thailand, sirirat.sr@gmail.com

Mathupayas Thongmak, Thammasat Business School, Thammasat University, Bangkok, Thailand, mathupayas@tbs.tu.ac.th

Atcharawan Ngarmyarn, Thammasat Business School, Thammasat University, Bangkok, Thailand, a_ngarmyarn@yahoo.com

Abstract

This research aimed to investigate factors that affect computer crime protection behavior, based on the protection motivation theory. Personal factors were considered, including: conscientious personality, perceived value of data, prior experience, and environmental factors. In addition, other factors were evaluated, including: subjective norm, security knowledge, and safeguard costs. These factors are mediated by threat appraisal and coping appraisal. The data were collected from 600 personal computer users by use of a questionnaire. Data were analyzed using structural equation modeling. Findings showed that all factors had significant effects on the computer crime protection behavior. In addition, the results showed that security knowledge, one of the environmental factors, had the strongest effects on coping appraisal which subsequently had the strongest impact on protection behavior.

Keywords: Protection Motivation Theory (PMT), Computer crime, Protection behavior.

1 INTRODUCTION

We lives in the computer age. Personal and mobile computers have proliferated, and have become an integral part of our everyday lives. Computer users, however, may not be fully mindful of cyber security. Valuable information can be obtained by criminal elements, such as through e-mail, internet banking, online shopping, instant messaging, online trading, etc. Computer users also confront various security threats in the cyber infrastructure (Anderson & Agarwal 2010).

Computer crime refers to any acts in which a computer or a network is used to harm others (Parker 2007). Computer crime has become a major area of concern for both law enforcement and the businesses sector. According to the computer crime and security survey in 2010, malware injection, phishing, computer thefts, and bots attacks have become relatively common means of attack to obtain sensitive information and subsequently cause so much damage (Richardson 2011).

The damage from computer crime drives organizations to adopt some protective measures such as technological measures (Ng, Kankanhalli, & Xu 2009). Technological measures are applied to reduce the chance of attacks using technical means, for example, antivirus software. Regulations and security policy are also widely used methods. Nevertheless, several studies indicate that many computer users do not follow the policy (Warkentin & Willison 2009). Such solutions are also insufficient for computer crime protection. This may be because the ultimate success of computer crime protection depends on the effectiveness of user behavior (Anderson & Agarwal 2010).

Based on the theory of behavioral prediction, previous studies tended to examine factors influencing personal behavior. Previous studies on end-user security behaviors often examine factors related to personal traits, cost-benefit considerations, organizational commitments, habits, etc. (Anderson & Agarwal 2010; Johnston & Warkentin 2010; Pahnilaa, Siponena, & Mahmoodb 2007; Zhang, Reithel, & Li 2009). However, a few studies have focused on the importance between personal and environmental factors. The main purpose of this study is to analyze factors that affect protection behavior and discern the importance between personal and environmental factors. Our research questions are:

Q1: What are the factors that affect users' behavior to protect computer crime?

Q2: Personal factors or environmental factors - which one most affects users' behavior to protect against computer crime?

2 THEORY

2.1 Computer Crime

Computer crime is caused by criminal or irresponsible actions of individuals who are taking advantage of the widespread use and vulnerability of computers, the internet and other networks (Gupta 2011). Dr. Debarati Halder and Dr. K. Jaishankar defined computer crime as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" (Halder & Jaishankar 2011). Such crimes may threaten the integrity, safety, and survival of most business systems. Thus, the development of effective security methods is a top priority.

Computer crime is defined by the Association of Information Technology Professionals (AITP) as including (1) the unauthorized use, access, modification, and destruction of hardware, software, and data; (2) the unauthorized release of information; (3) the unauthorized copying of software; (4) denying an end user access to his or her own hardware, software, and data; and (5) using or conspiring to use a computer or network resource to obtain property illegally.

2.2 Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT), which was developed by Rogers (Rogers 1983) expanded the health-related belief model in the social psychology and health domains (Rippetoe & Rogers 1987). Drawing from the expectancy-value theories and the cognitive processing theories, PMT was developed to help clarify fear appeals. The theory explains that if the threat can be perceived by people as fearful, they will be more cautious and prevent the possible threat (Humaidi & Balakrishnan 2012). PMT has been noted as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions (Anderson & Agarwal 2010). In essence, protection motivation emanates from both the threat appraisal and the coping appraisal. Threat appraisal describes an individual's assessment of the level of danger posed by a threatening event (Woon, Tan, & Low 2005). It is composed of the following two items: Perceived vulnerability and Perceived severity. The coping appraisal is defined as an individual's assessment of his or her ability to cope with and avert the potential loss or damage arising from the threat (Woon et al. 2005). Coping appraisals are made up of two subconstituents - perceived benefit and self-efficacy.

