INFORMATION SECURITY COLLECTIVE EFFICACY AND VULNERABILITY: A CROSS-COUNTRY COMPARISON

Completed Research Paper

Dan J. Kim
University of North Texas
Denton, Texas 76201
dan.kim@unt.edu

Young U. Ryu
The University of Texas at Dallas
Richardson, Texas 75080
ryoung@utdallas.edu

Young Kwark
University of Florida
Gainesville, Florida 32611
young.kwark@warrington.ufl.edu

Abstract

Since Bandura's proposal of self-efficacy, studies have explained behavioral motivations at the individual level. However, little is known concerning self-efficacy's applicability at the group level in the information systems security (InfoSec) domain. Also, despite extensive cross-cultural analyses at the individual level, works at a group level are still in infancy. We, therefore, define InfoSec self-efficacy as a group-level construct and examine its impact on InfoSec vulnerability from cross-cultural perspectives. We draw on interdependent security and separate InfoSec vulnerability into vulnerability from self and partners. The goal is fourfold: (i) proposing InfoSec collective efficacy as a cultural construct, (ii) modeling relationships among InfoSec collective efficacy, InfoSec vulnerability, vulnerability from partners, and InfoSec control awareness from cross-cultural perspectives, (iii) validating the model using data collected from executive-level IS managers in the U.S. and South Korea, and (iv) providing implications for IS managers operating in multinational businesses.

Keywords: Security, Collective efficacy, Cross-country comparison, Cross-cultural issues

Introduction

Today's economy has been called an economy of computers and interconnection (McKnight and Bailey 1997), where the reliance on computers and network-based information systems is a routine matter not only within organizations but also throughout whole society. Firms heavily rely on various forms of inter-organizational systems for the success and sustainment. However, this reliance on globalized and interconnected networks has brought about a noticeable negative effect in the form of information security risk and vulnerability (EIU 1998; Udo 2001; Voloper 2008). Various forms of security breaches caused by both outside intruders and inside attackers (Deloitte 2009; ITRC 2011) are currently threatening not only firms but also ordinary members of the society. In-depth and multifaceted measures covering both technical and behavioral or perceptual aspects are needed for effective defense against security threats. This study addresses a basis of perceptual aspects of security behaviors of managers.

Following Bandura's proposal for a socio-cognitive concept of self-efficacy (Bandura 1986), researchers (Kwon et al. 2007; e.g., Lin 2006; Rhee et al. 2009; Scholz et al. 2002; Staples et al. 1999) have explained individuals' behavioral motivations and performances in different contexts. *Self-efficacy* refers to, "people's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances" (Bandura 1986, p.391). Self-efficacy can be understood as a person's own controllability or capabilities to obtain desirable outcome, as well as the "beliefs in one's capabilities to mobilize the motivation" needed to manage given situational tasks (Wood and Bandura 1989). High levels of self-efficacy contribute not only to higher levels of motivation and ability perception but also to higher levels of performance (Bandura 1995). Building self-efficacy is therefore a known method increasing an individual's performance.

The concept of self-efficacy can be extended to group-level efficacy, namely *collective efficacy* or *group efficacy*, defined as a group's shared belief in their capability to perform a specific task. Collective efficacy is an important group-level resource that contributes to a productive group climate. According to Bandura (1997), the self-efficacy at the group level has been shown to operate similarly to that at the individual level and through similar processes. In a group setting, knowledge of an individual's efficacy is related to perceived efficacy at the group level. While self-efficacy has been introduced and utilized in many information systems (IS) and behavioral sciences studies (e.g., Agarwal and Karahanna 2000; Compeau and Higgins 1995; Marakas et al. 1998; Venkatesh and Davis 1996), little is known regarding the applicability of collective efficacy in the area of information security (InfoSec). We are specifically interested in InfoSec collective efficacy from information systems executive managers' perspective because they are in charge of the overall information security within their organizations; they set priorities for the implementation of InfoSec measures and policies, determine InfoSec budgets, and make important decisions for their InfoSec programs.

Culture is an important element in the development of collective efficacy, and in turn it influences what people choose to do as a group (Bandura 1982). Comparisons of individual-level self-efficacy from a cross-cultural perspective have been conducted extensively in prior research (Cheung and Sun 1999; Klassen 2004; Scholz et al. 2002; Schwarzer et al. 1997; Schwarzer et al. 1999); however, research in the area of collective efficacy from a cross-cultural perspective is still in its infancy. In this study, focusing on information security we define InfoSec self-efficacy as a group level construct (i.e., *InfoSec collective efficacy*) and examine its impact on InfoSec vulnerability from a cross-cultural perspective. Moreover, drawing from the concept of interdependent security introduced by Kunreuther and Heal (2003), where Information security problems are interdependent when a risk faced by one firm is determined in part by the behavior of others, we divide InfoSec vulnerability into two separate elements: vulnerability from self and vulnerability from partners.

This study intends to focus on the following two research questions: *Does InfoSec collective efficacy influence InfoSec vulnerability in a group setting? Is there a significant difference in the effect of InfoSec collective efficacy between two countries: the U.S. and South Korea?* More specifically, the goal of this study is fourfold: (i) to propose *InfoSec collective efficacy* as a cultural construct, (ii) to propose a research model including theoretical relationships among InfoSec collective efficacy, InfoSec vulnerability, vulnerability from partners, and InfoSec control awareness and examine the effect of InfoSec collective efficacy from a cross-cultural perspective, (iii) to validate the proposed model using two sets of empirical

data collected from executive-level information systems managers in the U.S. and South Korea, and (iv) to provide theoretical and practical implications for information systems managers operating in multinational business settings.

Literature Review

We facilitate understanding of collective efficacy and its effect on vulnerability in the area of information security, by briefly reviewing its existing theoretical and empirical foundations as well as its relationship with culture, InfoSec vulnerability and awareness, and interdependent security.

Collective Efficacy and Culture

Self-efficacy has been found as the foundation of human agency in social cognitive theory and is considered to be an important factor governing human thought motivation and action (Bandura 1989). The self-efficacy belief leads to agency and an individual's overall judgment of his or her capacity to complete a task. As a part of social cognitive theory's extension to the group level, the concept of self-efficacy can be extended toward group efficacy or collective efficacy as a shared belief in the group's collective power to produce the desired outcome (Gibson 1999). Bandura (1986) asserts that collective efficacy beliefs are influenced by the same four sources of information that lead to the development of self-efficacy: prior performance accomplishments, vicarious experience, verbal persuasion, and physiological and emotional arousal (Bandura 1997). Various forms of efficacy terminologies have been used in publications such as collective efficacy, group efficacy, collective self-efficacy, and perceived collective efficacy. To be consistent, in this paper, we will use the terminology collective efficacy.

Studies have showed the influential role of self-efficacy as a universal construct (Bandura 1977; Bandura 1997; Bandura 2000; Bandura 2002; Bandura et al. 2001; Pajares and Graham 1999; Scholz et al. 2002; Stajkovic and Luthans 1998). In electronic commerce literature, several studies (Kacen and Lee 2002; Lee 2000; Pavlou and Chai 2002; Tan et al. 2004; Zakour 2004) have shown that consumers' online purchase behaviors are affected by several cognitive factors such as self-efficacy, trust, and controllability that are influenced by the cultural aspects. Although the effects of self-efficacy on cognition and motivation are universal across cultures, the ways it is developed and exercised vary (Bandura 2002; Klassen 2004; Oettingen 1995; Scholz et al. 2002; Schunk and Pajares 2009; Sia et al. 2009). A meta-analytical revie

Table 1. Cultural Characteristics of the U.S. and South Korea		
Cultural Constructs	Western Culture in the U.S.	Eastern Culture in South Korea
High Collective Efficacy vs. Low Collective Efficacy	- High self-efficacy at individual level - High collective-efficacy at group level - Optimism - Overconfidence	- Relatively low self-efficacy at individual level - Relatively low collective efficacy at group level - Humility and modesty
Individualism vs. Collectivism	- High individualism score - Goals, needs, and values of collectives are subordinated to those of individuals - Separate from social context, constant and stable - Internal, private (abilities, thoughts, and feelings) - Independent view of self - Decisions are weakly influenced by the group norm and members' opinions	- Low individualism score - Goals, needs, and values of individuals are subordinated to those of collectives - Connected with social context, flexible and variable - External, public (statuses, roles, and relationships) - Interdependent view of self - Decisions are strongly influenced by the group norm and members' opinions

Note: Cultural characteristics are based on results from Hofstede (1994; 2001), Morden (1999), and (Klassen 2004) .

InfoSec Awareness and Vulnerability

Awareness refers to an individual's passive comprehension on the needs, impetus, and specificity of issues, events, and processes; it increases interest toward certain issues such as social, sexual, medical, technology, and information security (Choi et al. 2008). Dinev and Hu (2007) defined general technology awareness as an individual user's knowledge of technological issues, problems, and skills. In the context of information security awareness concerns users' overall knowledge and understanding of issues related to information security as well as their ramifications (Bulgurcu et al. 2010). For organizations' InfoSec policies, awareness refers to a state where employees are aware of and committed to organizational security requirements (Siponen 2000). An organization is able to adjust its' preparation toward possible risk, remaining aware of the state of threats and vulnerabilities related to current information security environments. This can therefore be a highly significant factor leading an organization's overall security performance.

