Asia Pacific Journal of Information Systems
Vol. 21, No. 3, September 2011

Understanding Security Knowledge and National Culture: A Comparative Investigation between Korea and the U.S*

Dong-Heon Kwak**, Donna McAlister Kizzier***, Hangjung Zo****, Euisung Jung**

Security has been considered one of the most critical issues for managing IT resources in many organizations. Despite a growing interest and extensive research on security at various levels, little research has focused on the comparison of security knowledge levels between different cultures. The current study investigates and compares the security knowledge level between Korea and the U.S. Based on the literature review of spyware, Hofstede's cultural dimensions, and security knowledge, this study identifies three constructs (i.e., security familiarity, spyware awareness, and spyware knowledge) to examine the difference of security knowledge levels between Korea and the U.S. Six hundred ninety-six respondents from Korea and the U.S. participated in the survey, and an in-depth analysis based on analysis of covariance (ANCOVA) was carried out. The results show that the levels of security familiarity, spyware awareness, and spyware knowledge are significantly lower in Korea than in the U.S., as expected. These findings present a significant association between national culture and security knowledge, and the degree of individualism (or collectivism) plays an especially critical role in the perception of security. A number of implications for academia and practitioners emerge. Limitations and future research directions are discussed in the conclusion.

Keywords : IS Management, Security, Spyware, Familiarity, Awareness, Knowledge, Culture, Collectivism, Individualism, Analysis of Covariance (ANCOVA)

---

* We would like to thank an associate editor and two anonymous reviewers for their constructive reviews. The comments provided by them greatly enhanced the content and presentation of the paper. We also thank Tim Mooney for his editorial support. This paper was based on the first author's master's thesis.

** Ph. D. Student, Lubar School of Business, University of Wisconsin-Milwaukee

*** Associate Professor, College of Business and Public Affairs, Morehead State University

**** Corresponding Author, Assistant Professor, Department of Management Science, Korea Advanced Institute of Science and Technology (KAIST)

Ⅰ. Introduction

Information technology (IT) plays a critical role for individuals, organizations, and global businesses. IT designed to facilitate individual and organizational productivity is called positive technology (e.g., ERP systems, office software, programming languages, etc.) [Dinev and Hu, 2007]. Contrary to positive technologies, negative technologies [Dinev and Hu, 2007] are developed and used for malicious purposes and can pose serious threats to stakeholders. Viruses, spyware, Trojan horses, and rootkits are just a few examples of negative technologies. Negative technologies impact both individuals and firms. For example, Consumer Reports [2010] estimates that cybercrimes cost users in the U.S. $4.5 billion over the past two years and caused them to replace 2.1 million computers. Computer Security Institute [2009] insists that the average annual financial loss caused by security breaches reported by the U.S. firms was $234,244 in 2009, which is much higher than the $168,000 loss reported in 2006.

The significance of security issues has led researchers to conduct security research at organizational, individual, and cross-cultural levels. The majority of security research has focused on information security at the organizational level [Dhillon and Backhouse, 2001; Im and Baskerville, 2005; Straub, 1990; Straub and Welke, 1998; Sun *et al*., 2006]. Meanwhile, research on an individual level of security has been a growing research interest [Chen and Zahedi, 2009; Johnston and Warkentin, 2010; Liang and Xue, 2009; Myyry *et al*., 2009]. Although the cross-cultural level is not as broadly studied as the organizational and individual levels, researchers have continuously paid attention to security issues among different countries, focusing on cultural differences [Chen *et al*., 2008; Dinev *et al*., 2009; Schmidt *et al*., 2008].

In practice, several institutional initiatives exist to cope with security problems, including law enforcement and government legislation, as well as development and distribution of protective technologies (e.g., anti-spyware programs and anti-virus programs) by firms. From an individual perspective, various coping mechanisms for reducing security threats are being used [Liang and Xue, 2009], and adoption of protective technologies is one coping mechanism for individuals. According to Lee and Kozar [2005], the best way for users to reduce spyware problems is to adopt anti-spyware programs. In addition to adopting protective technologies, Sriramachandramurthy *et al*. [2009] suggest a user's knowledge about negative technologies is an important source of security threat reduction.

Previous researchers have studied protective technology adoption to cope with negative technologies [Dinev and Hu, 2007; Johnston and Warkentin, 2010; Lee and Kozar, 2008]. Dinev and Hu [2007] argue that awareness of negative technologies is a key predictor in protective technology adoption. Knowledge related constructs including familiarity, awareness, and information play important roles in security threat reduction behaviors as well as technology adoption and e-commerce adoption [Gefen *et al*., 2003]. Given the importance of knowledge, prior researchers have attempted to extend knowledge research to the cross-cultural level, comparing knowledge levels between different countries. For example, there are sig-

nificant differences in security knowledge between the U.S. and China [Schmidt *et al*., 2008].

Despite extensive knowledge research and a growing interest in security research at the cross-cultural level, little research exists which compares the security knowledge level between Korea and the U.S. This lack of research suggests a need to investigate the differences in security knowledge levels between Korea and the U.S., focusing on cultural differences.

Schmidt *et al*. [2008] suggest that culture affects how security policies are formulated and implemented, and also establishes how a society will recognize computer security risks. Based on Schmidt *et al*., the current study addresses how and why cultural differences lead to differences in security knowledge levels in two selected countries. This study compares Korea and the U.S. because both countries have highly developed IT infrastructures [Hwang *et al*., 2006; Internet World Stats, 2010] and similar Internet penetration rates (Korea: 81.8%, U.S.: 77.3%). These two selected countries have distinct cultures according to Hofstede's cultural indices [Dinev *et al*., 2009]. Comparing these two countries with highly developed IT infrastructure could provide insights into the cultural effect on the differences of security knowledge levels of both countries. In addition, the findings of this study would provide implications for dealing with security issues to practitioners in different cultures.

The remainder of this study is organized as follows. Section Ⅱ reviews existing spyware literature, addressing the security knowledge process and national culture. Section Ⅲ develops the hypotheses for this study. The research methods and results are discussed in Section Ⅳ. Finally, Section Ⅴ discusses the implications for research and practice and concludes the paper with limitations and future research directions.