Previous research that has used PMT found it useful in predicting behaviors related to an individual's computer security behaviors both at home and in organizations (Anderson & Agarwal 2010; Crossler 2010; Herath & Rao 2009; Ifinedo 2011; Johnston & Warkentin 2010; Lee & Larsen 2009; Ng et al. 2009; Pahnilaa et al. 2007)

3 THE DEVELOPMENT OF HYPOTHESES

The research model in Figure 1 was developed based on PMT and various other research. We define each construct and present the related hypotheses below.

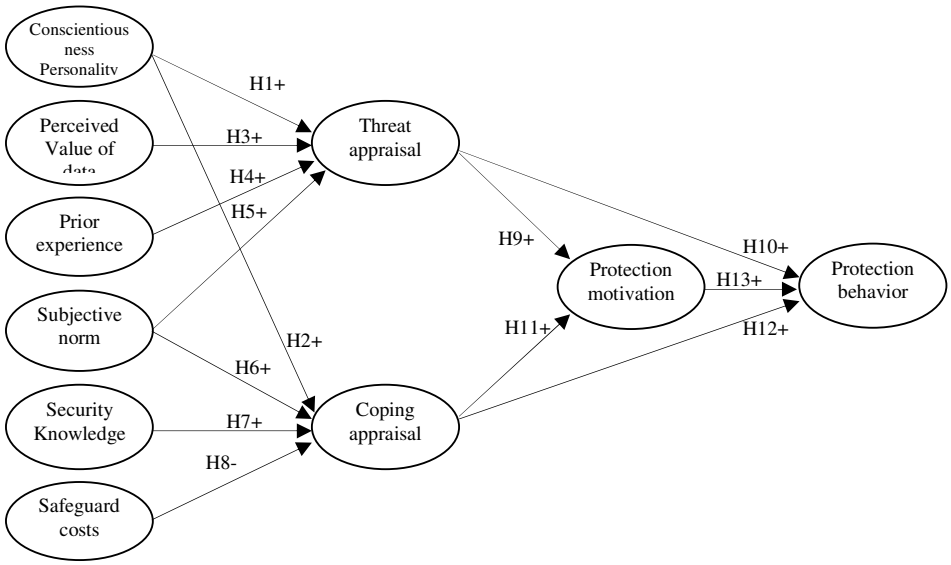


Figure 1. The Proposed Research Model

Conscientiousness Personality

One of the most widely accepted theories of personality is the five-factor theoretical model (McCrae & Jr. 2004). The five personality dimensions are extraversion, neuroticism, openness, agreeableness, and conscientiousness. Extraversion assesses the quantity and intensity of interpersonal interactions, neuroticism assesses the degree to which individuals are prone to emotional instability, openness assesses individuals' tendency to seek out new experiences, agreeableness assesses individuals' concern for cooperation and social harmony, and conscientiousness assesses organization and goal-directed behavior. These five dimensions are consistent across cultures, have high temporal stability,

and are extremely heritable (McCrae & Jr. 1987). The theory of challenge and threat states that in athletes (TCTSA) personality traits can affect the likelihood of athletes responding to goal-relevant performance situations with either coping appraisal or threat appraisal (Jones, Meijen, McCarthy, & Sheffield 2009). Previous research found that the conscientiousness personality induces greater awareness and goal-directed behavior (Devaraj, Easley, & Crant 2007) while insecurity and anxiousness tend to precautionary behavior (Vance, Suponen, & Pahnila 2009). Preliminary investigations have established that the traits of conscientiousness may be strongly linked with an individual employee's intention to comply with security policies and to adopt protective technologies (Siponen, Pahnila, & Mahmood 2006; Warkentin & Willison 2009). In addition, the conscientiousness personality factor strongly reinforces the threat and coping appraisal mechanisms theorized by PMT (Vance et al. 2009). Thus, this research proposes the following hypotheses:

H1: A conscientious personality positively affects threat appraisal.

H2: A conscientious personality positively affects coping appraisal.