Many studies (Furnell et al. 2002; Hawkins et al. 2000; Hu and Dinev 2005; McLean 1992; Morwood 1998; Siponen 2000; Siponen 2001; Siponen and Kajava 1998; Spurling 1995; Straub 1990; Straub and Welke 1998) have shown that InfoSec awareness has been considered the most significant determinant of success in protecting information systems from security threats. Defining the usage of protective technology (e.g., anti-spyware) as an individual user's voluntary involvement to protect against negative technologies, Dinev and Hu (2007) found that the awareness of protective technology is a central determinant in a user's intention to use such protective technologies. They also found an organization, influence from InfoSec awareness on employees' attitudes toward compliance and outcome belief formation (Bulgurcu et al. 2010); An employee's attitude related to compliance is indirectly influenced by outcome beliefs shaped from the benefits or costs of compliance or noncompliance. To highlight the lack of security concern, Goodhue and Straub (1991) raise the importance of awareness in an individual's belief regarding InfoSec and argue that a user's concern for security is a function of three factors: industry risk, company actions made to maintain security, and individual awareness. They found that individual awareness is related to computer literacy.

Straub and Welke (1998) raised the issues of managers' naive responses to the challenges posed by the threat (Lock et al. 1992) and pointed to managers' lack of knowledge for effective control. They showed the theoretical background for effective countermeasures, suggesting a managerial guideline for coping with system risk by empirically identifying an approach that can effectively deal with the security risk. They presented how managers should cope with system risk more effectively by conducting qualitative studies in two information services Fortune 500 firms. Although researchers have noted the importance of managers' vigilance concerning the information security (Goodhue and Straub 1991; Hu and Dinev 2005; Loch et al. 1992; Straub and Welke 1998), few studies have examined the effect of managers' cognitive factors such as the managers' efficacy and awareness of the managers' perceived risk. Moreover,

to our best knowledge no study has yet been conducted on the effect of collective efficacy in the domain of information security (InfoSec) from the cross-cultural perspective.

Interdependent Security and Vulnerability from Others

In this study we view the source of InfoSec vulnerability as partially initiating with other connected partners. A recently raised issue concerning information security is the interdependent security problem introduced by Kunreuther and Heal (2003). The concept of interdependent security provides the theoretical background for vulnerability from others. Kunreuther and Heal (2003) argued that an organization's incentive to invest in protection against information security risk depends on how others manage their risks as well as how the firm manages its own risks. This is similarly understood for financial contagion issues where perceived financial weakness in one institution can lead to weaknesses in others that were not initially vulnerable (Allen and Gale 2000; Musumeci and Sinkey 1990; Polonchek and Miller 1999). Similarly, how managers perceive the risk induced by their partners is a critical factor influencing the managers' perceived risks due to the interplay between one agent's incentive that is more likely induced by the perceived risk and the behavior of the others (Kunreuther and Heal 2003). Due to its relative novelty in the area of interdependent security, very limited empirical studies have investigated the effect of vulnerability from other partners.

Group-level Construct in Information Systems Research

In this study, we measure the collective efficacy as a construct that bears the cultural traits from two different countries. Recently, research regarding technology adoption and virtual team performance has studied at the group-level (Hardin et al. 2007; Sarker et al. 2005). For example, Sarker et al. (2005) noticed the importance of group communication and group opinion formation toward Technology adoption and showed the psycho-social factors that affect group valence via group interaction and negotiation by changing a priori individual attitude toward technology. Rather, our focus is in finding cultural comparison between two groups by investigating the impact of collective efficacy in Information Security.

Research Model and Hypotheses

Motivated by this unaddressed issue we found through literature review, we propose InfoSec collective efficacy as an extended concept of self-efficacy at the group level in the context of information security. We develop a research model drawing from the literature on the theoretical relationships among collective efficacy, culture, awareness, and two types of vulnerabilities from the interdependent security perspective. A graphical form of nomological network with hypotheses is illustrated in Figure 1.

InfoSec Collective Efficacy and Two Types of Vulnerabilities

Self-efficacy focuses on what people believe they can accomplish. Many studies (e.g., Pajares and Graham 1999) have found that self-efficacy is a stronger predictor of subsequent performance than other motivation constructs. Self-efficacy is an optimistic sense of individual competence that increases personal effort in order to promote accomplishment under challenging circumstances. In turn, subsequent performance will be achieved. An individual who believes in his or her capability to produce a desired outcome can lead a more positive sense of control over a challenging environment. General self-efficacy is distinguished from domain-specific self-efficacy. For example, as a domain-specific self-efficacy, computer self-efficacy (CSE) has been defined as an individual judgment of one's capability to use a computer (Compeau and Higgins 1995; Davis et al. 1989; Gist et al. 1989). The IS literature further distinguishes two levels of CSE: general and task-specific CSE. General CSE refers to an individual's overall confidence in his or her ability to use computers, while task-specific CSE refers to one's confidence toward specific IS tasks (Marakas et al. 2007; Marakas et al. 1998).

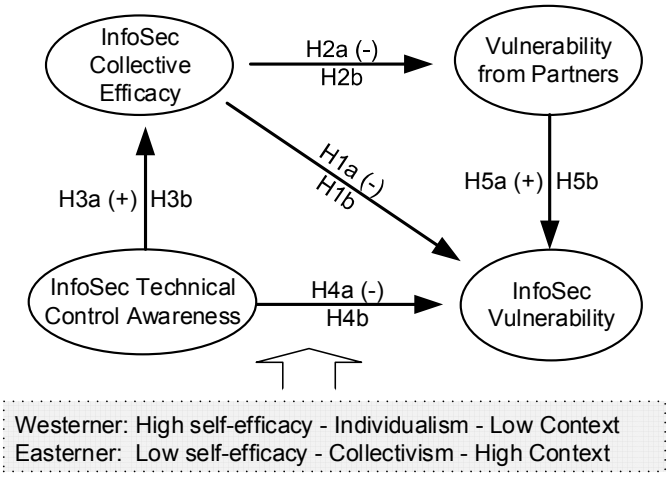


Figure 1. A Research Model and Hypotheses

In the few information security literature studies dealing with employees' compliance self-efficacy has been handled as an employee's judgment of personal skills and competency in obeying information security policies (Bulgurcu et al. 2010). Despite the large volume of self-efficacy studies dedicated to research in IS or IT and behavioral sciences (e.g., Agarwal and Karahanna 2000; Compeau and Higgins 1995; Marakas et al. 1998; Venkatesh and Davis 1996), little is known of self-efficacy's applicability at the group level. In the context of information security we define *InfoSec collective efficacy* as a group's shared belief in their controllability or capabilities to take courses of action to protect their valuable assets from security vulnerability. In this study since we are specifically interested in InfoSec collective efficacy from a IS or IT executive managers' perspective; we will measure InfoSec collective efficacy from IS or IT executive managers across different cultural settings.

Previous studies have further shown a strong link between collective efficacy and group performance (Gibson 1999; Gist and Mitchell 1992; Peterson et al. 1996; Peterson et al. 2000; Silver and Bufanio 1996; Stajkovic and Luthans 1998). A number of studies (Hsiu-Fen 2006; Kwon et al. 2007; Rhee et al. 2009; Scholz et al. 2002; Staples et al. 1999) have supported the strong negative relationship between self-efficacy and risk perception such that individuals with higher self-efficacy are more likely to perceive less risk. This would also be true at the group level. In the context of information security it is therefore reasonable to expect that the higher the degree of InfoSec collective efficacy perceived by executive managers, the lower the degree of InfoSec vulnerability will be expected in both countries. This is because higher levels of group efficacy reduce negative outcomes and in turn lead to positive performance (e.g., successfully operating groups' operational plans, and achieving group standards and goals).

The information security risks and vulnerabilities faced by any individual, business firm, or country depend not only on their choices but also on those of all other closely interdependent partners. In the case of network security it is generally true that once malicious programs such as viruses and worms reach one network, the remaining computer networks connected to the infected one can be easily compromised. This *interdependent security* concept was introduced by Kunreuther and Heal (2003) to find Nash equilibrium for a wide range of cost and risk parameters related to partners (Kunreuther and Heal 2004). Similar to InfoSec vulnerability, the perception of vulnerability from partners would be moderated with a higher level of self-efficacy. When executive managers perceive a higher level of their firms' capabilities to control InfoSec vulnerability, their perceptions of vulnerability from partners would be likely low in both countries. We therefore propose the following hypotheses:

H1a: InfoSec collective efficacy is negatively associated with InfoSec vulnerability across both countries.

H2a: InfoSec collective efficacy is negatively associated with InfoSec vulnerability from partners across both countries.