Ⅱ. Literature Review

The literature review begins with a synopsis of spyware technologies, followed by a review of relevant literature related to security and knowledge. Relevant literature related to broader cultural differences between Korea and the U.S., as well as the specific effect of the cultural differences on security, are also reviewed in this section.

2.1 Spyware

A specific type of negative technology (i.e., spyware] was selected for this study, examining specialized security knowledgeas well as general security knowledge. Spyware generally refers to programs that act as data sensors and illicitly collect and transmit information about end users, and then send it back to a third party [Cohen, 2003; Kenyon, 2004]. Adware, keyloggers, Trojan horses, scumware, dialers, and browser hijackers are under the category of spyware [Lee and Kozar, 2005]. Although the original intent of spyware was to create software that helps computer users solve their computer problems, it has become a type of negative technology [Baker, 2006]. Spyware is designed not to disrupt or destroy computers, but to reside and function unnoticed by users [Dinev and Hu, 2007]. Based on two key considerations (i.e., user consent/user consequences), Warkentin *et al*. [2005] describe four distinct characterizations of spyware: overt provider (high/positive), cov-

ert supporter (low/positive), double agent (high/negative), and parasite (low/negative). Unlike viruses, computer users are not immediately aware of the existence of spyware, and thus it is an increasingly notorious and noxious type of negative technology [Arnett and Schmidt, 2005; Stafford and Urbaczewski, 2004].

Spyware causes businesses to lose productivity and efficiency. Claburn [2009] mentions that "70 percent of the top 1000 websites either hosted malicious content or contained a link designed to redirect site visitors to a malicious web site during the second half of 2008," and "77 percent of websites with known malicious code are legitimate sites." Microsoft claims that half of all computer crashes reported by its customers were caused by spyware and its equivalents [Spring, 2004]. Dell notes that spyware is responsible for about twelve percent of all technical support calls and accounts for the biggest category of customer complaints [Asaravala, 2004]. Since spyware is an increasingly serious security issue, previous research on protective technology adoption has incorporated anti-spyware programs [Dinev and Hu, 2005, 2007; Dinev *et al*., 2009; Johnson and Warkentin, 2010; Lee and Kozar, 2005, 2008].

Having reviewed relevant studies that address spyware in this section of the literature review, the next section of the literature review addresses the broader topics of security and knowledge.

2.2 Security and Knowledge

The importance of knowledge has led to numerous studies in the social sciences that focus on knowledge research. In the knowledge-based view of the firm, knowledge is an important resource for sustainable competitive advantage in organizations, and one important activity within an organization is to transfer knowledge efficiently [Kogut and Zander, 1992]. In the theory of reasoned action, Fishbein and Ajzen [1975] regard knowledge as a belief, suggesting that knowledge affects individual behaviors in the long run. In protective technology acceptance, according to Dinev and Hu [2007], awareness of spyware is the key factor of intention to adopt anti-spyware programs. Zhang [2005] empirically tests four measures to assess the respondents' knowledge of spyware: tracking keystrokes, recording online transactions, monitoring online surfing habits and residing on computers. Zhang finds that the sample in the U.S. was familiar only with spyware monitoring surfing habits.

Other researchers have categorized knowledge types. In innovation diffusion theory (IDT), Rogers [2003] proposes three types of knowledge: awareness knowledge, how to knowledge, and principle knowledge. Alba and Hutchison [1987] make a distinction between experts and novices, and familiar and unfamiliar. Kogut and Zander [1992] propose information and know-how. Page and Uncles [2004] divide knowledge into common and specialized knowledge, respectively, referring to "general and or publicly-known information of the domain of interest required to perform general and common domain-related tasks successfully," and "skilled and/or extraordinary information about a domain of interest required to perform skilled domain-related tasks successfully"(p. 577).

Based on IDT and learning theory, Kwak *et al*. (forthcoming) propose the security knowledge process model. In IDT, Rogers [2003] states that knowledge influences persuasion, which in

turn affects decisions and implementation. Learning is generally defined as obtaining knowledge. Learning is applied in both the individual and organizational levels, and assumes that previous relevant knowledge of individuals and organizations is required to gain new knowledge and ideas. Bower and Hilgard [1981] argue that accumulation of previous knowledge facilitates the ability to put new information into an individual's memory system and the ability to remember and exploit it. The security knowledge process model posited by Kwak *et al*. (forthcoming) includes three constructs: security familiarity, spyware awareness, and spyware knowledge. Security familiarity is broad and general knowledge, while spyware knowledge deals with a narrow and specific topic. Spyware awareness lies between security familiarity and spyware knowledge.

Since the present study examines cultural differences in security knowledge levels between Korea and the U.S., the next section of this literature review briefly examines relevant cultural differences between the two countries.

2.3 Cultural Differences between Korea and the U.S.

This section briefly introduces the IT-related status and Hofstede's cultural dimensions of two countries (Korea and the U.S.), and provides rationales for the importance of the individual/collectivism dimension. Korea and the U.S. have democracies with well-developed economies. According to Internet World [2010], both countries are among the most wired and advanced countries in terms of IT infrastructure. These selection factors enable researchers to have a comparable base that is relatively unbiased from the noise of other unrelated factors [Dinev *et al*., 2009]. <Table 1> provides demographic, economic and Internet related profiles of Korea and the U.S.

In security research, cultural factors influence how a society perceives computer security issues [Schmidt *et al*., 2008]. Korea and the U.S. have quite different cultures based on Hofstede's cultural dimensions as shown in <Table 2>.

Korea has a high uncertainty avoidance (UAI) at 85 (vs. U.S. at 46), implying Korean society's low uncertainty tolerance [Hofstede, 2001]. Also, Korea has a higher power distance (PDI) (60) than the U.S. (40), suggesting that Koreans are relatively more admitting of unequal power distribution and more concerned with group interests [Dinev *et al*., 2008]. Koreans are likely to be more formal, cooperative and collectivistic, suggested from the long-term orientation index (Korea: 75 vs. U.S.: 29). Korea has a low masculinity index (MAS) (39) compared to the U.S. (62).