Perceived value of data

Previous studies indicated that perceived value of information is a factor motivating individuals to perform the protection behavior (Chai, Sharmistha, Claudia, R., & J. 2009; Warkentin & Willison 2009). The value of data can also be viewed as monetary value and emotional value. An individual with valuable assets (i.e. data) tends to take security threats seriously and take precautionary actions to prevent those threats (Chai et al. 2009). Perceived value directly influences protection behavior such as installation and use of antivirus software (Warkentin & Willison 2009). In this study, we try to identify the effect of the perceived value of data of an individual on threat appraisal of PMT. Thus, this research proposes the following hypothesis:

H3: Perceived value of data positively affects threat appraisal.

Prior experience

An individual's past experience affects that person's decision making on behavior. Past experience about computer crime threats may include: Virus hits, computer security problems, breaches of privacy, etc. An individual who has had bad experience with computer crime is more likely to perceive threat seriousness and take some protective actions (Chai et al. 2009; Rhee, Kim, & Ryu 2009). Thus, this research proposes the following hypothesis:

H4: Prior experience positively affects threat appraisal.

Subjective norm

Subjective norm refers to the perceived social pressure to perform or not perform a given behavior (Ajzen 1991). Subjective norms influence the willingness of individuals to behave in accordance with security policies. Protection behavior of important people such as family, friends, leaders, or colleagues has an effect on recognizing the risks and severity of threats. It could also increase the ability of an individual to handle threats by acquiring the protective knowledge from those people (LaRose, Rifon, & Enbody 2008; Pahnilaa et al. 2007; Zhang et al. 2009). Social norms positively influence the intention to comply with the security protection behavior in the workplace (Pahnilaa et al. 2007) and home (Li & Siponen 2011). Thus, this research proposes the following hypothesis:

H5: Subjective norm positively affects threat appraisal.

H6: Subjective norm positively affects coping appraisal.

Security knowledge

Security knowledge has an influence on the learning process of an individual, which leads to protection motivation (Siponen, Pahnila, & Mahmood 2010). When computer users gain some knowledge about computer security, they will evaluate their ability to handle computer security threats (Bulgurcu, Cavusoglu, & Benbasat 2009, 2010). Organizations usually design training programmes for security purposes. Providing security knowledge education includes security events that usually occur in organizations, the risks confronted, the basic concepts of IS security, how to

establish good security habits, and recommended supports available when facing security problems. This helps computer users understand the current protections served - by technical control, formal control, law enforcement and others building up to ethical cyber behavior (Li & Siponen 2011; Lu & Jen 2010). In terms of communication, organizations have many options, with various media formats including newsletters, videos, handouts, leaflets, etc. In the home context, end users hardly receive any formal security knowledge training. Security knowledge mostly comes from self-learning and self-experience. In the case of home users, security awareness often arises after a crisis -the end user encounters a threat such as a virus, Trojan horse, a worm, etc., causing a compromise in data. The channels to influence home users include mass media, friends and family (Ng & Rahim 2005). Thus, this research proposes the following hypothesis:

H7: Security Knowledge positively affects coping appraisal.

Safeguard costs

Safeguard costs are defined as the perceived costs incurred by a user in performing a recommended coping behavior (i.e., installing and configuring antispyware software). This definition is in terms of the effort involved in using anti-spyware software, not the dollar cost of purchasing and updating the software (Chenoweth, Minch, & Gattiker 2009). Response cost is primarily seen in reference to the cost of implementing a security measure versus its potential benefits (Workman, Bommer, & Straub 2008). Individuals normally perform cost-benefit analysis before making a decision. They will be more motivated to use safeguarding measures if they realize the effectiveness of safeguarding measures and lower safeguard costs (Liang & Xue 2010). These efforts may increase or decrease the ability to handle threats. Safeguard costs have a negative relationship with behavior --as reducing safeguard costs will increase the likelihood of the respondent performing the recommended behavior (Woon et al. 2005). Prior research supports a negative impact of perceived costs on the protective behavior (Lee & Larsen 2009; Siponen et al. 2006; Woon et al. 2005; Workman et al. 2008). Thus, this research proposes the following hypothesis:

H8: Safeguard costs negatively affect coping appraisal

Threat appraisal

Threat appraisal refers to a person's assessment of the level of danger posed by the threat (Woon et al. 2005). Perceived threats relate to motivation to comply with security policies (Pahnilaa et al. 2007) and to perform security protection behaviour (Lee & Larsen 2009; Woon et al. 2005; Workman et al. 2008; Zhang et al. 2009). Different people perceive threats on different levels (Ng et al. 2009). When the threat level is high, users tend to experience emotional disturbance caused by the prospect of the threat (Liang & Xue 2009). The more a user perceives the magnitude of negative consequences resulting from threat incidents, the more he or she will implement protective actions (Lee & Larsen 2009; Liang & Xue 2009; Pahnilaa et al. 2007; Woon et al. 2005). In addition, threat appraisal also directly influences security behavior (Anderson & Agarwal 2010; Workman et al. 2008). Thus, this research proposes the following hypotheses:

H9: Threat appraisal positively affects protection motivation

H10: Threat appraisal positively affects protection behavior

Coping appraisal

Coping appraisal refers to the person's assessment of his ability to cope with and avert the potential loss or damage resulting from the danger (Woon et al. 2005). Coping appraisal is an important factor that drives the motivation and the willingness to comply with security policies and adopting security technologies and practices in organizations (Anderson & Agarwal 2010; Bulgurcu et al. 2010; Lee & Larsen 2009; Pahnilaa et al. 2007) and the home (Woon et al. 2005). In addition, coping appraisal also directly influences security behavior (Anderson & Agarwal 2010; Workman et al. 2008). Thus, this research proposes the following hypotheses:

H11: Coping appraisal positively affects protection motivation

H12: Coping appraisal positively affects protection behavior

Protection motivation

According to Social Learning Theory, an individual's behavior is influenced by the surrounding environment and his or her characteristics. Motivation is a good predictor of actual behaviour (Shropshire, Warkentin, Johnston, & Schmidt 2006; Siponen et al. 2006). Protection behavior will happen more often if individuals feel highly motivated (Bulgurcu et al. 2009; Herath & Rao 2009; Liang & Xue 2010; Ng et al. 2009). Thus, this research proposes the following hypothesis:

H13: Protection motivation positively affects protection behavior

4 RESEARCH METHODOLOGY

4.1 Samples and Data Collection

A survey-based approach using online questionnaires with convenience sampling was applied to test the proposed hypotheses. Subjects included both personal computer users in the home and the workplace in Thailand. Personal computers included desktop computers and notebook/laptop computers.

4.2 Measurement Development

We developed a questionnaire based on theoretical definitions and relevant literature. This questionnaire consists of 3 main sections. The first section collected demographic data of the respondents in a nominal scale. The second section surveys their computer security behavior in nominal scales and the third section reviews a respondent's opinions and computer crime protection behavior using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). Table 1 shows the measurement items.

Construct	Item	Measure Description	Source
Conscientiousness Personality: CP	CP1	I pay attention to details	(McCrae & Jr. 1987)
	CP2	I always follow the rules	(McCrae & Jr. 1987)
	CP3	I am persistent in the accomplishments of my work and ends	(McCrae & Jr. 1987)
	CP4	I get chores done right away	(McCrae & Jr. 1987)
Perceived Value of data: PV	PV1	I perceived importance regarding protecting computer from computer crime.	(Chai et al. 2009)
	PV2	Loss of data resulting from hacking is a serious problem for me	-
	PV3	I perceived importance regarding personal information	(Chai et al. 2009)
	PV4	I realize that I will be damaged if my computer was stolen or has been lost	(Chai et al. 2009)
Prior experience: PE	PE1	My friends often talk about bad things happening on their computer	(Chai et al. 2009)
	PE2	I have suffered from a computer security problem in the past	(Liang & Xue 2010)
	PE3	I had loss of important data because computer theft	(Chai et al. 2009)
	PE4	Have you ever had a virus on your computer in the past	(Chai et al. 2009)
Subjective norm: SN	SN1	My peers would think that I should take security measures on my primary computer to help secure the Internet	(Anderson & Agarwal 2010)
	SN2	Friends who influence my behavior would think that I should take measures to secure my primary computer	(Ifinedo 2011)
	SN3	My boss thinks that I should follow the organization's security policy	(Ifinedo 2011)
	SN4	My organization's IT department pressures me to protect the computer using antivirus software	(Anderson & Agarwal 2010; Ifinedo 2011)

