Exploring Factors That Influence Students' Behaviors in Information Security

Cheolho Yoon
Department of Business Administration,
Mokpo National University,
Muan-gun, 534-729, Korea
carlyoon@empal.com

Jae-Won Hwang
Department of General Education,
Kunsan National University
Kunsan, 573-701, Country
hjw504@ Kunsan.ac.kr

Rosemary Kim
School of Business Administration,
University of California, Riverside
Riverside, 92521, USA
rhkim@ucr.edu

ABSTRACT

Due to the ever-increasing use of the Internet, information security has become a critical issue in society. This is especially the case for young adults who have different attitudes towards information security practices. In this research, we examine factors that motivate college students' information security behaviors. Based on the concept of fear arousal in the presence of a threatened event, a well-founded theory known as Protection Motivation Theory (PMT) is adopted in the research model. Social norms and habit factors are integrated to the model as a means to assess students' behaviors of information security. A survey of 202 responses is used to test the designed model using structural equation modeling to analyze relationships among variables. Results indicated that students are very motivated to practice information security if they perceive high levels of severity, response efficacy, response costs and self-efficacy. Their intentions, however, are not affected by perceived vulnerability or by social influence. Our findings suggest that PMT is a valuable model for predicting students' attitudes towards information security and that their motivation is influenced by education in security awareness and understanding severity of such issues.

Keywords: Information Assurance and Security, Computer Security, Curriculum Design and Development, Privacy, Security

1. INTRODUCTION

Use of computers and the Internet is an integral part of college students' daily lives as they regularly use their computers and the Internet to access email, complete coursework, retrieve grades, register for courses, purchase books and supplies, pay tuition, and complete various other transactions that lead to leaving sensitive information on their computers and the Internet. With such dependency on the computer and the Internet, students are highly exposed to serious information security threats such as hacking, malware, and viruses. As information security threats continue to be a critical concern, importance of education in information security continues to be emphasized in information systems education.

According to Ng, Kankanhalli, and Xu (2009), information security education including security education, security training, and security awareness programs will influence users to become more security conscious. Thus, it is important to investigate the factors that influence users' security attitudes to design effective educational programs. This study aims to identify factors that motivate college students' behaviors towards information security.

As a framework for this study, we introduce a research

model based on Protection Motivation Theory (PMT) by Rogers (1983), subject norms, and habit factors. PMT is frequently used to analyze proactive behaviors and has been empirically tested by Woon, Tan and Low (2005) and Workman, Bommer, and Straub (2008). This study adds value to our field of research by designing a conceptual framework for understanding students' information security behaviors as a certain group. On a practical level, this study provides educators with suggestions for designing education in information security.

2. THEORETICAL BACKGROUND

2.1 Protection Motivation Theory

PMT was first introduced by Rogers (1975), to explain the effects of how fear appeals to individuals on health-related decisions such as dieting, quitting smoking and drinking, using condoms, and other concerns imposing health risks. PMT has since been widely extended to other fields of research and it is a powerful explanatory theory to predict individuals' intentions to take protective actions in other situations when threat is perceived. According to Rogers (1983), PMT consists of the cognitive appraisal process based on an individual's experience when faced with a threat. The cognitive process is divided into threat appraisal process and coping appraisal process.

The threat appraisal process evaluates a maladaptive behavior (e.g., smoking). Factors of the threat appraisal are maladaptive response rewards, intrinsic and extrinsic, and the perception of threat, severity and vulnerability. Reward factors increase the probability of selecting the maladaptive behavior, whereas threat factors decrease the probability of selecting the maladaptive behavior (Floyd, Prentice-Dunn and Rogers 2000).

The coping appraisal process evaluates the ability to cope with the threatened danger. Factors of the coping appraisal are response efficacy, self-efficacy, and response costs. Response efficacy is a person's belief that an adaptive response (a recommended action) will be effective in protecting him or her from the threat. Self-efficacy refers to a person's perceived ability to actually carry out the adaptive response. Response costs are any costs for taking the adaptive response (e.g., monetary, time, and effort). Response efficacy and self-efficacy increase the probability of selecting the adaptive behavior, whereas response costs decrease the probability of selecting the adaptive behavior (Floyd, Prentice-Dunn and Rogers 2000).