The most explicit difference between Korea and the U.S. is on the individualism/collectivism dimension. An individualism indicator (IDV) pertains to a culture in which group relationships are weak and not unified. The U.S. (91), Australia (90), and the United Kingdom (89) are in the extreme of high individualism cultures, while Taiwan (17), Korea (18), and China (20) are in the other extreme of high collectivism cultures. According to Triandis [2001] individualism/collectivism has been regarded as the most significant dimension explaining differences across cultures. In the individualistic cultures, social behaviors are mainly guided by personal goals, while in collectivistic cultures the

<Table 1> Demographic, Economic and Internet-Related Profiles of Korea and the U.S.

Categories		Korea	U.S.
Demography	population[2] (2010 est.)	48,636,068 ***(26)***	310,232,863 ***(3)***
	Literacy[2] (Age 15+ can read and write)	Total population: 97.9% Male: 99.2% Female: 96.6% (2002 est.)	Total population: 99% Male: 99% Female: 99% (2003 est.)
	Ethnic groups[2]	Homogeneous (Korean)	White 79.96%, Black 12.85%, Asian 4.43%, Amerindian and Alaska Native 0.97%, Native Hawaiian and other Pacific islander 0.18%, two or more races 1.61% (2007 est.)
	Religions	Buddhist 26% Protestant 19% Roman Catholic 7% Others 2% None 46% (2008 est.)[3]	Protestant 51.3% RomanCatholic 23.9% Mormon 1.7% Other Christian 1.6% Jewish 1.7% Buddhist 0.7% Muslim 0.6% Other or unspecified 2.5% Unaffiliated 12.1% None 4% (2007 est.) [2]
Economy	GDP per capita[4] [2009]	$17,078	$46,436
	GNI per capita[4] [2009]	$27,310	$46,730
Internet	Internet Users[2] [2009]	39,440,000 ***(11)***	245,000,000 ***(2)***
	Internet Host[2] [2010]	291,329 ***(58)***	439,000,000 ***(1)***
	Internet Penetration[1] (Internet use/ Population)	39.6%[2000] 63.3%[2005] 66.5%[2006] 70.7%[2008] 77.3%[2009] 81.8%[2010]	44.1%[2000] 50.0%[2001] 58.0%[2002] 59.2%[2003] 68.8%[2004] 68.1%[2005] 70.2%[2007] 72.5%[2008] 74.1%[2009] 77.3%[2010]

Source) Adapted from Hwang *et al*. [2006].

Note) 1) The Internet World Stats. http://www.internetworldstats.com [2/13/2011].

2) CIA World Factbook. https://www.cia.gov/library/publications/the-world-factbook/[2/13/2011].

3) Korean National Statistics Office. http://kostat.go.kr/portal/korea/[10/6/2008].

4) World Bank, http://www.worldbank.org/[2/13/2011].

(Number) Rank comparison to the world.

<Table 2> Definitions of Cultural Dimensions

Dimensions	Definitions	Korea	U.S.
Power Distance (PDI)	Degree to which the less powerful members of groups accept and expect that power is distributed unequally	60	40
Individualism/ Collectivism (IND)	Degree to which the individual highlights one's own needs as opposed to the group needs and prefer to act as an individual rather than as a member of a group.	18	91
Masculinity/Femininity (MAS)	Degree to the distribution of roles between the genders	39	62
Uncertainty Avoidance (UAI)	Degree to which one feels threatened by uncertain and ambiguous situation.	85	46
Long-Term Orientation (LTO)	Degree to which the society places great significance on thrift, persistence and long-term alliance.	75	29

Source) Hofstede [2010] and Srite and Karahanna [2006].

goals of the collective have the dominant influence in shaping behaviors [Triandis, 1989]. It is also an important theme in almost 100 published articles annually on cultural differences [Triandis and Suh, 2002].

This section discussed broad cultural differences between Korea and the U.S.; the next section examines a more specific set of literature related to this study; that is, how these cultural differences influence IT security issues.

2.4 Cultural Effects on Security

Previous literature has addressed cultural effects in a security domain. In the security knowledge process model, Kwak *et al*. (forthcoming) argue that cultural differences moderately influence the relationship between spyware awareness and spyware knowledge. The researchers posit that this occurs because an individual who is aware of spyware and who comes from a high uncertainty avoidance society will readily shape her knowledge of spyware in order to avoid unexpected spyware risks.

Dinev *et al*. [2008] report in a comparative study between Korea and the U.S. that notable differences are detected in the relationship between subjective norms and intention to use anti-spyware, between spyware awareness and attitude toward spyware, and between spyware awareness and intention to use anti-spyware. Similarly, Schmidt *et al*. [2008] report that the U.S. respondents perceive themselves to be more aware of spyware and viruses than do Chinese respondents, suggesting that two distinct cultures (i.e., individualism and collectivism) are significant factors which explain differences in security awareness between the U.S. and China.

To set the base for the current research hypotheses, analyses and discussions that follow, the literature review has discussed spyware technology as well as relevant literature related to security and knowledge. The current research addresses cultural differences as related to security knowledge. Given the literature on cultural differences between Korea and the U.S. and previous research that studied the impact of culture on IT perception, this study provides three hypotheses, which are found in the next section.

Ⅲ. Hypotheses

Based on the security knowledge process model [Kwak *et al*., forthcoming], the current study examines three constructs (i.e., security familiarity, spyware awareness, and spyware knowledge) to compare between Korea and the U.S. Security familiarity is defined as an individual's understanding based on prior interaction, experience, and learning regarding issues of security [Gefen *et al*., 2003]. Spyware awareness is defined as an individual's "raised consciousness of interest in knowing about technological issues and strategies to deal with spyware" [Dinev and Hu, 2007, p. 391]. Spyware knowledge is defined as an individual's understanding of spyware in terms of what it is and what it does [Zhang, 2005].