Construct	Item	Measure Description	Source
Security Knowledge: SK	SK1	I attend the training class to help improve my awareness of computer and information security issues	(D'Arcy, Hovav, & Galletta 2009)
	SK2	My organization educates employees on their computer security responsibilities	(D'Arcy et al. 2009)
	SK3	I read information security bulletins or newsletters	(D'Arcy et al. 2009)
	SK4	I am interested in information about computer security	(D'Arcy et al. 2009)
Safeguard costs: SC	SC1	The inconvenience of implementing recommended IS security measures	(Liang & Xue 2010)
	SC2	Enabling IS security measures in my organization would be time consuming	(Siponen et al. 2010)
	SC3	There are too many overhead costs associated with implementing IS security measures in my organization	(Siponen et al. 2010)
	SC4	The cost of implementing recommended IS security policy measures is expensive	-
Threat appraisal: TA	TA1	I know my computer could be vulnerable to security breaches if I don't adhere to protection measures.	(Ifinedo 2011)
	TA2	It is extremely likely that crime will infect my computer	(Liang & Xue 2010)
	TA3	Threats to the security of my computer are harmful	(Liang & Xue 2010)
	TA4	The likelihood of an information security violation occurring at my workplace is likely	(Johnston & Warkentin 2010)
Coping appraisal: CA	CA1	I have the necessary skills to protect myself from information security violations	(Johnston & Warkentin 2010)
	CA2	I have the expertise to implement preventative measures to stop people from getting my confidential information	-
	CA3	For me, taking information security precautions is easy	-
	CA4	My ability to prevent information security violations at my workplace is adequate	(Liang & Xue 2010)
Protection Motivation: PM	PM1	I intend to comply with information security policies and follow the guidelines on how to use a computer safely	(Liang & Xue 2010)
	PM2	I intend to protect my computer from computer crime	(Siponen et al. 2010)
	PM3	I predict I would use antivirus/anti-spyware software	(Liang & Xue 2010)
	PM4	I intend to follow the security news and find out how to prevent computer crimes	-
Protection Behavior: PB	PB1	I installed antivirus software and keep it updated to prevent my computer from getting viruses and malware	(Liang & Xue 2010)
	PB2	I always follow the suggestions for using a computer safely and appropriately	(Liang & Xue 2010)
	PB3	I always follow the security policy whenever possible	-

Table 1. Measurement Items

A pre-test was conducted with fifty computer users to ensure that questionnaire items were clear and to identify any issues of concern to the survey participants. Minor adjustments were subsequently made to the survey instrument. The assessment of reliability was analyzed by calculating Cronbach's alpha coefficient. The Cronbach's alpha statistics of all constructs were over 0.7, showing that all measures had good reliability (Liang & Xue 2010).

5 DATA ANALYSIS

5.1 Respondents' Profile

The survey received 600 complete responses out of a total of 625 submitted surveys. Table 1 presents the distribution of respondents according to their gender, age, and educational level. Major respondents are female. Most people are in the age group between 26 and 35 years old. More than 50% of the respondents obtained a bachelor's degree.

Variable	Frequency	Percentage
Gender		
Male	279	46.50
Female	321	53.50
Age (Years)		
18–25	96	16.00
26–35	384	64.00
36–45	65	10.83
46–55	30	5.00
Over 55	25	4.17
Educational Level (Degree)		
Less than bachelor's degree	48	8.00
Bachelor's degree	306	51.00
Postgraduate degree	246	41.00

Table 2. Respondent's Profile

5.2 Analysis of the Measurement Model

The collected data were analysed using structural equation modeling (SEM). The measurement model of ten constructs was estimated using reflective indicators. Composite reliability was used to assess convergent reliability. The composite reliabilities for each of the study's constructs were all above the recommended 0.7 benchmark (Diamantopoulos & Siguaw 2000). Convergent validity was examined using AVE (Average Variance Extracted). Again, all constructs were well above the 0.5 benchmark (Diamantopoulos & Siguaw 2000).

Construct	CR	AVE	CP	PV	PE	SN	SK	SC	TA	CA	PM	PB
CP	0.87	0.63	**0.80**									
PV	0.92	0.74	0.20	**0.86**								
PE	0.92	0.74	0.47	0.23	**0.86**							
SN	0.91	0.72	0.40	0.48	0.33	**0.85**						
SK	0.93	0.77	0.50	0.27	0.46	0.32	**0.88**					
SC	0.95	0.84	-0.28	-0.16	-0.15	-0.12	-0.38	**0.91**				
TA	0.93	0.78	0.52	0.32	0.41	0.45	0.34	-0.16	**0.88**			
CA	0.89	0.68	0.53	0.26	0.39	0.40	0.67	-0.36	0.36	**0.83**		
PM	0.86	0.60	0.37	0.20	0.28	0.29	0.38	-0.20	0.42	0.53	**0.77**	
PB	0.86	0.66	0.46	0.23	0.33	0.35	0.55	-0.29	0.37	0.80	0.56	**0.82**