Although PMT was originally developed to explain the effects of fear appeals on health attitudes and behaviors such as the use of condoms to prevent HIV infections, the theory has found broad empirical support (Johnston and Warkentin 2010). According to Pechmann, Zhao, Goldberg, et al. (2003), people can be motivated to engage in desirable health behaviors not only to avoid health risks but also to avoid social or interpersonal risks. Thus, PMT has recently been used as the basis theory in many studies related to information security in organizations, and the theory is verified in these studies (Workman, Bommer and Straub 2008; Liang and Xue 2010; Lee and Larsen 2009).

2.2 Subjective Norm

Subjective norm is a core construct in the theory of reasoned action (Fishbein and Ajzen 1975). It is a function of a person's belief that specific referent individuals or groups approve of the behavior, and therefore the person is motivated to comply with those referents. Namely, if a person perceives pressure from family, friends, or spouse, he or she is likely to act in accordance with the expected behavior.

As a form of social influence, many studies have verified that subjective norm plays an important role in predicting health-related behaviors such as condom use, dental hygiene, alcohol use, AIDS-related behaviors, safe driving, smoking, and mammography along with the attitude toward these behaviors (see Kim 2010).

Subjective norm is influenced by social networks and organizations such as peer groups, school, workplace, and family (An and Zhou 2008). The subjective norm construct, which is usually used to assess social influence, proves to be a welcome addition in predicting these behaviors (Finlay, Trafimow and Jones 1997). Also, the subjective norm is an important determinant of an individual's behavior in various areas such as information technologies acceptance (Schepers and Wetzels 2007) and information security (Anderson and Agarwal 2010).

2.3 Security Habits

Habits are commonly understood as "*learned sequences of acts that become automatic responses to specific situations which may be functional in obtaining certain goals or end states*" (Verplanken, Aarts and Van Knippenberg 1997; Limayem, Hirt and Cheung 2003). They are performed automatically in the sense that their performance requires little conscious attention and only minimal mental effort (Limayem, Hirt and Cheung 2003).

Security behavior can be regarded as continuous actions. Example of such actions is locking the door every night before going to sleep. In examining continuous actions, habit serves as the antecedent as commonly demonstrated in food consumption and consumer behavior. Scholars have argued that habit is an influencing factor on a given action along with a conscious intention to do the action. Particularly in connection with PMT, Maddux (1993) argued that situational cues and habits have important effects on the decision-making process of taking protective actions. An example is exercising to be healthy.

Aarts, Verplanken and Knippenberg (1998) also argued that although PMT or the theory reasoned action have given more light on the reason-based and deliberate nature of behavior, one important aspect has been overlooked in these theories; namely, the fact that many of the behaviors related to health (e.g., smoking, exercising) and safety (e.g., following safety instructions at work, using seat belts) are executed on a daily, repetitive basis, and therefore may become routine or habitual. Thus, we include security habit as a factor in our model.

3. RESEARCH MODEL AND HYPOTHESES

Five constructs for the design of this study are: perceived vulnerability, perceived severity, response efficacy, response costs, and self efficacy, which are variables derived from PMT and subjective norm construct to measure the affect of a student's intention to practice information security. In turn,

the intention and security habits affect information security behaviors. Figure 1 represents the research model.

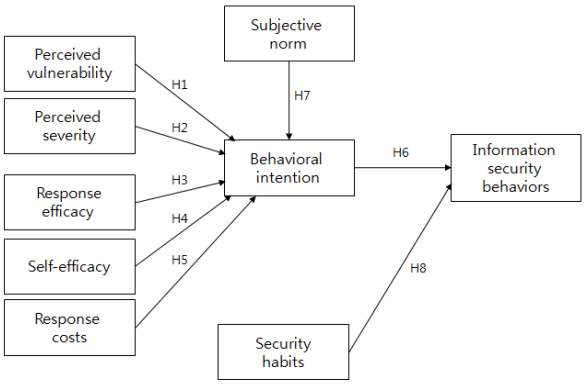

Figure 1. Research Model

3.1 Protection Motivation Theory

According to PMT, the higher the perception of a threat, the more one is willing to cope and adapt his behavior. Threat factors measured are perceived vulnerability and perceived severity. Perceived vulnerability is a person's assessment of his or her own probability of being exposed to a threat. Perceived severity refers to one's fear towards the significance of the threat. A number of studies (Rippetoe and Rogers 1987; Brewer, Chapman, Gibbons, et al. 2007; Albarracín, Gillette, Earl, et al. 2005) have proven that threat factors increase an individual's intention to practice a coping response. In this study, the students' perceived threat is personal information may be stolen by hackers leading to serious consequences. This study proposes:

Hypothesis 1. Students' perceived vulnerability of losses by security threats has a positive effect on their behavioral intention to practice information security.