The current study argues that security knowledge levels vary across cultures. The purpose of this study is to examine whether security knowledge levels are different across countries with different cultures. This study mainly deals with individualism/collectivism to examine its effect on security knowledge. As mentioned in the literature review, the U.S. has an individualistic culture, whereas Korea has a more collectivistic culture.

The present study posits that an individualistic culture strongly influences security awareness of U.S. people. However, since Korean society regards harmony and collaboration as important values, these could negatively influence Koreans' awareness of security and privacy. Similarly, Schmidt *et al*. [2008] find that U.S. respondents have a higher security awareness level than Chinese respondents in terms of spyware and viruses.

While Korean culture embraces a collective norm, U.S. culture emphasizes individuals' independence. For U.S. people, personal interests take priority over a group's goal. In addition, those from the U.S. are repulsed by the acceptance of group norms when the group norm infringes upon their privacy and interests. Moreover, U.S. individuals generally make decisions independently. The individualistic lifestyle in the U.S. contrasts with Koreans' collectivistic lifestyle, which highlights group norms.

In the U.S., individuals' lives and privacies are strongly protected. On the other hand, Korea has a lower level of privacy protection for individuals. Collectivistic cultures emphasize group identity rather than personal identity. In addition, personal privacy is sometimes sacrificed for community interests in a collectivistic culture. In the job security context, individualists respond more positively to job insecurity, while collectivists react negatively [Probst and Lawler, 2006].

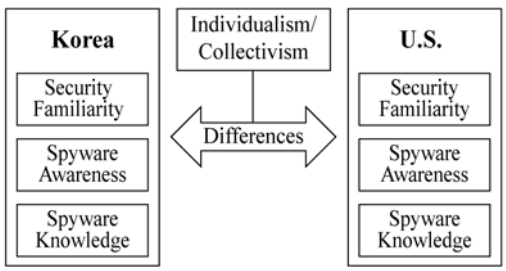
Individualists have a higher tolerance of risks and are more willing to adopt strategies that safeguard IT. Also, individualists are more sensitive to privacy and security issues than collectivists [Chen *et al*., 2008]. In addition, U.S. users who receive situational security awareness learning outperform those users who receive the traditional face-to-face instruction, whereas Taiwanese users do not perform significantly differently [Chen *et al*., 2008] based on instructional strategies. Based on the above findings, the following hypotheses are posited:

Hypothesis 1: The level of security familiarity is lower in Korea than in the U.S.

Hypothesis 2: The level of spyware awareness is lower in Korea than in the U.S.

Hypothesis 3: The level of spyware knowledge is lower in Korea than in the U.S.

<Figure 1> presents the research model of this study. Having addressed the purpose and hypotheses in this section, research methods and results are discussed in the next section.



<Figure 1> Research Model

Ⅳ. Methods and Results

4.1 Item Development and Participants

The current research study employs and modifies previously validated scales to measure the research constructs. <Table 3> illustrates all measurement items used in this study. After developing the survey in English, a pilot test was conducted to test initial validity and reliability as well as to identify ambiguity in item wording. Based on the survey in English, the first author, a native Korean, translated the survey instrument into Korean. The survey in Korean was then peer-reviewed to verify the English to Korean translation.

The participants for this study were undergraduate and graduate students currently enrolled at both a mid-sized public university in the U.S. and a large private university in Korea. A paper-based survey was filled out by respondents in selected classes at both the Korean and U.S. universities.

A total of 696 students (Korea: 336, U.S.: 360) participated in the survey. Surveys with more than two missing values for one construct were eliminated. The total number of usable responses was 686 (Korea: 329, U.S.: 357). The demographics in both Korea and the U.S. were analyzed and are presented in <Table 4>.

<Table 3> Survey Items

Constructs	Codes	Names	Items	Sources
Security Familiarity (SF)	SF1*	Privacy Violation	I am familiar with privacy violation issues on the Internet.	Zhang [2005] Gefen *et al.* [2003]
	SF2	Protection Knowledge	I am familiar with technologies which protect people.	
	SF3	Security Technology	I am familiar with security technology.	
	SF4	Information Security	I am familiar with information security.	
Spyware Awareness (SA)	SA1	Malicious Software	I know about the problems of malicious software intruding Internet users' computers.	Dinev and Hu [2007]
	SA2	Seeking Advice	I seek advice on computer web sites or magazines about anti-spyware products.	
	SA3	Spyware Problem	I have knowledge of spyware problems and consequences.	
Spyware Knowledge (SK)	SK1	Tracing Keystroke	What is your knowledge that spyware can trace keystrokes?	Dinev and Hu [2007] Zhang [2005]
	SK2	Residing on Computer	What is your knowledge that spyware can reside on computer?	
	SK3	Monitoring Users	What is your knowledge that spyware can monitor surfing behavior?	
	SK4	Recording Transaction	What is your knowledge that spyware can record online transactions?	

Note) *: Items dropped after testing of measurement properties.

<Table 4> Demographic Information

Variables	Category	Korea N = 329(%)	U.S. N = 357(%)
Gender	Male	167(50.8)	143(40.1)
	Female	162(49.2)	214(59.9)
Age	18~27	326(99.1)	334(93.6)
	28~35	-	19(5.3)
	> 35	3(0.8)	4(1.1)
Class Standing	Freshman	74(22.5)	155(43.4)
	Sophomore	95(28.9)	62(17.4)
	Junior	90(27.4)	57(16.0)
	Senior	63(19.1)	74(20.7)
	Graduate	7(2.1)	9(2.5)

<Table 5> Results of Exploratory Factor Analysis

	Korea			U.S		
	SF	SA	SK	SF	SA	SK
SF1	**.543**	.137	.156	**.885**	.161	.108
SF2	**.838**	.175	.044	**.904**	.261	.165
SF3	**.877**	.212	.150	**.864**	.350	.194
SF4	**.872**	.218	.177	**.814**	.384	.235
SA1	.275	**.817**	.191	.373	**.752**	.314
SA2	.219	**.787**	.296	.279	**.797**	.254
SA3	.249	**.840**	.309	.346	**.827**	.269
SK1	.147	.200	**.831**	.190	.196	**.790**
SK2	.121	.245	**.782**	.108	.267	**.877**
SK3	.141	.230	**.904**	.162	.212	**.915**
SK4	.172	.184	**.883**	.169	.178	**.892**

4.2 Measurement Model

Broadly, two steps are applied for this study: measurement validation and hypothesis testing. In measurement validation, exploratory factor analysis (EFA) using SPSS 15.0 and confirmatory factor analysis (CFA) using AMOS 7.0 are employed. To test research hypotheses, analysis of covariance (ANCOVA) is incorporated using SPSS 15.0.