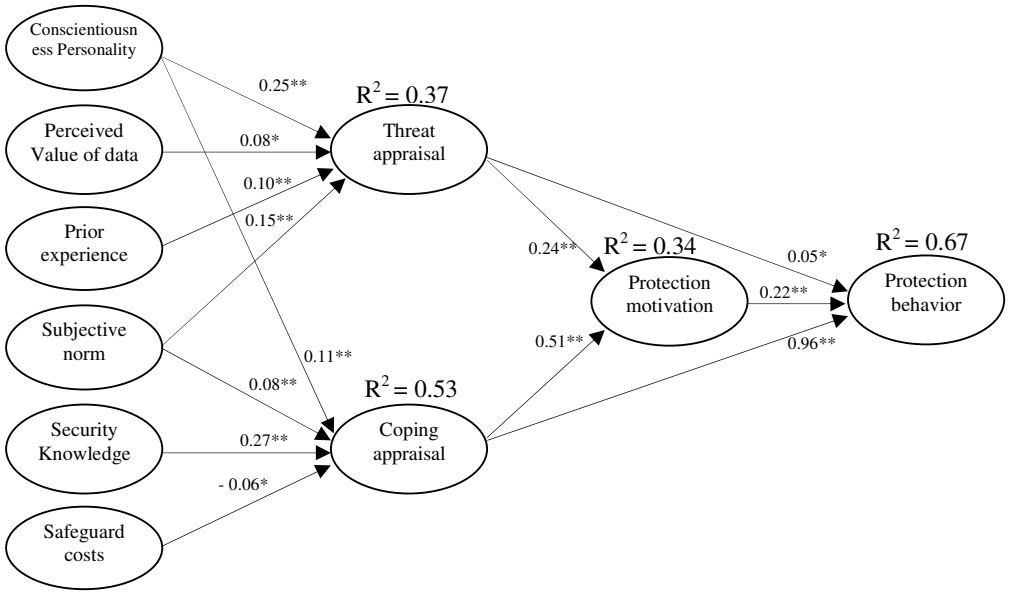
Table 3. Composite reliability (CR), Average valance extracted (AVE), and Correlations between constructs (diagonal elements are square roots of AVE)

Discriminant validity was tested via correlation matrix. As suggested by Fornell and Larcker (Fornell & Larcker 1981) the correlation of the construct was also compared with and the square root of AVE. The discriminant validity is assured when the following two conditions are met: (a) the value of the AVE is above the threshold value of 0.50; (b) the square root of the AVEs is larger than all other cross-correlations. Table 3 shows that the AVE ranged from 0.60 to 0.84, and in no case was any correlation between the constructs greater than the squared root of AVE. Overall, the results showed the study's measures were psychometrically adequate for this study. The values of AVE, composite reliability, and correlation are presented in Table 3. Hence, the reliability and validity of the constructs in the model are acceptable.

5.3 Analysis of the Structural Model

The hypotheses were tested by examining the structural model. The results, as shown in Figure 2 and Table 4, reveal that the model explains 67% of the variance of protection behavior. Protection motivation has a coefficient of 0.22; coping appraisal has a coefficient of 0.96 and threat appraisal

significantly has a coefficient of 0.05 affected protection behavior. Coping appraisal has a coefficient of 0.51 and threat appraisal has a coefficient of 0.24 significantly affecting protection motivation. It is interesting to find out that Conscientiousness Personality, Prior experience and Subjective norm are all significantly affecting threat appraisal. Conscientiousness Personality, Subjective norm, Security Knowledge are all significantly affecting coping appraisal equal to the level of significance of 0.001. Perceived Value of data is significantly affecting threat appraisal. Safeguard cost is significantly affecting coping appraisal equal to the level of significance of 0.01.