Hypothesis 2. Students' perceived severity of losses by security threats has a positive effect on their behavioral intention to practice information security.

In PMT, the coping appraisal factors include response efficacy, response costs, and self-efficacy. According to PMT, response efficacy and self-efficacy increase the probability of selecting the adaptive response, whereas response costs decrease the probability of selecting the adaptive response. Response efficacy is a person's belief that a recommended response will effectively avert a threat (Rogers 1975). Self-efficacy (Bandura 1986) is the expectancy of a person's capability in performing a recommended coping behavior. PMT-related studies show that efficacy effects have a significant positive correlation on intention to practice proactive behaviors (Woon, Tan and Low 2005). Namely, if students think that using security technologies is effective for protecting confidential information and they have confidence in protecting their personal information from external threats, they may have a higher chance of taking measures to protect their information and data. Thus, we hypothesize the following:

Hypothesis 3. Response efficacy has a positive effect on students' behavioral intention to practice information security.

Hypothesis 4. Self-efficacy has a positive effect on students' behavioral intention to practice information security.

Response costs, the costs perceived by an individual in performing a recommended coping behavior, include inconvenience, difficulty, and the side effects of performing the coping behavior including money and time. According to PMT, the response cost decreases an individual's intention to practice a coping response. Therefore, we also hypothesize the following:

Hypothesis 5. Response costs have a negative effect on students' behavioral intention to practice information security.

Consistent with general behavior theories such as the theory reasoned action (TRA) and the theory of planned behavior (TPB) (Ajzen 1991), we postulate that students' motivation to practice information security has a positive impact on their information security behaviors.

Hypothesis 6. Students' behavioral intention to practice information security has a positive effect on their information security behaviors.

3.2 Subject Norm

In the context of this study, subjective norm is defined as a student's belief about the extent of approval from friends, peers or family for his or her behavior in information security. As argued by the TRA and the TPB, a person is more likely to be influenced by social influence. Therefore, we hypothesize that:

Hypothesis 7. Subjective norms have a positive effect on behavioral intention to practice information security.

3.3 Security Habit

Behaviors related to health and safety such as exercising or using the seat belt requires continuous action on a routine basis to become a habit (Aarts, Verplanken and Knippenberg 1998). Similarly, information security behavior, as a safety measure, is triggered by awareness of an external threat or peer pressure on information security. The security behaviors will become routine or habitual through repetitive actions. Therefore, security habits, along with a conscious intention to practice the behaviors, may influence students' information security behaviors. Thus, we hypothesize that:

Hypothesis 8. Security habits have a positive effect on students' information security behaviors.

4. RESEARCH METHODOLOGY

4.1 Data Collection

In this study, we surveyed students from a university in South Korea. We carried out the survey in four different classes, Enterprise Resource Planning, Management Innovation, Culture and Art Management, and Global Trade

Environment. The students' majors are in business administration or international trade, and most of them have no prior education in information security. The university has no special security policy or procedure. We explained the purpose of this survey and asked the students to take part in our study.

Table 1
Descriptive statistics of respondents' characteristics

Measure	Value	Frequency (%)
Gender	Male	100(49.5)
	Female	102(50.5)
Age	Younger than 20	9(4.5)
	20 – 24	159(78.7)
	25 – 30	32(15.8)
	Older than 40	2(1.0)
Degree of computer usage (hour per day)	Less than 1	27(13.4)
	< 3	101(50.0)
	< 5	49(24.3)
	More than 5	25(12.3)

A total of 209 students voluntarily participated in this study and completed a questionnaire in class. Among the returned questionnaires, seven were incomplete and discarded, leaving 202 questionnaires for analysis. Of the respondents, 100 are male and 102 are female, approximately 79% of the respondents are in the age group 20-24, and more than 87% of the respondents use computers for more than an hour a day. Detailed descriptive statistics relating to the respondents' characteristics are shown in Table 1.

4.2 Measurements

The questionnaire for data collection contains scales to measure the various constructs of the research model. The measurements for PMT constructs are adapted from several studies, including Ng, Kankanhalli and Xu (2009), Workman, Bommer and Straub (2008), and Woon, Tan and Low (2005). The measurements for the subjective norm construct and the security habit construct are adapted from studies conducted by Yoon (2011) and Limayem, Khalifa and Chin (2004), respectively. The measurements for the behavioral intention construct are adapted from Workman, Bommer and Straub's (2008) study and the items for information security behaviors are newly developed in this study. In the questionnaire, all items are measured using a seven-point Likert scale, with responses ranging from "*strongly disagree*" to "*strongly agree*." All items in the questionnaire are shown in Appendix.