Extensive comparisons of self-efficacy from a cross-cultural perspective have been conducted in prior

research (Cheung and Sun 1999; Klassen 2004; Scholz et al. 2002; Schwarzer et al. 1997; Schwarzer et al. 1999). Focusing on general self-efficacy, Scholz, Dona, Sud, and Schwarzer (2002) confirmed that perceived self-efficacy is a unidimensional and universal construct across cultures. Their study showed that the psychometric properties of this universal construct would be useful for detecting cultural differences. They examined the differences of self-efficacy scores between countries and gender using 19120 samples from 25 different countries. The results of their study show that Asian samples from collectivistic cultures reported lower self-efficacy beliefs than their non-Asian peers.

Studies (e.g., Klassen 2004) examining the effect of self-efficacy across cultures have found that efficacy beliefs operate differently in non-Western cultures than they do in Western cultures. The overall self-efficacy of Western cultural groups (e.g., American, Canadian, Western European, and Australian) is higher than that of Eastern cultural groups (e.g., South Korean, Chinese, and of other Asian countries). Based on the results of prior comparison studies, we expect that the effect of self-efficacy in a group setting is also effective in the context of information security. We also expect that the effect of InfoSec collective efficacy in Western culture of the U.S. is stronger than in Eastern culture in South Korea, due to differences in levels of efficacy beliefs. We therefore hypothesize:

H1b: The negative effect of InfoSec collective self-efficacy on InfoSec vulnerability is stronger in Western culture of the U.S. than in Eastern culture of South Korea.

H2b: The negative effect of InfoSec collective self-efficacy on InfoSec vulnerability from partners is stronger in Western culture of the U.S. than in Eastern culture of South Korea.

InfoSec Technical Control Awareness and InfoSec Collective Efficacy

Awareness refers to individuals' understanding and increased interest toward certain issues, and is viewed as one of the key components of consciousness-raising (Choi et al. 2008). The concept of awareness is broadly used in different disciplines with different terminologies such as security awareness (information systems), sexual awareness (psychology), social awareness (sociology), and disease awareness (medical science). In the information systems area InfoSec awareness has been recognized as the most important determinant of success in protecting information systems from security vulnerabilities and threats (Furnell et al. 2002; Hawkins et al. 2000; Hu and Dinev 2005; McLean 1992; Morwood 1998; Siponen 2000; Siponen 2001; Siponen and Kajava 1998; Spurling 1995; Straub 1990; Straub and Welke 1998).

Understanding security threats and vulnerabilities is crucial to protecting system resources and valuable business assets. By staying aware of the current state of technologies as vulnerability control mechanisms people are able to develop skills and knowledge to perform their jobs more securely. Executive-level managers' awareness of information security in particular is a significant factor in an organization's information security performance (Cline and Jensen 2004). In this study, as a domain-specific awareness, *InfoSec technical control awareness* refers to an executive manager's belief in the availability of technological means and solutions to control security threats and vulnerability. The involvement and support of executive-level managers is critical and their role in this effort cannot be overstated for any successful organization-wide effort in InfoSec implementation. When executive managers have higher levels of understanding on the current state of vulnerability control technologies it is expected that they will implement their knowledge within the firm in order to prevent undesired outcomes. This in turn can lead a more positive sense of control over a challenging environment at the group level (i.e., a higher degree of InfoSec collective efficacy). In addition, when this knowledge is affiliated with InfoSec vulnerability, executives will drive their firm to ensure it has capability to manage the proper level of information systems risk and vulnerability through control mechanisms. We therefore posit that:

H3a: Executive-level managers' awareness of InfoSec technical control is positively associated with InfoSec collective self-efficacy across both countries.

H4a: Executive-level managers' awareness of InfoSec technical control is negatively associated with InfoSec Vulnerability across both countries.

In today's network environment business firms and individuals are linked either physically or logically; information security threats and vulnerabilities are therefore in interdependent. The vulnerabilities faced by a firm depend on both its own security strategies and those of its partners. A theoretical support for the

interdependency of information security can be found in the literature on *interdependent security* (Kunreuther and Heal 2004).

Since information security risks are intricately interrelated, a firm's InfoSec vulnerability is at least partially dependent on the vulnerabilities of its partner firms. It would therefore be a logical expectation that the higher level of vulnerability from partners is perceived, the greater the degree of vulnerability perception will be associated with information security. This expectation would be valid across different cultures. Based on the arguments above we propose that:

H5a: Vulnerability from partners has a strong positive effect on InfoSec vulnerability across both countries.

Unlike the case of the cross-cultural effect of self-efficacy in both individual and group settings, we cannot find any evidences and/or arguments that support cross-cultural effects for an executive-level manager's awareness and vulnerability from partners. We therefore argue that:

H3b: There is no significant difference in the effect of executive-level manager's awareness on InfoSec control between two countries.

H4b: There is no significant difference in the effect of executive-level manager's awareness on InfoSec vulnerability between two countries.

H5b: There is no significant difference in the effect of vulnerability from partner on InfoSec vulnerability between two countries.

Research Methodology and Data Collection

In order to validate the proposed research model from a cross-cultural perspective we collected survey data in two countries, the U.S. for Western culture and South Korea for Eastern culture. In addition to the fact that they belong to the Western and the Eastern cultures respectively, we have another resilient reason to choose these two countries. Both countries are known to have extensive IT infrastructures that significantly affect their economies. The IT sector's output in year 2010 occupied 4.6% and 11.0% of the gross domestic product (GDP) in the U.S. (source: U.S. Department of Commerce, Bureau of Economic Analysis) and South Korea (source: Bank of Korea) respectively. Further, the use of IT in non-IT sectors has grown significantly in these countries during the past decades. Information security is therefore a major issue for overall risk management in these two countries.

The English version of the survey questionnaire was developed first. Focusing on the domain of information security control and vulnerability, the survey items measuring InfoSec collective efficacy, InfoSec technical control awareness, perceived vulnerability, and vulnerability from others were initially developed based on previous literature (Armitage et al. 1999; Gibson 1999; Goodhue and Straub 1991; Skinner 1995; Straub 1990), published security survey reports (DTI 2004; Ernst&Young 2008), and interviews with two information security professionals: chief security officers of a for-profit firm and a non-profit organization respectively. A professional business writer corrected and improved the phrasing of the survey questionnaire. A group of 48 IT professionals and graduate students reviewed the questionnaire to verify whether or not the wordings of items we are accurate and correctly measured the intended constructs. As the result of the item-construct-validity test any ambiguous or misrepresenting items were removed. Two-round pilot tests were conducted. The first pilot test was conducted with two information security professionals who are security officers of for-profit firms. A group of 27 graduate students majoring in Information Systems (IS) participated in the second pilot test. We used these two-round pilot tests in order to ensure the reliability of the scales and general mechanics of the survey questionnaire, including the appropriateness of instructions and completion time. Based on the pilot test results the survey questionnaire was further streamlined and finalized. All measurement items are shown in Appendix 1.

We obtained the Korean version of the survey questionnaire using multi-stage translation process. First, the English version was translated into a Korean version by a professional English-Korean translator. The wordings of ambiguous and misrepresenting items were corrected. Then the Korean version of the questionnaire was translated back into an English version by another professional Korean-English translator. The translated English version's item-construct validity was tested by a group of graduate

students. Ambiguous and misrepresenting items' Korean wordings were improved and translated into English again for an additional round of item-validity testing. The Korean version of the survey questionnaire was finalized when both the Korean version's and re-translated English version's item-construct validity was successfully tested.

Since this study specifically focuses on InfoSec collective efficacy and InfoSec technical control awareness from information security managers' perspective, it is appropriate to collect information security managers' perceived InfoSec collective efficacy and perceived InfoSec technical control awareness through survey questionnaires completed by IT or IS executives (i.e., managers with the title of chief information officer, IT director, or similar).

For data collection purposes, we selected IS executives from 2027 organizations in the U.S. and 320 organizations in South Korea. In order to encourage subjects' participation and improve the response rate in the US, we carried out two rounds of survey-questionnaire mailings over a period of six weeks and post-card reminders between the two rounds. In South Korea we mailed the survey questionnaire once followed by both email and phone call encouragement. A total of 222 and 83 survey responses in the U.S. and South Korea were received respectively. Out of the U.S. survey responses 46 were dropped due to missing data points or multiple answers for the same item. The organizations of responding IS executives included companies and institutes from various for-profit and non-profit sectors such as manufacturing, banking, transportation, retail, healthcare, various other service sectors, education, and government. The average annual revenues of the U.S. and South Korean organizations were approximately $135 million U.S. dollars and $17.5 million U.S. dollars respectively.

Model Testing and Result

The structural equation modeling (SEM) approach was used to analyze the data for both the measurement and structural models. Compare to a conventional regression analysis that ignores the interrelationships between latent constructs measured by multiple measurement items (Bollen1989; Chin1998), SEM is a statistical methodology that takes a confirmatory (i.e., hypothesis-testing) approach toward the analysis of causal relationships among latent constructs (i.e., a structural theory) (Byrne 2001). There are two families of SEM techniques: covariance-based techniques (e.g., AMOS) and variance-based techniques (e.g., smart PLS). In this study we used both AMOS 19.0 (build 1375) and Partial Least Squares (SmartPLS version 2.0.M3) to test the measurement and structural models because SmartPLS and AMOS can be regarded as complementary. SmartPLS reports the composite reliability (CR) and average variance extracted (AVE) for content validity and discriminant validity. Based on covariance analysis, similar to LISREL AMOS is more confirmatory in nature and it provides various overall goodness-of-fit indices assessing model fit for convergent validity (Byrne 2001). Furthermore, AMOS and SmartPLS allow multiple group analysis.