Chi-Square=1361.91, df=636, p-value=0.000, X^2/df = 2.14, CN = 298.10, GFI=0.90, AGFI=0.87, RMR= 0.030, RMSEA= 0.044

*Figure 2. The Results of the Structural Model Testing (*P<0.01; **P<0.001)*

Hypothesis (with Direction)	Path coefficient	t-statistic	Significance Levels	Result
H1: Conscientiousness Personality → threat appraisal (+)	0.25	7.72	P < 0.001	Supported
H2: Conscientiousness Personality → coping appraisal (+)	0.11	4.93	P < 0.001	Supported
H3: Perceived Value of data → threat appraisal (+)	0.08	2.88	P < 0.01	Supported
H4: Prior experience → threat appraisal (+)	0.10	3.45	P < 0.001	Supported
H5: Subjective norm → threat appraisal (+)	0.15	4.68	P < 0.001	Supported
H6: Subjective norm → coping appraisal (+)	0.08	4.13	P < 0.001	Supported
H7: Security Knowledge → coping appraisal (+)	0.27	10.62	P < 0.001	Supported
H8: Safeguard cost → coping appraisal (-)	-0.06	3.18	P < 0.01	Supported
H9: Threat appraisal → protection motivation (+)	0.24	6.58	P < 0.001	Supported
H10:Threat appraisal → protection behavior (+)	0.05	2.70	P < 0.01	Supported
H11: Coping appraisal → protection motivation (+)	0.51	9.61	P < 0.001	Supported
H12: Coping appraisal → protection behavior (+)	0.96	13.32	P < 0.001	Supported
H13: Protection motivation → protection behavior (+)	0.22	4.27	P < 0.001	Supported

Table 4. Standardized, and Significance Levels for Model

6 DISCUSSION

The results show that all the proposed hypotheses were supported. Consistent with the proposed research model, Conscientiousness, Subjective Norm, Prior experience and Perceived value of data were found as significant predictors of Threat appraisal respectively. Conscientiousness has a greater impact than other factors. The results of this study imply that computer users need to perceive the severity and likelihood of being threatened by computer crime. Motivated people tend to display greater awareness and goal-directed behavior. Moreover, increased dissemination of computer crime information through various media such as websites, TV and Newspaper etc. would likely increase the perception of computer crime.

Coping appraisal was significantly influenced by Security Knowledge, Subjective Norm, Conscientiousness, and Safeguard cost respectively. Ability to protect against computer crime of computer users is usually promoted through education and training programs that show the users what to do and why they should do it. Step-by-step installation procedures for these protective programs would be useful. Moreover, creating a culture well aware of computer crime will help encourage users to realize the importance of protection.

The most important factors affecting protection motivation were coping appraisal and threat appraisal. Coping appraisal had a greater impacted than threat appraisal. Therefore, to motivate users to protect their computer, efforts should be focused on coping appraisal. In addition, Protection behavior was affected by protection motivation and coping appraisal. Coping appraisal had a greater impact than protection motivation. Thus, this result confirms that the factors affected by coping appraisal should be encouraged, which help to increase the protection motivation and behavior as well. In addition, the result shows that Security knowledge, one of the environmental factors had the most important effect on coping appraisal which in turn directly affecting protection behavior.

7 CONCLUSIONS

Because computer users remain as the weakest link in computer crime protection, this study sought to explore the factors that affect human behavior in this regard. The factors consist of personal factors: conscientiousness personality, perceived value of data, prior experience, and environmental factors: subjective norm, security knowledge, safeguards cost. These factors were mediated by threat appraisal and coping appraisal. The data were collected from 600 personal computer users by application of a questionnaire. Data analyzed used structural equation modeling. Findings showed that all factors exerted significant effects on computer crime protection behavior. This study found that all factors were important to affect protection motivation and behavior. The results can be applied to guidelines and encourage computer users to preventive action to avoid victimization and abuse of computer crime.

Our findings show that a computer user's security knowledge had the strongest effects on coping appraisal which in turn leads to protection behavior. Thus, ensuring security knowledge can directly and indirectly alter computer users' motivation and in turn their protection behavioral. As an important practical implication of these results, providing security knowledge to computer users both home and workplace users will improve the ability to cope with and avert the potential loss or damage arising from computer crime.

This study applied the Protection Motivation Theory to study the computer crime protection behavior. Protection behavior is affected from protection motivation which emanates from both the threat appraisal and the coping appraisal. Findings suggest that threat appraisal and coping appraisal also directly affect the protection behavior.

Limitations of the study include the following: 1) this study focuses on only personal computer (i.e. PC, notebook, and laptop) users. Presently, the usage of tablets, smartphones or mobile devises has steadily increased. This is an important issue that must be addressed as a priority. Thus, future studies

should explore the users' protection behavior in other devices. 2) it is possible that Computer users in each group might have different reactions to protection behavior. Future research should compare different groups such as between IT and Non-IT people.

Reference

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, ScienceDirect, 50(2), 179-211.

Anderson, C. L., and Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS Quarterly, 34.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2009). Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance. AMCIS 2009 Proceedings, 419.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 334(3), 523-548.