5. RESULTS

Data analysis proceeded in two stages. First, a confirmatory factor analysis is performed to validate the research measurements. Second, a structural equation model is used to validate the research model. To explore the fundamental relationships between variables, Partial Least Squares (PLS) regression is used. Previous studies support the adoption of PLS as acceptable method of exploratory study (Chin 1998).

Table 2
Results of confirmatory factor analysis

Construct		Construct loading scores									t-value
		1)	2)	3)	4)	5)	6)	7)	8)	9)	
Information security behaviors	ISB1	**0.78**	0.37	0.06	0.13	0.22	-0.08	0.20	0.31	0.43	22.73
	ISB2	**0.77**	0.27	0.19	0.13	0.43	-0.04	-0.02	0.29	0.45	15.16
	ISB3	**0.63**	0.36	0.01	0.24	0.26	-0.17	0.03	0.20	0.27	7.56
Behavioral intention	BI1	0.40	**0.87**	0.09	0.22	0.34	-0.09	0.22	0.37	0.25	35.28
	BI2	0.32	**0.86**	0.15	0.22	0.38	-0.16	0.24	0.33	0.23	41.71
	BI3	0.39	**0.70**	0.20	0.25	0.24	-0.12	0.10	0.14	0.20	12.84
Perceived vulnerability	PV1	-0.01	0.05	**0.69**	0.30	0.03	0.07	-0.07	0.12	0.08	2.68
	PV2	0.14	0.20	**0.98**	0.34	0.17	0.12	-0.11	0.14	0.15	8.13
Perceived severity	PS1	0.00	0.12	0.31	**0.75**	0.02	0.09	0.10	0.09	0.00	6.15
	PS2	0.28	0.31	0.33	**0.97**	0.25	-0.05	0.14	0.31	0.25	53.60
Response efficacy	RE1	0.35	0.38	0.13	0.19	**0.89**	0.03	0.14	0.45	0.39	34.70
	RE2	0.39	0.33	0.12	0.17	**0.92**	0.14	0.12	0.47	0.48	56.82
	RE3	0.39	0.38	0.16	0.19	**0.92**	0.06	0.16	0.48	0.46	59.31
Response costs	RC1	-0.09	-0.13	0.07	0.00	0.08	**0.89**	0.02	0.00	0.00	5.09
	RC2	-0.13	-0.14	0.15	-0.02	0.07	**0.92**	-0.01	-0.05	-0.02	6.64
Self-efficacy	SE1	0.16	0.26	-0.06	0.19	0.20	-0.06	**0.90**	0.26	0.20	25.28
	SE2	0.05	0.17	-0.14	0.11	0.06	0.02	**0.88**	0.30	0.10	22.37
	SE3	0.00	0.13	-0.11	0.02	0.11	0.11	**0.75**	0.21	-0.02	8.97
Subjective norm	SN1	0.32	0.29	0.16	0.29	0.48	-0.02	0.29	**0.87**	0.53	30.46
	SN2	0.36	0.36	0.13	0.24	0.47	-0.04	0.25	**0.94**	0.51	101.60
	SN3	0.28	0.28	0.10	0.21	0.43	-0.02	0.27	**0.84**	0.55	24.21
Security habits	SB1	0.35	0.25	0.10	0.14	0.39	0.04	0.26	0.57	**0.76**	13.96
	SB2	0.53	0.23	0.14	0.19	0.43	-0.05	0.02	0.46	**0.90**	43.76

5.1 Reliability and Validity of Measurement Items

Partial least squares can test the convergent and the discriminant validity of the scales. In a confirmatory factor analysis, convergent validity is evident when each of the measurement items loads significantly, with the p-value of its t-value well within the 0.05 level, on its assigned construct (Gefen and Straub 2005). Table 2 shows the factor loadings of the measurement items and t-values.

All t-values in the Table 2 are above 1.96. The factor loadings of all items also loaded highly (above 0.80). This demonstrates convergent validity of all the measurement items for the constructs.

Discriminant validity is demonstrated when the following two things occur: (1) measurement items load more strongly on their assigned construct than on the other constructs in a confirmatory factor analysis, and (2) when the square root of the average variance extracted (AVE) of each construct is larger than its correlations with the other constructs (Gefen and Straub 2005).