Testing the Measurement Model

We ensured the psychometric properties of the instrument by testing the reliability and validity of the measurement model before the structural model testing. Since all constructs in this study are reflective the assessment of the measurement model includes the estimation of internal consistency for reliability, convergent validity, and discriminant validity (Chin and Gopal 1995). The internal consistency of the measurement models was tested by examining the Cronbach's alpha and Fornell's composite reliability (Fornell and Larcker 1981). Table 3 shows the summarized reliability indices. The values of the Cronbach reliability coefficients range from 0.745 to 0.957, which are higher than the minimum cutoff score of 0.70 (Nunnally 1978; Nunnally and Bernstein 1994). Composite reliability should be greater than the benchmark of 0.7 to be considered adequate (Fornell and Larcker 1981). The lowest composite reliability is 0.861, which is a value higher than 0.7 indicating adequate internal consistency.

Convergent validity is assessed using two methods: factor loading of each item on its corresponding construct and the average variance extracted (AVE) for each construct. We assessed the factor loading of each item of the corresponding construct (Bollen 1989) by conducting CFAs using AMOS 19.0. Figures 2 and 3 show the results of the CFAs for the U.S. and Korea models respectively. By examining the inter-construct correlations we can assess whether or not the constructs are too highly correlated. According to

the results of two CFAs, the lambda coefficients of each item are higher than the minimum recommended cutoff score of 0.60 (Bagozzi and Yi 1988) except for one item (i.e., VU1 has 0.59) in the U.S. model. However, this item is very close to the cutoff score, and the *t*-statistic for each path is significant at the 0.05 level (Gefen et al. 2000), and each path loading is greater than twice its standard error (0.043-0.188 for the U.S. sample and 0.037-0.125 for South Korean sample) (Anderson and Gerbing 1988). We also examine the AVE for each construct across the models. All AVE values are higher than the 0.5 threshold suggested by Forell and Larcker (1981).

Table 3. Reliability, Correlation, and Discriminant Validity of Constructs (US Data)

(US Data)							
Constructs	Alpha	CR	AVE	1	2	3	4
InfoSec Control Awareness	.757	0.861	0.675	**0.822**			
InfoSec Collective Efficacy	.888	0.940	0.759	0.370	**0.871**		
Vulnerability from Partners	.934	0.967	0.907	-0.114	-0.273	**0.952**	
InfoSec Vulnerability	.745	0.910	0.719	-0.274	-0.670	0.516	**0.848**
(South Korea Data)							
Constructs	Alpha	CR	AVE	1	2	3	4
InfoSec Control Awareness	0.939	0.960	0.890	**0.943**			
InfoSec Collective Efficacy	0.935	0.951	0.796	0.350	**0.892**		
Vulnerability from Partners	0.957	0.972	0.921	-0.162	-0.161	**0.960**	
InfoSec Vulnerability	0.851	0.898	0.690	-0.079	0.019	0.378	**0.831**

Note: (1) *N* = 176 (US) and 83 (South Korea). (2) CR: Composite Reliability, AVE: Average Variance Extracted. (3) Diagonal elements are the square root of AVE. These values should exceed the off-diagonal inter-construct correlations for adequate discriminant validity.

The AVE can also be used for evaluating discriminant validity. In order to satisfy discriminant validity, the square roots of AVE for the construct should be higher than the variance shared between the focal construct and other constructs in the model (Fornell and Larcker 1981). As shown in Table 3, in all cases the correlations between each pair of constructs are lower than the square root of the AVE for the relevant constructs across two data sets.

Overall, all constructs of the research models demonstrate acceptable internal consistency for reliability, convergent validity, and discriminant validity in terms of the suggested criteria perspectives.

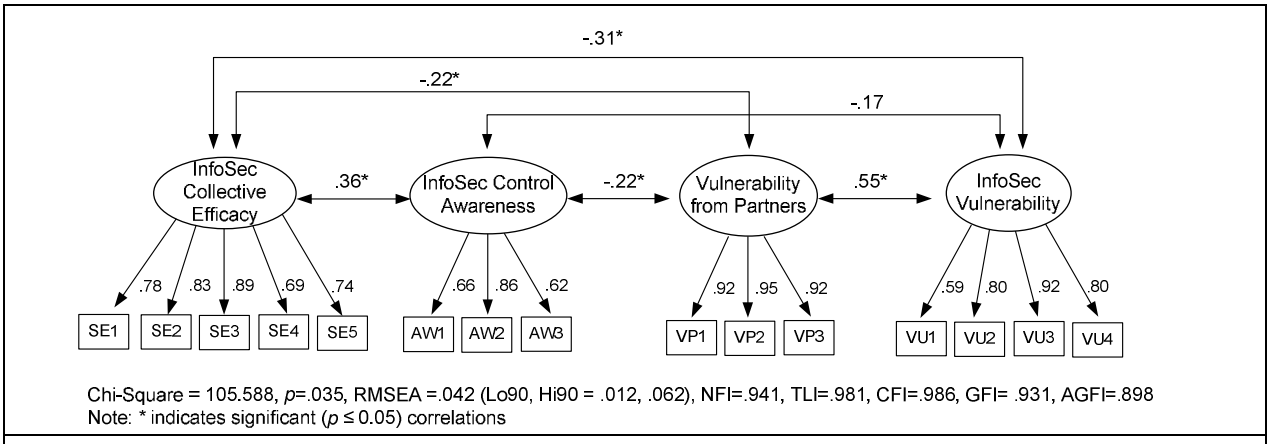


Figure 2: Results of Confirmatory Factor Analysis (US data)

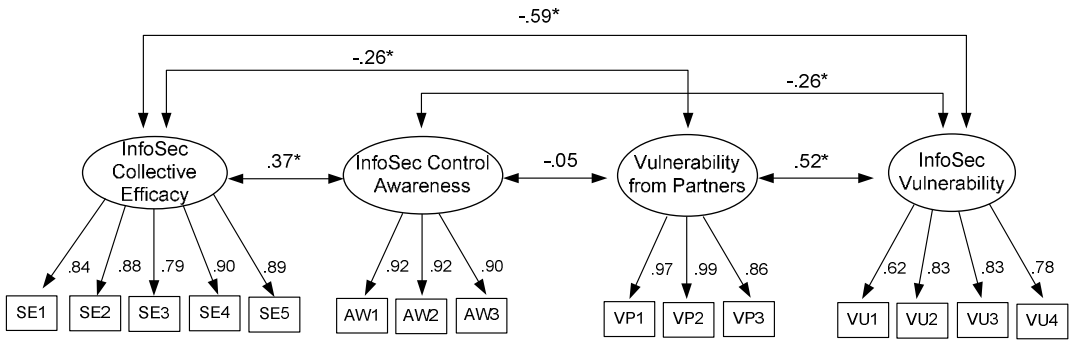


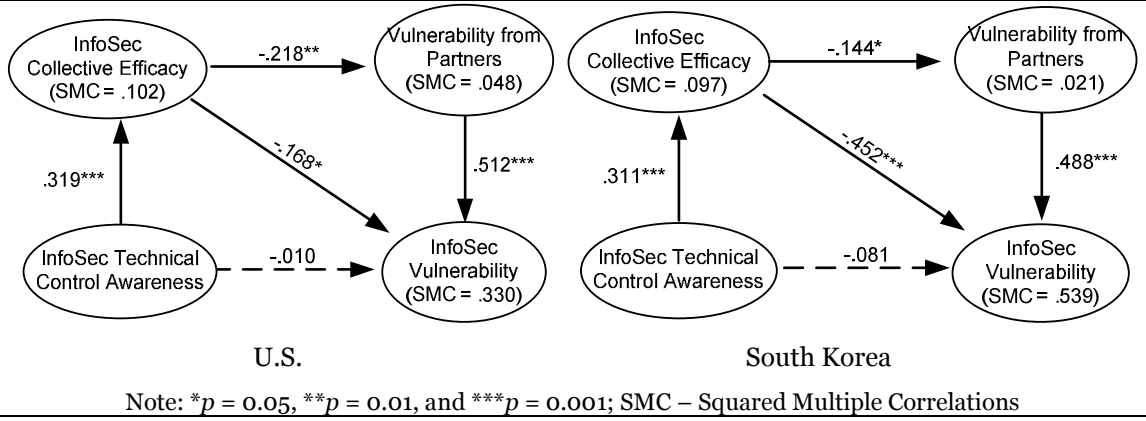
Figure 3: Results of Confirmatory Factor Analysis (South Korea data)

Testing the Structural Model Using Multi-group Analysis

The major goal of the study is to examine the impact of InfoSec collective efficacy on InfoSec vulnerability across two different cultural groups. When the same measurement items are applicable to multiple groups (i.e., the U.S. and South Korea) multi-group analysis is a very powerful method to determine whether or not a grouping construct (e.g., gender, culture) affects a research model (Byrne 2001). A multi-group SEM analysis is used for comparing the path coefficients of the structural model. We conducted the three general phases of multi-group analysis discussed in Kim (2008): 1) finding a baseline model representing a reasonably well-fitting model from the perspectives of both parsimony and substantive meaningfulness (Byrne 2001), 2) testing the pattern of factor loadings for the baseline (Although showing the number of factors must be equivalent across groups is not a necessary condition, it is a logical starting point before structure testing (Byrne 2001)), and 3) testing the equivalence of the hypothesized structural path of the structural models using AMOS 19.0 multi-group analysis with two structural models (one for the U.S. and the other for South Korea).