EFA was conducted to identify whether the correlations between a set of indicators stem from their relationship to one or more constructs in the data, suggesting discriminant validity. Three of the proposed constructs that have been drawn from and modified from previous studies were examined with a principal components factor analysis using a Varimax rotation. No cross loadings above 0.40 werefound [Hair *et al.*, 2009]. All items measuring each construct were loaded into the intended factor, supporting the discriminant validity of the constructs.

After identifying initial validity from EFA, CFA was conducted to assess the measurement model. All criteria used for measurement of U.S. data were acceptable. In the Korean measurement, however, SF1 (Privacy Violation: 0.415) was below the recommended value of 0.70 of factor loading [Gefen *et al.*, 2000]; and composite reliability of security familiarity (0.659) was lower than the cutoff value of 0.70 [Hair *et al.*, 2009]. There are two possible reasons of the low factor loading of SF1. It could result from Korean respondents' misunderstanding of the survey questionnaire. In addition, since the original items were developed in the U.S. context, more reasonably, the survey item may not have been appropriate to measure security familiarity in Korea. To obtain an appropriate measurement model and to relevantly compare both countries, SF1 was removed and CFA was conducted again.

After dropping SF1, admissible measurement models for Korea and the U.S. are obtained. The factor loadings of the revised measurement

model were well above 0.70, [Gefen *et al.*, 2000], supporting convergent validity <Table 6>. The Cronbach's Alpha values were well above the cutoff value of 0.70 and composite reliability scores were over 0.70, suggesting a high reliability of the measurement model. The average variance extracted (AVE) values for the constructs were higher than 0.50 [Hair *et al.*, 2009], suggesting that the constructs captured a relatively high level of variance.

<Table 6> presents reliability and AVE values. To test discriminant validity, the square root of AVE for each construct was compared with the correlation values of the construct. Since AVE values were higher than the correlation values, the constructs were determined to be distinct <Table 7>. As shown in <Table 8>, the fit indices of the revised measurement models are within the desired values.

<Table 6> Standardized Factor Loading

Constructs	Items	Initial Model		Revised Model	
		Korea	U.S.	Korea	U.S.
Security Familiarity (SF)	SF1	**.415**	.812	Dropped	
	SF2	.726	.925	.723	.912
	SF3	.931	.962	.938	.967
	SF4	.936	.924	.932	.928
Spyware Awareness (SA)	SA1	.793	.871	.793	.870
	SA2	.796	.782	.796	.782
	SA3	.923	.917	.923	.918
Spyware Knowledge (SK)	SK1	.793	.741	.793	.741
	SK2	.751	.887	.751	.887
	SK3	.957	.967	.957	.967
	SK4	.907	.908	.907	.908

<Table 7> Reliability, AVE, and Correlations

Constructs	Cronbach's Alpha		Composite Reliability		Korea			U.S.		
	Korea	U.S	Korea	U.S	SF	SA	SK	SF	SA	SK
Security Familiarity	0.835	0.949	0.780	0.884	**0.757**			**0.877**		
Spyware Awareness	0.871	0.889	0.739	0.765	*0.541*	**0.705**		*0.738*	**0.737**	
Spyware Knowledge	0.912	0.930	0.761	0.795	*0.378*	*0.581*	**0.733**	*0.435*	*0.584*	**0.774**

Note) Bold: Average Variance Extracted (AVE), Italic: Correlation Coefficient.

<Table 8> Goodness of Fit of Measurement Model

	Korea		U.S.		Desired Level
	Initial	Revised	Initial	Revised	
# of Items	11	10	11	10	-
X^2	121.499	74.422	136.278	86.338	Smaller
df	41	32	41	32	-
X^2/df	2.963	2.326	3.324	2.698	< 3.0
GFI	.933	.955	.931	.953	> 0.9
AGFI	.893	.922	.889	.920	> 0.8
RMSEA	.077	.064	.081	.069	< 0.08
NFI	.953	.970	.965	.975	> 0.90
CFI	.968	.983	.975	.984	> 0.90

4.3 Hypothesis Testing

Using the revised measurement models, the hypotheses were tested using ANCOVA. ANCOVA is a type of analysis of variance (ANOVA) which can choose covariates. Based on previous literature [Looney *et al.*, 2008; Venkatesh *et al.*, 2003], gender, age, major, and college year are selected as covariates. Gender is a significant predictor of online channel preference [Looney *et al.*, 2008]. In the Unified Theory of Acceptance and Use of Technology [Venkatesh *et al.*, 2003], gender, age, voluntariness, and experience are moderators of technology acceptance. In addition, college major and year are chosen because they are related to students' experiences.

The results indicate that level of security knowledge of the U.S. is significantly higher than that of Korea, supporting H1 (security familiarity: $F = 21.275$, $p < 0.001$), H2 (spyware awareness: $F = 19.242$, $p < 0.001$), and H3 (spyware knowledge: $F = 16.201$, $p < 0.001$). Results of ANCOVA and a summary of hypothesis testing results are shown in <Table 9> and <Table 10>, respectively.

In this section, the analyses of hypotheses were summarized; the next section discusses implications and conclusions of the research study.