Chai, S., Sharmistha, B.-S., Claudia, M., R., R. H., and J., U. S. (2009). Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens. IEEE Transactions on Professional Communication, 52(2), 167-182.

Chenoweth, T., Minch, R., and Gattiker, T. F. (2009). Application of Protection Motivation Theory to Adoption of Protective Technologies. 42nd Hawaii International Conference on System Sciences, 1-10.

Crossler, R. E. (2010). Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data. Proceedings of the 43rd Hawaii International Conference on System Sciences.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, 20(1), 79-98.

Devaraj, S., Easley, R. F., and Crant, J. M. (2007). Research Note - How Does Personality Matter? Relating the Five-Factor Model to Technology Acceptance and Use. Information Systems Research, 19(1), 93-105.

Diamantopoulos, A., and Siguaw, J. A. (2000). Introducing LISREL: A Guide for the Uninitiated: Sage Publications, London.

Fornell, C., and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement errors. Journal of Marketing Research, 18(1), 39-50.

Gupta, H. (2011). Management Information System (First Edition ed.).

Halder, D., and Jaishankar, K. (2011). Cyber Crime and the Victimization of Women: Laws, Rights and Regulations.

Herath, T., and Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18, 106-125.

Humaidi, N., and Balakrishnan, V. (2012). The Influence of Security Awareness and Security Technology on Users' Behavior towards the Implementation of Health Information System: A Conceptual Framework. 2nd International Conference on Management and Artificial Intelligence, 35.

Ifinedo, P. (2011). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers&Security, ScienceDirect, 31(1), 83-95.

Johnston, A. C., and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 34(3).

Jones, M. V., Meijen, C., McCarthy, P. J., and Sheffield, D. (2009). A theory of challenge and threat states in athletes.

LaRose, R., Rifon, N. J., and Enbody, R. (2008). Promoting personal responsibility for internet safety. Communications of The ACM - CACM, 51(3), 71-76.

Lee, Y., and Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems, 18, 177-187.

Li, Y., and Siponen, M. (2011). A Call for Research On Home Users' Information Security Behaviour. PACIS 2011 Proceedings, 112.

Liang, H., and Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. MIS Quarterly, 33(1), 71-90.

Liang, H., and Xue, Y. L. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journal of the Association for Information Systems, 11(7).

Lu, C.-C., and Jen, W.-Y. (2010). A Historical Review of Computer User's Illegal Behavior Based on Containment Theory. Journal of Software, 5(6), 593-599.

McCrae, R. R., and Jr., P. T. C. (1987). Validation of the five-factor model of personality across instruments and observers. Journal of Personality and Social Psychology, 52(81-90).

McCrae, R. R., and Jr., P. T. C. (2004). A contemplated revision of the NEO Five-Factor Inventory. Personality and Individual Differences, 36, 587-596.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. 46(4), 815-825.

Ng, B.-Y., and Rahim, M. (2005). A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security. PACIS 2005 Proceedings.

Pahnilaa, S., Siponena, M., and Mahmoodb, A. (2007). Employees' Behavior towards IS Security Policy Compliance. Proceedings of the 40th Hawaii International Conference on System Sciences.

Parker, D. B. (2007). The Dark Side of Computing: SRI International and the Study of Computer Crime. IEEE Annals of the History of Computing, 1058-6180.

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

Richardson, R. (2011). 15th Annual 2010/2011 Computer Crime and Security Survey.

Rippetoe, P. A., and Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. 52, 596-604.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. Social psychophysiology, 153-176.

Shropshire, J., Warkentin, M., Johnston, A., and Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. Americas Conference on Information Systems (AMCIS), 3443-3449.

Siponen, M., Pahnila, S., and Mahmood, A. (2006). Factors Influencing Protection Motivation and IS Security Policy Compliance. Innovations in Information Technology, 1-5.

Siponen, M., Pahnila, S., and Mahmood, A. (2010). Compliance with Information Security Policies: An Empirical Investigation. IEEE Computer Society, 43(2), 64-71.

Vance, A., Suponen, M., and Pahnila, S. (2009). How Personality and Habit Affect Protection Motivation. Workshop on Information Security and Privacy (WISP), 14-21.

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

Woon, I., Tan, G.-W., and Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. ICIS 2005 Proceedings, 31.

Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799-2816.

Zhang, J., Reithel, B. J., and Li, H. (2009). Impact of perceived technical protection on security behaviors. Information Management & Computer Security, 17(4), 330 - 340.