First, separate single-group analyses for the testing of the U.S. and Korea measurement models were conducted using AMOS. For comparison, Figure 4 and Table 4 summarize the results of the structure model testing for each group. The standardized path coefficients and squared multiple correlations of dependent constructs shows the model fit indices of both models with suggested values. The overall fit of both models is acceptable in terms of suggested values: RMSEA, NFI, TLI, CFI, GFI, and AGFI. Nearly 33 and 54 percent of the variance in InfoSec vulnerability for the U.S. and Korea models respectively are explained by InfoSec collective efficacy, vulnerability from partners, and executive manager's InfoSec technical control awareness in the model.

By comparing the results of the separated single-group analysis we can test the first part of the proposed hypotheses (i.e., H1a, H2a, ..., and H5a). As anticipated, the causal paths from InfoSec collective efficacy to InfoSec vulnerability (β_{USA} = -.168, p < 0.05; β_{Korea} = -.452, p < 0.001) are highly significant at the 0.05 level for both the U.S. and Korea models. This result supports H1a. The causal relationships between InfoSec collective efficacy and vulnerability from partners (β_{USA} = -.218, p < 0.01; β_{Korea} = -.144, p < 0.05) also show statistically significant results in both the U.S. and Korea models; H2a is therefore supported. Consistent with the results of self-efficacy studies in cross-culture settings, according to these results InfoSec collective efficacy has a universal effect across cultures. Executive-level managers' InfoSec technical control awareness has a strong positive effect on InfoSec collective efficacy (β_{USA} = -.319, p < 0.001; β_{Korea} = -.311, p < 0.001) across the data sets of two countries, thereby supporting H3a. However, against our expectation, executive-level managers' awareness is not found to have a significant effect on InfoSec vulnerability (β_{USA} = -.010, p > 0.05; β_{Korea} = -.081, p > 0.05) in both countries. H4a is therefore not supported by the data sets of both countries. As expected, vulnerability from partners has a statistically strong positive effect on InfoSec vulnerability (β_{USA} = .512, p < 0.001; β_{Korea} = .488, p < 0.001) in both groups, supporting H5a.



Note: *p = 0.05, **p = 0.01, and ***p = 0.001; SMC – Squared Multiple Correlations

Figure 4: U.S. versus Korea model

Table 4. Model Fit Indices

Statistic	Suggested Value	U.S. (N = 176)	Korea (N = 83)
Chi-Square (χ2)		129.624	94.793
df		84	79
Chi-Square Significance	$p \leq .05$	0.001*	0.019*
Chi-Square/*df*	< 5.0	1.543*	1.200*
RMSEA	≤ 0.06 (Hu and Bentler 1999)	.056*	.049*
NFI	> 0.90 (Kelloway 1998; Kline 1998)	.928*	.926*
TLI	≥ 0.96 (Hu and Bentle 1999)	.966*	.982*
CFI	≥ 0.90 (Bentler 1990)	.973*	.987*
GFI	> 0.80 (Joreskog and Sorbom 1988)	.918*	.873*
AGFI	> 0.80 (Joreskog and Sorbom1988)	.883*	.807*

Note: * satisfies the suggested value.

Based on the results of the single-group analyses we find that there is no evidence to reject the measurement model, and the U.S. model can be used as a baseline because it shows a reasonably well-fitting model. Using the baseline model we moved to the next phases of multi-group analysis (i.e., testing the group invariance of factor loadings and testing the hypothesized structural path). For the factor loading invariance testing we conducted AMOS multi-group analysis by running two separate groups within a single analysis. Table 5 summarizes the results of the multi-group analysis.

According to the results, compared to Model 1 (unconstrained model) Model 2 (factor loadings constrained equal model) shows statistically insignificant p-values at the 0.05 probability level and all factor loadings are invariant across the groups. The models of both groups are therefore not significantly different at the measurement model level. Having established a baseline model and the equality of measurement between both groups, we can now move to the next step of testing for the equivalence of the model's structural path across both groups. By examining the equivalence of the structural paths for both groups we can test the second part of our proposed hypotheses for the research model (i.e., H1b, H2b, …, and H5b).

Before testing for the invariance of each structural path we tested the invariance of all hypothesized structural paths. The comparison between Model 3 (factor loadings and all structural paths constrained equal) and Model 2 yields a statistical significant at the 0.05 level, signaling some inequality in the structural paths between the U.S. and Korea models. Given this evidence of inequality we then tested the equivalent of each structural path individually in order to determine the nonequivalent regression paths. According to the results of structural path invariance tests between two groups summarized in Table 5, compared to the Model 2 (factor loadings constrained equal) Model 4 shows a $\Delta\chi^2$ value of 12.82 with 1 degree of freedom and a p-value less than 0.001. This comparison shows that the structural path between InfoSec collective efficacy and InfoSec vulnerability is different across the two groups. Although we can see the inequality of the structural path between groups, this result does not indicate whether it is positive

or negative in this test. However, because the path coefficient between InfoSec collective self-efficacy to vulnerability in the Korea model is more highly significant than that in the U.S. model in Figure 4, we can conclude that the negative effect of InfoSec collective efficacy on InfoSec vulnerability is stronger in South Korea than in the U.S. Against our expectation H1b is not supported; the result is in fact opposite. The result of Model 5 indicates that the effect of InfoSec collective efficacy on vulnerability from partners across the U.S. and South Korean sample is invariant because the *p*-value is not significant at the 0.05 probability level. H2b is therefore not supported. As reported in Table 5, all the remaining series of test results showed that the proposed structural paths in the models were not different across the groups. We can therefore conclude that there are no differences in the effects of InfoSec managers' technical control awareness and InfoSec vulnerability from partners on the models across the two groups.

Table 5: Goodness-of-Fit Statistics of Structural Paths across U.S. and Korea models

Model # : Model Description	$\chi 2$	*df*	$\Delta\chi 2$	Δdf	*p*-value	Meaning
1: Unconstrained Model	329.50	165	-	-	-	-
2: Factor Loadings Constrained Equal	351.08	180	21.58	15	0.119	Groups are not different at the measurement model level. They may be different at the path level.
3: Factor Loadings and All Structural Paths Constrained Equal	370.59	185	19.51	5	.002*	Inequality in the structural paths across both groups; must check path differences.
4: Model 2 with Structural Path InfoSec Collective Efficacy →InfoSec Vulnerability Constrained Equal	363.90	181	12.82	1	.000*	The structural path is different. It should be checked whether it is positive or negative variant to confirm H1a. The path coefficient in the Korea model is stronger than that in the U.S. model.
5: Model 2 with Structural Path InfoSec Collective Efficacy →Vulnerability from Partners Constrained Equal	352.97	181	1.90	1	.168	The path is invariant. H2b is not supported
6: Model 5 with Structural Path InfoSec Technical Control Awareness →InfoSec Collective Efficacy Constrained Equal	353.10	182	2.02	2	.364	The path is invariant. H3b is supported
7: Model 6 with Structural Path InfoSec Technical Control Awareness →InfoSec Vulnerability Constrained Equal	353.22	183	2.14	3	.544	The path is invariant. H4b is supported
8: Model 7 with Structural Path Vulnerability from Partners → InfoSec Vulnerability Constrained Equal	355.15	184	4.07	4	.396	The path is invariant. H5b is supported

Note: $\Delta\chi 2$ – difference in $\chi 2$ values between models; Δdf – difference in number of degrees of freedom between models; * - significant at $p < 0.05$.

Discussion and Conclusion

This study has *several key findings*. First, as we proposed InfoSec collective efficacy negatively influences InfoSec vulnerability and vulnerability from partners across both Western culture in the U.S. and Eastern culture in South Korea. A higher level of managers' InfoSec technical control awareness positively prompts the level of InfoSec collective efficacy across both cultures. Second, consistent with the theory of interdependent security we found that information security vulnerability is not an independent issue across these cultures. When managers in both cultures perceive a higher level of InfoSec vulnerability from partner networked systems, the level of InfoSec vulnerability of their firms significantly increases. This empirical result shows that information security is a culturally neutral global issue that is interdependent with partners in a networked systems environment.