As shown in Table 2, all the measurement items loaded were considerably stronger on their respective factor than on other constructs. Table 3 shows the square root of the AVE and the inter-construct correlations. Comparisons of the correlation with the square root of the AVE show that all correlations between the two constructs are less than the square root of the AVE of both constructs.

Table 3
Average Variance Extracted and Correlation Matrix

Construct	Factor									CCR*	AVE**
	1)	2)	3)	4)	5)	6)	7)	8)	9)		
Information security behaviors	(0.73)									0.77	0.53
Behavioral intention	0.46	(0.81)								0.85	0.66
Perceived vulnerability	0.12	0.18	(0.85)							0.83	0.72
Perceived severity	0.22	0.28	0.36	(0.87)						0.86	0.75
Response efficacy	0.41	0.40	0.15	0.20	(0.91)					0.94	0.83
Response costs	-0.13	-0.15	0.12	-0.02	0.08	(0.90)				0.90	0.82
Self-efficacy	0.10	0.24	-0.11	0.14	0.16	0.01	(0.85)			0.88	0.72
Subjective norm	0.37	0.35	0.15	0.28	0.51	-0.03	0.30	(0.88)		0.92	0.78
Security habits	0.54	0.28	0.15	0.20	0.49	-0.01	0.14	0.60	(0.84)	0.82	0.70

*CCR : Composite Construct Reliability
**AVE: Average Variance Extracted
( ) : Square root of AVE

To assess the reliability of a measurement item, the study computed a composite construct reliability coefficient, as shown in Table 3. Composite reliabilities ranged from 0.77 (for information security behaviors) to 0.94 (for response efficacy), which exceeded the recommended level of 0.60 (Bagozzi and Yi 1988). The AVE ranged from 0.53 (for information security behaviors) to 0.83 (for response efficacy), which also exceeded the recommended level of 0.50 (Fornell and Larcker 1981). The results, therefore, demonstrated a reasonable reliability level for the measured items.

5.2 Hypothesis Testing Results

Having assessed the structural model, we then examined the coefficients of the causal relationships between constructs, which would validate the hypothesized effects. Figure 2 illustrates the paths and their significance on the structural model. The coefficients, their t-value on the structural model, and the coefficients of determination (R^2) for each dependent construct are shown in Table 4.

Based on the structure model, we performed hypotheses testing. As indicated in Table 4, the results show that perceived severity, response efficacy, response costs, and self-efficacy have a significant impact on behavioral intention to practice information security with α=0.05; in turn, behavioral intention and security habits have a significant impact on information security behaviors with α=0.01. Perceived vulnerability and subjective norms, however, do not have any significant impact on behavioral intention to practice information security. Therefore, hypotheses H1 and H7 are rejected.

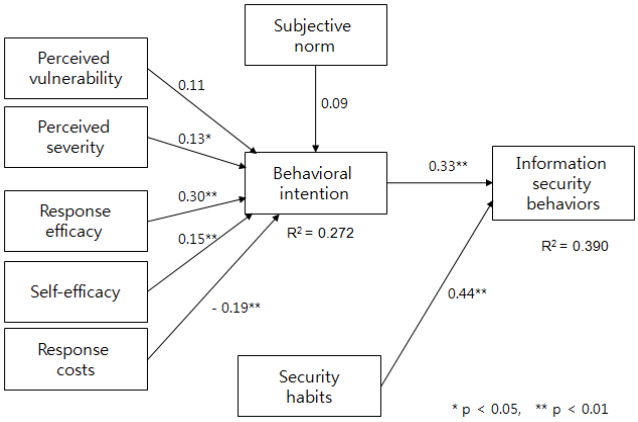

Figure 2. Path Diagram for Research Model

In addition, about 27% of the variance of behavioral intention (R^2= 0.272) is explained by perceived vulnerability, perceived severity, response efficacy, response costs, self-efficacy, and subjective norm, and 39% of the variance of information security behaviors (R^2=0.390) by behavioral intention to practice information security and security habits. Table 4 shows the results of the hypotheses testing in more detail.