<Table 9> Results of ANOVA and ANCOVA

Source of Variance	Korea		U.S.		Mean difference	ANOVA		ANCOVA	
	Mean	Std. Dev	Mean	Std. Dev		t-value	p-value	Mean Square	F-Value
Security Familiarity	3.379	1.155	4.311	1.552	.932	8.865	***	39.073	21.275***
Gender								2.704	1.472
Major								20.596	11.214**
College Year								.021	.011
Age								4.579	2.493
Spyware Awareness	2.829	1.342	3.329	1.598	.500	4.418	***	38.232	19.242***
Gender								40.653	20.461***
Major								25.135	12.651***
College Year								2.970	1.495
Age								8.857	4.458*
Spyware Knowledge	3.388	1.725	3.592	1.759	.204	1.527	0.127	44.379	16.201***
Gender								55.837	20.384***
Major								56.477	20.618***
College Year								19.849	7.246**
Age								.089	.033

Note) *: p-value < .05, **: p-value < .01, ***: p-value < .001.

<Table 10> Summary of Hypothesis Testing

Hypotheses		Results
H1	Level of security familiarity is lower in Korea than in the U.S.	Supported
H2	Level of spyware awareness is lower in Korea than in the U.S.	Supported
H3	Level of spyware knowledge is lower in Korea than in the U.S.	Supported

V. Discussion and Conclusion

5.1 Discussion and Implications

The results show that significant security knowledge differences exist between Korea and the U.S. Regarding all levels of security knowledge, the U.S. results were significantly higher than Korean results. Like the U.S., Korea has a well-developed Internet environment and the Internet is one of the major channels of selling and marketing for businesses. However, Korean respondents consider themselves less knowledgeable regarding security issues. As mentioned earlier, the diversity reflected in the individualistic/collectivistic culture of the two countries studied might explain why individualists' possessed a high security awareness and collectivists' possessed a low security awareness. This individualistic/collectivistic cultural difference might also explain Koreans' relatively low security knowledge.

Individualists are more sensitive to privacy and are thus more aware of security issues. Moreover, they are willing to acquire relevant security knowledge to cope with potential threats [Chen *et al*., 2008]. In addition, a possible explanation for the results is that privacy issues have been well instilled in individualistic countries, and thus people in the individualistic countries are more knowledgeable in security issues. Some researchers suggest cultural aspects regarding Koreans' low security and privacy concerns. For example, Sung [2004] suggests that Koreans have been in a unified community with large family systems and have less privacy overall.

To compare Korea with the U.S., this study controlled four variables (i.e., gender, major, college year, and age) which could influence security knowledge levels. Without controlling those variables, the results of ANOVA <Table 5> indicate that there are significant differences in security familiarity and spyware awareness, but no significant difference emerged in spyware knowledge, suggesting confounding effects of those control variables. To remove the confounding effects, this study conducted ANCOVA.

Gender has effects on spyware awareness and spyware knowledge but no effect on security familiarity. One possible explanation is that there is no difference between men and women in the broad concept of security (e.g., security familiarity) while significant differences exist in the specific domain of security (e.g., spyware awareness and spyware knowledge). Attitudinal research suggests that more accurate results are derived from more specific (as opposed to general) factors; this may also explain why significance was found between genders for the more specific factors and not for the more general factor studied.

As expected, college major influences all levels of security knowledge, confirming that there are differences among engineering, business majors, and others. College year only impacts spyware knowledge, suggesting that the more specialized area of security knowledge is influenced by college experience. For example, seniors can be assumed to have more specialized learning in their major than freshmen and are therefore significantly more knowledgeable. Age influences only spyware awareness, implying that people can be aware of spyware issues in their general experience (web shopping, Internet

surfing, or media).

This study has several implications for research and practice. For researchers, this study divided security knowledge levels into three types (security familiarity, spyware awareness, and spyware knowledge) and showed that there are significant differences between Korea and the U.S. This implies that the cultural difference is an important factor affecting security knowledge levels among different countries. The findings of this study extend research for security, culture, and knowledge.

For practitioners, the findings of this study will help multi-national corporations address concerns about customers regarding security and privacy in terms of different cultures. Providing more information about security issues and education in collectivistic cultures would be an effective strategy to increase the number of visits to their Websites. In addition, security managers could focus on instilling security knowledge to employees from collectivistic cultures. This would help firms reduce their overall security costs. Moreover, multi-national corporations can design different security management and education programs for firms operating in different cultural contexts.

The implications of the research findings were discussed in this section; next, limitations and directions for future research are provided.

5.2 Limitations and Future Research

As usual, this study is not free from limitations. The first limitation is using student samples. To achieve generalizability, future researchers should incorporate more generalized samples. According to Cook and Campbell [1979], convenience sampling limits representativeness of the population, suggesting a second limitation of this study. Third, Korea and the U.S. were selected to compare security knowledge levels with respect to individualistic/collectivistic cultures. This study design may have limited the global implications of the results. The study shows that Korean and U.S. respondents have different levels of security knowledge as expected due to different cultures. More countries which represent different cultures should be included in future research for validity of cross-cultural research. For example, China (collectivism) and Canada (individualism) can be added for extension and validation of the results of this and related studies. Fourth, this study used one university in each country. The selected Korean university is large and private, and located in a suburban area. The chosen U.S. university is middle sized and public, and located in rural area. Possible biases from these factors could exist. This study follows the guidelines of cross-cultural research [Karahanna *et al*., 2002], but there could be administrative errors and mistranslations in conducting research at two different countries.

Many research opportunities exist for future research related to this study. This study found that some demographic factors influence security knowledge levels in Korea and the U.S., and other factors could be examined such as Internet infrastructure levels. This study examined two groups (Korea and the U.S.); other comparison groups (e.g., gender) could be studied in the future. This study assumed that Korea and the U.S. represent collectivism and individualism based on Hofstede's cultural dimension. This may or may not be true. For

example, Srite and Karahanna [2006] examine how espoused cultural value moderated technology adoption. Future researchers can incorporate such specified items which can measure culture at the individual level. Also, more detailed security knowledge can be compared between Korea and the U.S. as Schmidt *et al*. [2008] do. Schmidt *et al*. examine security knowledge comparison between the U.S. and China in terms of rootkits, spyware, computer viruses and Trilobyte viruses.