Against our expectations, the negative effect of InfoSec collective efficacy for the U.S. group (i.e., Western culture group) on perceived vulnerability was not stronger than that for the South Korea group (i.e., Eastern culture group). More interestingly, the negative effect of InfoSec collective efficacy on InfoSec vulnerability was significantly stronger in South Korea than in the US, which is opposite from the proposed hypothesis H1a. Although InfoSec collective efficacy is an important factor controlling perceived vulnerability in both culturally different groups, it plays a stronger role in South Korea. This unexpected result can be interpreted from the cross-cultural perspective of individualism or collectivism and low context or high context in Western and Eastern groups respectively. As Bandura discussed (Bandura 2000), collective efficacy is not a simple sum of individual's efficacies. Although many studies report a lower level of self-efficacy in Eastern culture groups, this does not mean that members of Eastern culture groups (i.e., South Korean group) share a lower level of collective efficacy beliefs. As the meaning of collective explains, it is a shared belief in the group's communal power that can be achieved through interdependent efforts among group members. As previous cross-cultural studies (Goddard et al. 2004; Hodges and Carron 1992; Lichacz and Partington 1996; Little and Madigan 1997; Sampson et al. 1997) have reported, members of Eastern cultural groups have interdependent views of self; they are deeply involved with each other; the goals, needs, and values of individuals are less important than those of collectives; and decisions are strongly influenced by group norms. The stronger effect of InfoSec collective efficacy on InfoSec vulnerability in South Korea is probably a valid result from the cross-cultural perspective due to these group dynamics and synergetic interdependent efforts in Eastern cultures in South Korea.

We also can interpret this unforeseen result from the theoretical lenses of theory of IT-culture conflicts proposed by Leidner and Kayworth (2006). According to this theory, communication and information technology (IT) changes culture over time as the types of IT-cultural conflicts arise and are resolved. Encounters between new technologies and cultures often lead to nascent use of technologies as well as cultural transformations (Madon 1992). The case of South Korea with the world's fifth largest Internet market and the highest Internet penetration in the world (ITU 2003) presents a unique and advanced IT-cultural environment. The South Korean government has continually expressed its intentions to centralize policy coordination, and has invested in the IT industry based on the view that IT will help the South Korean economy as a driving force of economic growth. It provided a master plan to guide organizations and citizens in how to use IT in dealing with new social and economic demands as well as carry out nationwide innovation in order to become the world's leading country in terms of IT (NCA 2006). Based on the advanced IT infrastructure and continued efforts toward shaping the nation's IT direction, South Korea's IT-based innovative businesses are a major growth engine of the national economy based on technological competitiveness and growth potentials (Lallana 2004). As a result, South Korea was ranked first in the deployment of nationwide broadband Internet and its rate of adoption far exceeds that of other developed countries even beyond the U.S. (ITU 2005; OECD 2004). We can recognize that subtle changes in culture may occur gradually, such as IT used in South Korea to strategically and innovatively support both individual and organizational needs. In light of this theory and the advanced IT-cultural environment, South Korea may experience significant changes at the individual, organizational, and national levels in terms of cultural transformation. Its current IT culture may accordingly be significantly different from reported in previous cross-cultural studies on South Korean cultural values.

Another possible interpretation of this result is that there is relatively different emphasis found in the U.S. and South Korea in terms of security practices. While greater emphasis is placed on post-breach remedies (e.g., information security insurance, emergent customer liability restrictions, intrusion handling policies, etc.) in the US, firms in South Korea invest in and emphasize relatively preventive technical measures (e.g., multi-layer security access controls, safeguard computing facility, etc.). For instance, in order to remotely access a bank account' users in South Korea must go through several steps of security clearance processes including the traditional password, public or governmental certification, a personalized table of random numbers, and a safeguarded computing facility such as a section key lock or virus scanner. On the other hand, information security insurance is a popular product in the U.S. but not in South Korea; this reduces the impact of security breaches for firms. The effect of InfoSec collective efficacy on InfoSec vulnerability may therefore be relatively weaker in the U.S. than in South Korea. Further investigation is required to validate this proposition.

Another finding of the study is that the InfoSec technical control awareness does show a significant positive effect on perceived vulnerability across both cultures. This result demonstrates that simply

understanding and knowledge of the availability of technological means and solutions to control security vulnerabilities do not diminish InfoSec vulnerability in either both groups. The role of InfoSec technical control awareness toward vulnerability may be boosting the level of InfoSec collective efficacy, and in turn dropping the level of vulnerability regardless of culture.

This study has several limitations that should be considered in future investigations. First, this study uses IS executive managers' perceptions of InfoSec collective efficacy. We measured of collective efficacy from executive managers' viewpoints as reflecting the collective efficacy of the firm at the organization level, rather than from other employees' viewpoints, because IS executive managers are better informed regarding the level of control at the organizational level than any other individuals. However, it is certainly a limitation of a group-level study.

Second, this study also uses managers' perceived vulnerability perceptions as a proxy for organizational-level InfoSec future vulnerability because of the nature of limited public access to internal reports of information security vulnerabilities and breaches. We believe that there are other ways to directly measure a firm's information security vulnerability (e.g., the frequency of breaches during a given time period). Future studies should therefore examine the effect of InfoSec collective efficacy on actual information security vulnerabilities, providing a better clarification of the role of InfoSec collective efficacy on vulnerability.

Third, our sample from two countries limits our study to comparison between two countries because South Korea and the U.S. may not be a representative of Eastern and Western culture. Extension of our samples that represent the particular cultural traits can be promising for the future research.

Fourth, in this study, the sample size (83 survey responses) for the South Korea is rather small while that for the U.S. is large enough. This can be considered not enough for AMOS-based SEM analysis.

Fifth, our investigation is not on the basis of firm-level characteristics. In particular, firm size, portion of the IS/IT spending, and/or industrial traits can be the factors which form the firms' attitude toward perceived risk or policy decision on Information Security.

Finally, this study only focuses on few limited factors that affect information security vulnerability. There are other cognitive and non-cognitive factors (e.g., previous security incidents and information security needs) that affect an organization's formation of the collective efficacy or information security vulnerability. Further studies examining the effect of other factors such as past experience with information security breaches, network dependency, needs for information security, and other factors for the perceived vulnerability will enhance the explanatory power of the model and provide more complete insights.

This study has several unique theoretical and practical contributions. First, from a theoretical perspective this study extends the concept of self-efficacy into a new domain-specific group-level construct (i.e., *InfoSec collective efficacy*). Since research on the effect of collective efficacy in the context of information security is very limited, we hope this study ignites a fire on this less explored area. Second, this study proposes two separated concepts of vulnerability in an organization setting drawing the theory of interdependent security and empirically tests their relationships: vulnerability from the organization itself and vulnerability from partner organizations. Since limited empirical investigations have been made on this relationship, this is another unique contribution. We expect that the result of this strong positive effect of vulnerability from partner organizations on the vulnerability of the organization itself will provide additional clear empirical evidence.

Third, along with executive manager's awareness of InfoSec technical controls, this study considers *InfoSec collective efficacy* as a cultural construct and juxtaposes its effects on InfoSec vulnerability from a cross-cultural perspective. The findings and interpretations of the study provide some theoretical insights into the perspectives of South Korea group (i.e., Eastern tradition) versus the U.S. group (i.e., Western traditions). For example, in contrast to the general results of prior cultural comparison studies on self-efficacy, the present study shows that the effect of InfoSec collective efficacy in South Korea is stronger than in the U.S. This study provides several different interpretations on this unpredicted result from three different angles: the cross-cultural perspective, the theory of IT-cultural conflict, and different security practices. We believe the findings and interpretations of this study improve our understating of the role of collective efficacy, particularly in the domain of information security. This will contribute to the

theoretical depth and breadth of the self-efficacy literature.

From a practical standpoint this study provides important insights for IT managers operating in multinational business settings. Since we collected data from executive-level information systems managers, the results of the study directly benefit them in understating current information systems security issues. In light of this study's findings, it is crucial for executive-level managers to enhance their understanding and knowledge of emerging technological solutions along with means to manage their information security vulnerabilities, since their awareness of InfoSec technical control is an important factor forming InfoSec collective efficacy. Previous studies (Goodhue and Straub 1991; Loch et al. 1992; Straub and Welke 1998) have also raised the importance of understanding managers' perceptions concerning the information security since coping with information security risk requires significant managerial vigilance; an appropriate level of concern may be a prerequisite for adequate security protection.

However, simply enriching managers' knowledge is not the goal in directly controlling vulnerability. As the results of the study suggest, higher InfoSec collective efficacy moderates security vulnerability. In order to increase the level of InfoSec collective efficacy a security education, training, and awareness (SETA) program is the solution. The SETA program is the responsibility of IT managers and is designed to supplement the general security education and training that many organizations use to educate their employees on information security, improve capability to combat information security threats, and remediate their vulnerabilities. The goal of a SETA program is to enhance information security by improving employees' awareness of the need to protect system resources, developing their skills and knowledge to perform their jobs more securely, and building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems (NIST 1995). An effective SETA program allows business organizations to improve the levels of InfoSec collective efficacy.

The results of the study also indicate that different strategies may apply for information security project and control management because the effect of InfoSec collective effect on InfoSec vulnerability is significantly stronger in South Korean group (i.e., Eastern culture). Managers in this cultural group may plan and assign more team-based security projects and tasks for their employees since group dynamics and synergetic interdependent work show higher performance in Eastern cultural groups.