Table 4
Hypothesis testing results

Hypothesis	Path	Path coefficient	t-value
H1	Perceived vulnerability -> Behavioral intention	0.11	1.60
H2	Perceived severity -> Behavioral intention	0.13	2.05*
H3	Response efficacy -> Behavioral intention	0.30	4.24**
H4	Self-efficacy -> Behavioral intention	0.15	2.37**
H5	Response costs -> Behavioral intention	-0.19	3.37**
H6	Behavioral intention -> Information security behaviors	0.33	4.74**
H7	Subjective norm -> Behavioral intention	0.09	1.13
H8	Security habits -> Information security behaviors	0.44	6.44**

Behavioral intention R^2: 0.272
Information security behaviors R^2: 0.390
* Significant at the 0.05 level
** Significant at the 0.01 level

6. DISCUSSION AND CONCLUSIONS

In this research, we examined factors that motivate students' information security behaviors. A research model based on PMT including subject norms and habit factors was developed. Several insightful results are summarized from the research model and are presented below.

First, the results of this study show that PMT is a valuable model for predicting students' information security behaviors. In particular, response efficacy and self-efficacy have a strong impact on students' intentions to practice information security. These results imply that students will make more of an effort to apply information security and thus experience high levels of confidence in doing so when their efforts are perceived as being effective and practicable. Conversely, response cost has a negative impact and perceived vulnerability has no significant impact on motivation to practice information security.

These results differ from the findings of earlier studies that explored information security behaviors of working adults and professionals (Workman, Bommer and Straub 2008; Chenoweth, Minch and Gattiker 2009; Ng, Kankanhalli and Xu 2009). The difference in results may imply that there is a distinct difference between students and working professionals in perceiving the probability of potential risks. Namely, since students have little experience and perhaps a more liberal mind, they would not think deeply about the possibility of their own information being exposed and posing a threat.

Second, results show that the subjective norm has no significant impact on students' intentions to practice information security. These results imply that normative judgment on information security behaviors is not established for younger adults. While subjective norm as a core variable has been empirically proven to influence individuals' behaviors in various contexts, including health-related situations, this study did not find the same relationship. Behaviors such as smoking or not wearing a seatbelt are treated as undesirable behaviors in social and normative standards, but information security behavior is a comparatively new concept and its normative judgment may not be clearly established yet for students. Therefore, the subjective norm affected by normative belief and judgment has less of an effect on students' intention to practice information security behaviors. Another possible explanation of the result is that information security behavior is a voluntary activity rather than a required task. A study suggests that subjective norm is less influential in voluntary settings (Venkatesh and Davis, 2000).

Third, security habits show a significant impact on students' intentions to practice information security, this is demonstrated by a path coefficient of 0.44. Although security behaviors may first begin due to awareness of external threat or the surrounding pressure on information security, motivation towards information protection becomes routine and habitual over time based on the experiences of that repeated behavior.

6.1 Contributions and Implications

This study presents important implications for research and practice. To explore factors influencing students' information security behaviors, this study proposed a research model based on PMT, including subject norm and habit factors, and empirically supported the model with 202 university students. The significant contribution of this study is the theoretical framework for understanding students' information security behaviors. There are also important implications for researchers and educators.

First, this study reveals that the ability to respond to a threat is strongly tied to students being able to practice and perform techinques rather than conceptually understanding the perceived threat, vulnerability, and serverity. Therefore, in designing information security programs for college courses, it is desirable to put more weight on information security training than on security awareness. Specifically, practicing hands-on learning to manage anti-viruses and security settings should be heavily emphasized.

Second, the results of the study show that subjective norms have no significant impact on students' intention to practice information security. Therefore, rather than describing standards to communicate acceptable norms, students should be exposed to severity of losses due to security negligence and understand how proper measures can prompt favorable results.

Finally, the results show that security habits play an important role. Therefore, continuous education and reinforcement is necessary for students to build proper security habits. Strategies for teaching a course should include demonstrating security routines that have lead to successful otucomes and emphasizing immediate benefits

when practice is put in to place. It is also helpful to provide security techniques and resources that enable students to perform security procedures easily and quickly (Aarts, Paulussen and Schaalmas, 1997).

6.2 Limitations and Future Research Issues

Although this study's findings provide meaningful implications, the study has some limitations. First, just 27% of the variance of behavioral intention (R^2=0.272) is explained by the variables of PMT and subjective norm, and 39% of the variance of information security behaviors (R^2 = 0.390) by behavioral intention to practice information security and security habits. To improve the model's explanatory power, additional variables can be included to extend our framework.

Second, the survey was conducted to students with similar majors: business administration and international trade. The students can be perceived as same social group and similar background, leaving little room for dissimilar attitudes about information security. To further validate the results of the study, the survey should be conducted in more diverse student populations using greater number of students.