Positive technologies play a critical role in the world. However, negative technologies are serious threats. Security knowledge is one important factor in coping with these threats. This study showed that a country with collectivism has a lower level of security awareness compared to a country with individualism.

〈References〉

[1] Alba, J.W. and Hutchinson, J.W., "Dimensions of Consumer Expertise," *Journal of Consumer Research*, Vol. 13, No. 4, 1987, pp. 411-454.

[2] Arnett, K.P. and Schmidt, M.B., "Busting the Ghost in the Machine," *Communications of the ACM*, Vol. 48, No. 8, 2005, pp. 92-95.

[3] Asaravala, A., "Sick of Spam? Prepare for Adware," *Wired News*, Retrieved 2011. 2. 20 from http://www.wired.com/science/discoveries/news/2004/05/63345, 2004.

[4] Baker, W.M., "What's Your Main Technology Concern?," *Strategic Finance*, December, 2006, pp. 49-54.

[5] Bower, G.H. and Hilgard, E.R., *Theories of Learning*, Englewood Cliffs, NJ: Prentice-Hall, 1981.

[6] Chen, C.C., Medlin B.D., and Shaw, R.S., "A Cross-Cultural Investigation of Situational Information Security Awareness Programs," *Information Management and Computer Security*, Vol. 16, No. 4, 2008, pp. 360-376.

[7] Chen, Y. and Zahedi, F.M., "Internet Users Security Behaviors and Trust," *Proceedings of the Pre-ICIS Workshop on Privacy and Security*, 2009.

[8] Claburn, T., "70 of Top 100 Web Sites Spread Malware," *InformationWeek*, Retrieved 2011. 2. 20 from http://www.informationweek.com/news/internet/security/212901775, 2009.

[9] Cohen, J.E., "DRM and Privacy," *Communications of the ACM*, Vol. 46, No. 4, 2003, pp. 46-49.

[10] Computer Security Institute, "CSI Computer Crime and Security Survey 2009," Retrieved 2010. 2. 20, from http://gocsi.com/survey, 2009.

[11] Consumer Reports, "Social Insecurity: What Millions of Online Users Don't Know Can Hurt Them," Retrieved 2010. 8. 20 from http://www.consumerreports.org/cro/magazine-archive/2010/june/electronics-computers/social-insecurity/overview/index.htm, 2010.

[12] Cook, T.D. and Campbell, D.T., *Quasi Experimentation: Design and Analytical Issues for Field Settings*, Chicago, IL: Rand McNally, 1979.

[13] Dhillon, G. and Backhouse, J., "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal*, Vol. 11, No. 2, 2001, pp. 127-153.

[14] Dinev, T. and Hu, Q., "The Centrality of Awareness in the Formation of User Beha-

vioral Intention toward Protective Information technology," *Journal of the Association for Information Systems*, Vol. 8, No. 7, 2007, pp. 386-408.

[15] Dinev, T., Goo, J., Hu, Q., and Nam, K., "User Behaviour towards Protective Information Technologies: The Role of National Cultural Differences," *Information Systems Journal,* Vol. 19, No. 4, 2009, pp. 391-412.

[16] Fishbein, M. and Ajzen, I., *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley, 1975.

[17] Gefen, D., Karahanna, E., and Straub, D.W., "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly*, Vol. 27, No. 1, 2003, pp. 51-90.

[18] Gefen, D., Straub, D.W., and Boudreau, M.C., "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of AIS*, Vol. 4, No. 7, 2000, pp. 1-79.

[19] Hair, J.F., Tatham, R.L., Anderson, R.E., and Black, W., *Multivariate Data Analysis*, 7th ed., Englewood Cliffs, NJ: Prentice-Hall, 2009.

[20] Hofstede, G., *Culture's Consequences*, 2nd ed., Thousand Oaks, CA: Sage Publications, 2001.

[21] Hofstede, G., Geert Hofstede Cultural Dimensions, Retrieved 2010. 12. 12. from http://www.geert-hofstede.com, 2010.

[22] Hwang, W., Jung, H.-S., and Salvendy, G., "Internationalisation of E-Commerce: A Comparison of Online Shopping Preferences among Korean, Turkish and US populations," *Behaviour and Information Technology*, Vol. 25, No. 1, 2006, pp. 3-18.

[23] Im, G.P. and Baskerville, R.L., "A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error," *The DATA BASE for Advances in Information Systems*, Vol. 36, No. 4, 2005, pp. 68-79.

[24] Internet World Stat, "World Internet Usage and Population Statistics," Retrieved 2010. 8. 20 from http://www.internetworldstats.com, 2010.

[25] Johnston, A.C. and Warkentin, M., "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly*, Vol. 34, No. 3, 2010, pp. 549-566.

[26] Karahanna, E., Evaristo, J.R., and Srite, M., "Methodological Issues in MIS Cross-Cultural Research," *Journal of Global Information Management*, Vol. 10, No. 1, 2002, pp. 48-55.

[27] Kenyon, H.S., "Spyware Stymies Network Operators," *Armed Forces Communications and Electronics Association*, Vol. 58, No. 12, 2004, pp. 47-48.

[28] Kogut, B. and Zander, U., "Knowledge of the Firm, Combinative Capabilities and the Replication of Technology," *Organization Science*, Vol. 3, No. 3, 1992, pp. 383-397.

[29] Kwak, D.-H., Kizzier, D., Zo, H., and Jung, E., "Cross-Cultural Investigation of Security Knowledge Process," *International Journal of Business Information Systems*, Forthcoming.

[30] Lee, Y. and Kozar, K.A., "An Empirical Investigation of Anti-Spyware Software Adoption: A Multi theoretical Perspective," *Information and Management*, Vol. 45, No. 2, 2008, pp. 109-119.

[31] Lee, Y. and Kozar, K.A., "Investigating Factors Affecting the Adoption of Anti-spyware Systems," *Communication of the ACM*, Vol. 48, No. 8, 2005, pp. 72-77.