As a final remark, most IT-cultural studies define culture as being relatively stable and difficult to change. Leidner and Kayworth (2006) discussed how the empirical IT-cultural literature has primarily examined the one-way impact that cultural values have on IT outcomes. Only few studies consider the other direction for the impact that IT can have on culture. It would be true that IT alters the character of our symbols, the things we think about, the things we think with, the nature of community, and even the structure of our lives. IT has a role to play in facilitating both individual and organizational value changes, and ultimately national-level culture changes. We should accordingly change our view of culture based on more dynamic reciprocal relationships between IT and culture in line with IT evolutions.

Reference

Agarwal, R., and Karahanna, E. 2000. "Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage," *MIS Quarterly* (24:4) Dec, pp. 665-694.

Allen, F., and Gale, D. 2000. "Financial Contagion," *Journal of Political Economy* (108:1), pp. 1-33.

Anderson, J. C., and Gerbing, D. W. 1988. "Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach," *Psychological Bulletin* (103:3), pp. 411-423.

Armitage, C. J., Conner, M., Loach, J., and Willetts, D. 1999. "Different Perceptions of Control: Applying an Extended Theory of Planned Behavior to Legal and Illegal Drug Use," *Basic and Applied Social Psychology* (21:4), pp. 301-316.

Bagozzi, R. P., and Yi, Y. 1988. "On the Evaluation of Structural Equation Models," *Journal of the Academy of Marketing Science* (16:1), pp. 74-94.

Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review* (84:2), pp. 191-215.

Bandura, A. 1982. "Self-Efficacy Mechanism in Human Agency," *American Psychologist* (37:2), pp. 122-147.
Bandura, A. 1986. "The Explanatory and Predictive Scope of Self-Efficacy Theory," *Journal of Social and Clinical Psychology* (4:3), pp. 359-373.
Bandura, A. 1989. "Human Agency in Social Cognitive Theory," *American Psychologist* (44:9), pp. 1175-1184.
Bandura, A. 1995. *Self-Efficacy in Changing Societies*, Cambridge Univ Press.
Bandura, A. 1997. *Self-Efficacy: The Exercise of Control*, New York: Freeman.
Bandura, A. 2000. "Exercise of Human Agency through Collective Efficacy," *Current Directions in Psychological Science* (9:3), pp. 75-78.
Bandura, A. 2002. "Social Cognitive Theory in Cultural Context," *Applied Psychology* (51:2), pp. 269-290.
Bandura, A., Barbaranelli, C., Caprara, G. V., and Pastorelli, C. 2001. "Self-Efficacy Beliefs as Shapers of Children's Sspirations and Career Trajectories," *Child Development* (72:1), pp. 187-206.
Baskerville, R. F. 2003. "Hofstede Never Studied Culture," *Accounting, Organizations and Society* (28:1), pp. 1-14.
Bentler, P. M. 1990. "Comparative Fit Indexes in Structural Models," *Psychological Bulletin* (107:2), pp. 238-246.
Bollen, K. A. 1989. *Structural Equations With Latent Variables*, Wiley: New York, NY.
Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.
Byrne, B. M. 2001. *Structural Equation Modeling With AMOS: Basic Concepts, Applications, and Programming*, Lawrence Erlbaum Associates: Mahwah, New Jersey.
Cheung, S. K., and Sun, S. Y. K. 1999. "Assessment of Optimistic Self-beliefs: Further Validation of the Chinese Version of the General Self-Efficacy Scale," *Psychological Reports* (85:3f), pp. 1221-1224.
Chin, W. W. 1998. "The Partial Least Squares Approach to Structural Equation Modeling," in *Modern Methods for Business Research,* G. A. Marcoulides (Ed.), Lawrence Erlbaum Associates: Mahwah, NJ, pp. 295-336.
Chin, W. W., and Gopal, A. 1995. "Adoption Intention in GSS: Relative Importance of Beliefs," *ACM SigMIS Database* (26:2-3), pp. 42-64.
Choi, N., Kim, D., Goo, J., and Whitmore, A. 2008. "Knowing Is Doing: An Empirical Validation of the Relationship Between Managerial Information Security Awareness and Action," *Information Management & Computer Security* (16:5), pp. 484-501.
Cline, M., and Jensen, B. K. Year. "Information Security: An Organizational Change Perspective," The Tenth Americas Conference on Information Systems 2004.
Compeau, D. R., and Higgins, C. A. 1995. "Computer Self-Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), pp. 189-211.
Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), pp. 982-1003.
Deloitte 2009. "Global Security Survey for the Technology, Media & Telecommunications (TMT) Industry ", Deloitte Touche Tohmatsu, U.S.
Dinev, T., and Hu, Q. 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention Toward Protective Information Technologies," *Journal of the Association for Information Systems* (8:7), pp. 386-408.
DTI 2004. "Information Security Breach Survey 2004," Department of Trade and Industry, U.K.
EIU 1998. "Managing Business Risks in the Information Age 1998," The Economist Intelligence Unit(EIU), New York.
Ernst & Young 2008. "Moving Beyond Compliance - Ernst & Young's 2008 Global Information Security Survey," Ernst & Young.
Fornell, C., and Larcker, D. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18), pp. 39-50.
Furnell, S. M., Gennatou, M., and Dowland, P. S. 2002. "A Prototype Tool for Information Security Awareness and Training," *Logistics Information Management* (15:5/6), pp. 352-357.
Gefen, D., Straub, D. W., and Boudreau, M.C. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the AIS* (4:7), pp. 1-78.

Gibson, C. B. 1999. "Do They Do What They Believe They Can? Group Efficacy and Group Effectiveness Across Tasks and Cultures," *Academy of Management Journal* (42:2), pp. 138-152.
Gist, M. E., and Mitchell, T. R. 1992. "Self-Efficacy: A Theoretical Analysis of its Determinants and Malleability," *Academy of Management Review* (17:2), pp. 183-211.
Gist, M. E., Schwoerer, C., and Rosen, B. 1989. "Effects of Alternative Training Methods on Self-Efficacy and Performance in Computer Software Training," *Journal of Applied Psychology* (74:6), pp. 884.
Goddard, R. D., Hoy, W. K., and Hoy, A. W. 2004. "Collective Efficacy Beliefs: Theoretical Developments, Empirical Evidence, and Future Directions," *Educational Researcher* (33:3), pp. 3-13.
Goodhue, D. L., and Straub, D. W. 1991. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security," *Information & Management* (20:1), pp. 13-27.
Hall, E. T., and Hall, M. R. 1990. *Understanding Cultural Differences*, Intercultural Press.
Hardin, A. M., Fuller, M. A., and Davison, R. M. 2007. "I Know I Can, But Can We? Culture and Efficacy Beliefs in Global Virtual Teams," *Small Group Research* (38:1), pp. 130-155.
Hawkins, S., Yen, D. C., and Chou, D. C. 2000. "Awareness and Challenges of Internet Security," *Information Management & Computer Security* (8:3), pp. 131-143.
Heal, G., and Kunreuther, H. 2004. "Interdependent Security: A General Model," National Bureau of Economic Research.
Hodges, L., and Carron, A. V. 1992. "Collective Efficacy and Group Performance," *International Journal of Sport Psychology; International Journal of Sport Psychology* (23:1), pp. 48-59.
Hofstede, G. 1980. "Motivation, Leadership, and Organization: Do American Theories Apply Abroad?," *Organizational Dynamics* (9:1), pp. 42-63.
Hofstede, G. 1994. *Cultures and Organizations: Software of the Mind: Intercultural*, HarperCollins: London.
Hofstede, G. 2001. *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations*, Sage Publications: Thousand Oaks, CA.
Hsiu-Fen, L. 2006. "Understanding Behavioral Intention to Participate in Virtual Communities," *CyberPsychology & Behavior* (9:5), pp. 540-547.
Hu, L., and Bentler, P. M. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1-55.
Hu, Q., and Dinev, T. 2005. "Is Spyware an Internet Nuisance or Public Menace?," *Communications of the ACM* (48:8), pp. 61-66.
ITRC 2011. "2011 Data Breaches Report," Identity Theft Resource Center.
ITU 2003. "World Telecommunication Indicators Database," International Telecommunication Union.
ITU 2005. "ITU's New Broadband Statistics," International Telecommunication Union.
Joreskog, K. G., and Sorbom, D. 1988. *LISREL 7: A Guide to the Program and Applications*, SPSS Inc.: Chicago, IL.
Kacen, J. J., and Lee, J. A. 2002. "The Influence of Culture on Consumer Impulsive Buying Behavior," *Journal of Consumer Psychology* (12:2), pp. 163-176.
Kelloway, E. K. 1998. *Using LISREL for Structural Equation Modeling: A Researcher's Guide*, SAGE Publications, Inc.: Thousand Oaks, CA.
Kim, D., Pan, Y., and Park, H. S. 1998. "High-versus low-Context Culture: A Comparison of Chinese, Korean, and American Cultures," *Psychology and Marketing* (15:6), pp. 507-521.
Kim, D. J. 2008. "Self-Perception-Based Versus Transference-Based Trust Determinants in Computer-Mediated Transactions: A Cross-Cultural Comparison Study," *Journal of Management Information Systems* (24:4), pp. 13-45.
Klassen, R. M. 2004. "Optimism and Realism: A Review of Self-Efficacy From a Cross-Cultural Perspective," *International Journal of Psychology* (39:3), pp. 205-230.
Kline, R. G. 1998. *Principles and Practices of Structural Equation Modeling*, Guilford Press: New York, NY.
Kunreuther, H., and Heal, G. 2003. "Interdependent Security," *Journal of Risk and Uncertainty* (26:2), pp. 231-249.
Kwon, O., Choi, K., and Kim, M. 2007. "User Acceptance of Context-Aware Services: Self-Efficacy, User Innovativeness and Perceived Sensitivity on Contextual Pressure," *Behaviour & Information Technology* (26:6), pp. 483-498.