Third, future research can extend the survey questions pertaining to computer security behavior by asking about their conduct in: choosing a secure password, updating virus programs, and sharing information on Facebook. Finally, the number of constructs can be broadened beyond the factors of perceived vulnerability, perceived severity, response costs, subject norm, and security habits.

8. REFERENCES

Aarts, H., Paulussen, T., and Schaalma, H. (1997). Physical exercise habit: On the conceptualization and formation of habitual health behaviors, *Health Education Research*, 12(3), 363-374.

Aarts, H., Verplanken, B., and Knippenberg, A.V. (1998). Predicting behavior from actions in the past: Repeated decision making or a matter of habit, *Journal of Applied Psychology*, 28(15), 1355-1374.

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

Albarracín, D., Gillette, J.C., Earl, A.N., Glasman, L.R., Durantini, M.R., and Ho, M.H. (2005). A test of major assumptions about behavior change: a comprehensive look at the effects of passive and active HIV-prevention interventions since the beginning of the epidemic, *Psychological Bulletin*, 131(6), 856-897.

An, S. and Zhou, S., (2008). "A Conceptual comparison of the theoretical approaches in health campaigns: Focusing on SET, TRA, TPB, HBM, and EPPM," Paper presented at the annual meeting of the International Communication Association, TBA, Montreal, Quebec, Canada.

Anderson, C.L. and Agarwal, R. (2010). Practicing safe computing: A multi-method empirical examination of home computer user security intentions, *MIS Quarterly*, 34(3), 613–643.

Bagozzi, R.P., and Yi, Y., (1988). On the evaluation of structural equation models, *Journal of the Academy of Marketing Science*, 16 (1), 74–94.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*, Englewood Cliffs, Prentice-Hall, NJ.

Brewer, N. T., Chapman, G. B., Gibbons, F. X., Gerrard, M., McCaul, K. D. and Weinstein, N. D. (2007). Meta-analysis of the relationship between risk perception and health behavior: the example of vaccination, *Health Psychology*, 26(2), 136-145.

Chenoweth, T., R. Minch, and T. Gattiker (2009). Application of protection motivation theory to adoption of protective technologies," Proceedings of the 42nd Hawaii International Conference on System Sciences, 1-10.

Chin, W. W. (1998). Issues and opinion on structural equation modeling, *MIS Quarterly*, 22(1), vii–xvi.

Finlay, K. A., Trafimow, D., and Jones, D. (1997). Predicting health behaviors: Between-subjects and within-subjects analyses, *Journal of Applied Social Psychology*, 27(22), 2015-2031.

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

Floyd, D. L, Prentice-Dunn, S., and Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory, *Journal of Applied Social Psychology*, 30(2), pp. 407–429.

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

Gefen, D., and Straub, D. (2005). A practical guide to factorial validity using PLS graph: Tutorial and annotated example, *Communications of the AIS*, 16(5), 91–109.

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

Kim, H. J. (2010). Increasing the persuasiveness of gain vs. loss framing: the effects of gender and fear arousal on processing gain- vs. loss-framed breast cancer screening messages. Unpublished doctoral dissertation, University of Missouri-Columbia.

Lee, Y., and Larsen, K. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software, *European Journal of Information Systems*, 18(2), 177-187.

Liang, H., and Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective, *Journal of the Association for Information Systems*, 11(7), 394-413.

Limayem, M., Hirt, S. G., and Cheung, C. M. K. (2003). Habit in the context of IS continuance: Theory extension and scale development, in Proceedings of the 7th European Conference on Information Systems (ECIS 2003), Naples, Italy, June 19-21.

Limayem, M., Khalifa, M., and Chin, W. W. (2004). Factors motivating software piracy: A longitudinal study, *IEEE Transactions on Engineering Management*, 51(1), 414–425.

Maddux. (1993). Social cognitive models of health and exercise behavior: An introduction and review of conceptual issues, *Journal of Applied Sport Psychology*, 5(2), 116-140.

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

Pechmann, C., Zhao, G., Goldberg, M. E., and Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes, *Journal of Marketing*, 67(2), 1-18.

Rippetoe, S., and Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat, *Journal of Personality and Social Psychology*, 52(3), 596-604.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change, *The Journal of Psychology*, 91(5), 93- 1 14.