[32] Liang, H. and Xue Y., "Avoidance of Infor-

mation Technology Threats: A Theoretical Perspective," *MIS Quarterly*, Vol. 33, No. 1, 2009, pp. 71-90.

[33] Looney, C.A., Akbulut, A.Y., and Poston, R.S., "Understanding the Determinants of Service Channel Preference in the Early Stages of Adoption: A Social Cognitive Perspective on Online Brokerage Services," *Decision Sciences*, Vol. 39, No. 4, 2008, pp. 821-857.

[34] Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A., "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules: An Empirical Study," *European Journal of Information Systems*, Vol. 18, No. 2, 2009, pp. 126-139.

[35] Page, K. and Uncles, M., "Consumer Knowledge of the World Wide Web: Conceptualization and Measurement," *Psychology and Marketing*, Vol. 21, No. 8, 2004, pp. 573-591.

[36] Probst, T.M. and Lawler, J., "Cultural Values as Moderators of the Outcomes of Job Insecurity: The Role of Individualism and Collectivism," *Applied Psychology: An International Review*, Vol. 55, No. 2, 2006, pp. 234-254.

[37] Rogers, E.M., *Diffusion of Innovations*, 5th ed., New York, NY: Free Press, 2003.

[38] Schmidt, M.B., Johnston, A.C., Arnett, K.P., Chen, J.Q., and Li, S., "A Cross-Cultural Comparison of U.S. and Chinese Computer Security Awareness," *Journal of Global Information Management*, Vol. 16, No. 2, 2008, pp. 91-103.

[39] Spring, T., "Striking Back at Spyware," *PC World*, Vol. 33, No. 1, 2004, pp. 36-38.

[40] Sriramachandramurthy, R., Balasubramanian, S., and Hodis, M., "Spyware and Adware: How do Internet Users Defend Themselves?," *American Journal of Business*, Vol. 24, No. 2, 2009, pp. 41-52.

[41] Srite, M. and Karahanna, E., "The Role of Espoused National Cultural Values in Technology Acceptance," *MIS Quarterly*, Vol. 30, No. 3, 2006, pp. 679-704.

[42] Stafford, T.F. and Urbaczewski, A., "Spyware: The Ghost in the Machine," *Communications of the AIS*, Vol. 14, No. 1, 2004, pp. 291-306.

[43] Straub, D. and Welke, R., "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, Vol. 22, No. 4, 1998, pp. 441-469.

[44] Straub, D., "Effective IS Security: An Empirical Study," *Information Systems Research*, Vol. 1, No. 3, 1990, pp. 255-276.

[45] Sun, L., Srivastava, R.P., and Mock, T.J., "An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions," *Journal of Management Information Systems*, Vol. 22, No. 4, 2006, pp. 109-142.

[46] Sung, S., "There is No Cyber Privacy(?)," *Digital Contents*, April, 2004, pp. 120-128.

[47] Triandis H.C., "The Self and Social Behavior in Differing Cultural Contexts," *Psychological Review*, Vol. 96, No. 3, 1989, pp. 269-289.

[48] Triandis, H.C. and Suh, E.M., "Cultural Influences on Personality," *Annual Review of Psychology*, Vol. 53, 2002, pp. 133-160.

[49] Triandis, H.C., "Individualism-Collectivism and Personality," *Journal of Personality*, Vol. 69, No. 6, 2001, pp. 907-924.

[50] Venkatesh, V., Morris, M.G., Davis, F.D., and Davis, G.B., "User Acceptance of Infor-

mation Technology: Toward a Unified View," *MIS Quarterly*, Vol. 27, No. 3, 2003, pp. 425-478.

[51] Warkentin, M., Luo, X., and Templeton, G. F., "A Framework for Spyware Assessment," *Communication of the ACM*, Vol. 48, No. 8, 2005, pp. 79-84.

[52] Zhang, X., "What Do Consumers Really Know About Spyware?," *Communication of the ACM*, Vol. 48, No. 8, 2005, pp. 45-48.

◆ About the Authors ◆

Dong-Heon Kwak
Dong-Heon Kwak is a Ph.D. student in MIS at the University of Wisconsin – Milwaukee. He received BA in sociology and BBA in management from Yeungnam University, and MS in information systems from Morehead State University. His research interests are online prosocial behavior, technology acceptance, inter-organizational systems and relationships, security, culture, charity website design, and web mining. His research has appeared or is forthcoming in International Journal of Business Information Systems and HICSS.

Donna McAlister Kizzier
Donna McAlister Kizzier is an associate professor at Morehead State University. Her doctorate is from the University of Nebraska-Lincoln; she completed the advanced post-doctoral AACSB MIS Institute and has served three U.S. universities as a senior professor. Her research interests include collaborative and technological learning decision models, planning and implementing information systems, change strategies, and research methods. She has chaired graduate programs at multiple universities and has served in several leadership positions for state, national and international business professional organizations. She has authored and served in editorial positions for multiple scholarly books, chapters, proceedings, and refereed journals.

Hangjung Zo
Hangjung Zo is Assistant professor of MIS in the Department of Management Science at Korea Advanced Institute of Science and Technology. He received his Ph.D. in MIS from the University of Wisconsin-Milwaukee. His research interests include Web services and Web-based systems, e-business and e-commerce, software engineering, business process management, and IT strategy. His papers have appeared in IEEE Transactions on Systems Man and Cybernetics, Decision Support Systems, Journal of Business Research, Asia Pacific Journal of Information Systems, HICSS, among others. He was the chair for the ICT Innovations and Progresses in Developing Countries Workshop at ICCIT 2009.

Euisung Jung
Euisung Jung is a Ph.D. student in MIS at the University of Wisconsin – Milwaukee. He received BBA in management and MBA from Kyungpook National University. His research interests are inter-organizational systems and data integration, Internet banking and Database. Euisung has over 8 years of experience in information systems research and development at Korea Environment Institute and Shinhan Financial Group. His research has appeared or is forthcoming in International Journal of Business Information Systems, HICSS, and AMCIS.

Submitted : March 9, 2011 Accepted : July 15, 2011
1st revision : June 10, 2011