Rogers, R. W. (1983). Cognitive and physiological processes in fear-based attitude change: A revised theory of protection motivation. In J. Cacioppo and R. Petty (Eds.), Social psychophysiology. A sourcebook (pp. 153-176). New York. NY: Guilford.

Schepers, J., and Wetzels, M. (2007). A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects, *Information & Management*, 44(1), 90–103.

Venkatesh, V. and Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies, *Management Science*, 46(2), 186–204.

Verplanken, B., Aarts, H., and Van Knippenberg, A. (1997). Habit, information acquisition, and the process of making travel mode choices, *European Journal of Social Psychology*, 27(5), 539-560.

Woon, I., Tan, G. W., and Low, R., (2005). A Protection Motivation Theory Approach to Home Wireless Security, in Proceedings of the 26th International Conference on Information Systems (ICIS). 367-380.

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

Yoon, C. (2011) Theory of planned behavior and ethics theory in digital piracy: an integrated model, *Journal of Business Ethics*, 100(3), 405–417.

AUTHOR BIOGRAPHIES

Cheolho Yoon currently serves as an associate professor of management information systems (MIS) at Mokpo National University in Korea. He studied Computer Science at Kwangwoon University in Seoul, Korea, where he also earned his Ph.D in MIS. His research areas are ubiquitous computing, e-commerce, IT ethics and knowledge management. He has published articles in a number of journals such as Information & Management, Journal of Computer Information Systems, Journal of Business Ethics, Electronic Commerce Research and Applications, Computers in Human Behavior, Behaviour & Information Technology, and Journal of Organizational Computing and Electronic Commerce, etc.

Jae-won Hwang is an assistant professor of department of general education at Kunsan National University in Korea. He received his B.S. and M.S. degrees in Electronic Engineering from Korea University, and M.S. and Ph.D. degrees in Educational Counseling from Seoul National University, Korea. His research interests include Internet addiction, self-regulation, and happiness and positive psychology.

Rosemary Kim is an assistant clinical professor in Accounting and Information Systems at The Anderson Graduate School of Management, University of California Riverside. She received her Ph.D. in Information Systems & Technology from Claremont Graduate University and her MBA from University of Southern California. Her research interests include accounting information systems, auditing, and information technology.

APPENDIX

Construct		Items	Source
Information security behaviors	ISB1	I periodically check and erase viruses and malicious software	Self Developed
	ISB2	I immediately delete suspicious e-mails without reading them	Self Developed
	ISB3	Under no circumstances would I ever tell anyone my ID or password	Self Developed
Behavioral intention	BI1	I will take precautions against information security violations	Workman, et al. (2008)
	BI2	I will actively use security technologies to protect confidential information	Workman, et al. (2008)
	BI3	I will never install unreliable software or ActiveX on my computer	Self Developed
Perceived vulnerability	PV1	There's a chance that my personal information has been disclosed due to hacking	Workman, et al. (2008)
	PV2	The data on my computer is likely to be undermined by malicious software such as viruses	Workman, et al. (2008)
Perceived severity	PS1	Losing data privacy as a result of hacking would be a serious problem for me	Woon, et al. (2005)
	PS2	Having the data in my computer destroyed by malicious software such as viruses would be a serious problem for me	Woon, et al. (2005)
Response efficacy	RE1	Using security technologies is effective for protecting confidential information	Workman, et al. (2008)
	RE2	Taking preventive measures is effective for protecting my personal information	Workman, et al. (2008)
	RE3	Enabling security measures on my computer is an effective way of preventing computer data from being damaged by malicious software such as viruses	Workman, et al. (2008)
Response costs	RC1	Acquiring new security technology to protect confidential information is annoying	Self Developed
	RC2	Maintaining security procedures (such as changing the password regularly) to protect personal information is cumbersome	Self Developed
Self-efficacy	SE1	I am able to protect my personal information from external threats	Ng, et al. (2009)
	SE2	I am able to protect the data on my computer from being damaged by external threats	Ng, et al. (2009)
	SE3	I am capable of responding to malicious software such as viruses	Ng, et al. (2009)
Subjective norm	SN1	If I actively use security technologies, most of the people who are important to me would approve	Yoon (2011)
	SN2	Most people who are important to me think it is a good idea to take preventive measures to protect personal information	Yoon (2011)
	SN3	My friends think computer security behavior is important	Yoon (2011)
Security habits	SB1	I should periodically remove viruses and malicious software	Limayem, et al. (2004)
	SB2	I automatically send suspicious e-mails to the recycle bin	Limayem, et al. (2004)

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096