Lallana, E. C. 2004. "An Overview of ICT Policies and E-Strategies of Select Asian Economies," United Nations Development Programme-Asia Pacific Development Information Programme, Bangkok, Thailand.

Lee, J. A. 2000. "Adapting Triandis's Model of Subjective Culture and Social Behavior Relations to Consumer Behavior," *Journal of Consumer Psychology* (9:2), pp. 117-126.

Leidner, D. E., and Kayworth, T. 2006. "Review: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict," *MIS Quarterly* (30:2), pp. 357-399.

Lichacz, F. M., and Partington, J. T. 1996. "Collective Efficacy and True Group Performance," *International Journal of Sport Psychology* (27:2), pp. 146-158.

Lin, H. F. 2006. "Understanding Behavioral Intention to Participate in Virtual Communities," *CyberPsychology & Behavior* (9:5), pp. 540-547.

Little, B. L., and Madigan, R. M. 1997. "The Relationship Between Collective Efficacy and Performance in Manufacturing Work Teams," *Small Group Research* (28:4), pp. 517-534.

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), pp. 173-186.

Madon, S. 1992. "Computer-Based Information Systems for Development Planning: the Significance of Cultural Factors," *The Journal of Strategic Information Systems* (1:5), pp. 250-257.

Marakas, G., Johnson, R., and Clay, P. F. 2007. "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time," *Journal of the Association for Information Systems* (8:1), pp. 16-46.

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

Markus, H., and Kitayama, S. 1991. "Culture and the Self: Implications for Cognition, Emotion, and Motivation," *Psychological Review* (98:2), pp. 224-253.

McKnight, L. W., and Bailey, J. P. 1997. *Internet economics*, Mit Press Cambridge, Massachusetts.

McLean, K. Year. "Information Security Awareness - Selling the Cause," Proceedings of the IFIP TC11/Sec'92, Singapore, 1992.

Morden, T. 1999. "Models of National Culture - A Management Review," *Cross Cultural Management* (6:1), pp. 19-44.

Morwood, G. 1998. "Business Continuity: Awareness and Training Programmes," *Information Management & Computer Security* (6:1), pp. 28-32.

Musumeci, J. J., and Sinkey, J. F. 1990. "The International Debt Crisis, Investor Contagion, and Bank Security Returns in 1987: The Brazilian Experience," *Journal of Money, Credit and Banking* (22:2), pp. 209-220.

NCA 2006. "2006 Informatization White Paper," National Computerization Agency.

NIST 1995. "special Publication 800-12: An Introduction to Computer Security: The NIST Handbook," National Institute of Standards and Technology.

Nunnally, J. C. 1978. *Psychometric Theory*, (2nd Ed.) McGraw-Hill: New York.

Nunnally, J. C., and Bernstein, I. H. 1994. *Psychometric Theory*, (3rd Ed.) McGraw-Hill: New York.

OECD 2004. "OECD Broadband Statistics," Paris.

Oettingen, G. 1995. *Cross-Cultural Perspectives on Self-Efficacy*, in A. Bandura (Ed.), Self-Efficacy in a Changing Societies. pp. 149-176. New York: Cambridge University Press.

Pajares, F., and Graham, L. 1999. "Self-Efficacy, Motivation Constructs, and Mathematics Performance of Entering Middle School Students," *Contemporary Educational Psychology* (24:2), pp. 124-139.

Pavlou, P. A., and Chai, L. 2002. "What Drives Electronic Commerce Across Cultures? A Cross-Cultural Empirical Investigation of the Theory of Planned Behavior," *Journal of Electronic Commerce Research* (3:4), pp. 240-253.

Peterson, E., Mitchell, T., Thompson, L., and Burr, R. Year. "Group Efficacy and Shared Cognition As Predictors of Group Process and Performance," Academy of Management Meetings 1996.

Peterson, E., Mitchell, T. R., Thompson, L., and Burr, R. 2000. "Collective Efficacy and Aspects of Shared Mental Models as Predictors of Performance Over Time in Work Groups," *Group Processes & Intergroup Relations* (3:3), pp. 296-316.

Polonchek, J., and Miller, R. K. 1999. "Contagion Effects in the Insurance Industry," *Journal of Risk and Insurance* (66:3), pp. 459-475.

Rhee, H. S., Kim, C., and Ryu, Y. U. 2009. "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," *Computers & Security* (28:8), pp. 816-826.
Sampson, R. J., Raudenbush, S. W., and Earls, F. 1997. "Neighborhoods and Violent Crime: A Multilevel Study of Collective Efficacy," *Science* (277:5328), pp. 918-924.
Sarker, S., Valacich, J. S., and Sarker, S. 2005. "Technology Adoption By Ggroups: A Valence Perspective," *Journal of the Association for Information Systems* (6:2), pp. 37-71.
Scholz, U., Doña, B. G., Sud, S., and Schwarzer, R. 2002. "Is General Self-Efficacy a Universal Construct? Psychometric Findings From 25 Countries," *European Journal of Psychological Assessment* (18:3), pp. 242-251.
Schunk, D. H., and Pajares, F. 2009. "Self-Efficacy Theory," *Handbook of Motivation At School*, pp. 35-53.
Schwarzer, R., Bäßler, J., Kwiatek, P., Schröder, K., and Zhang, J. X. 1997. "The Assessment of Optimistic Self-Beliefs: Comparison of the German, Spanish, and Chinese Versions of the General Self-Efficacy Scale," *Applied Psychology* (46:1), pp. 69-88.
Schwarzer, R., Mueller, J., and Greenglass, E. 1999. "Assessment of Perceived General Self-Efficacy on the Internet: Data Collection in Cyberspace," *Anxiety, Stress and Coping* (12:2), pp. 145-161.
Sia, C. L., Lim, K. H., Leung, K., Lee, M. K. O., Huang, W. W., and Benbasat, I. 2009. "Web Strategies to Promote Internet Shopping: Is Cultural-Customization Needed?," *MIS Quarterly* (33:3), pp. 491-512.
Silver, W. S., and Bufanio, K. M. 1996. "The Impact of Group Efficacy and Group Goals on Group Task Performance," *Small Group Research* (27:3), pp. 347-359.
Siponen, M. T. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1), pp. 31-41.
Siponen, M. T. 2001. "Five Dimensions of Information Security Awareness," *Computers and Society* (31:2), pp. 24-29.
Siponen, M. T., Kajava, J. 1998. *Ontology of Organizational IT Security Awareness-From Fheoretical Foundations to Practical Framewo*, IEEE Computer Society Press: Los Alamitos, CA.
Skinner, E. A. 1995. *Perceived Control, Motivation, & Coping*, Sage Publications, Inc.
Spurling, P. 1995. "Promoting Security Awareness and Commitment," *Information Management and Computer Security* (3:2), pp. 20-26.
Stajkovic, A. D., and Luthans, F. 1998. "Self-Efficacy and Work-Related Performance: A Meta-Analysis," *Psychological Bulletin* (124:2), pp. 240-261.
Staples, D. S., Hulland, J. S., and Higgins, C. A. 1999. "A Self-Efficacy Theory Explanation for the Management of Remote Workers in Virtual Organizations," *Organization Science* (10:6), pp. 758-776.
Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.
Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risks: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.
Tan, F., Urquhart, C., and Yan, S. Year. "A Conceptual Model for Online Shopping Behavior: Trust and National Culture," Proceedings of the 5th International Business Research Forum, Temple University, Philadelphia, PA, USA, 2004.
Udo, G. J. 2001. "Privacy and Security Concerns as Major Barriers for E-Commerce: A Survey Study," *Information Management & Computer Security* (9:4), pp. 165-174.
Venkatesh, V., and Davis, F. D. 1996. "A Model of the Antecedents of Perceived Ease of Use: Development and Test," *Decision Sciences* (27:3), pp. 451-481.
Voloper 2008. "10 Barriers to Ecommerce and Their Solutions," Voloper Creations Inc., Vaughan, ON, Canada.
Wood, R., and Bandura, A. 1989. "Social Cognitive Theory of Organizational Management," *Academy of Management Review* (14:3), pp. 361-384.
Zakour, A. B. Year. "Cultural Differences and Information Technology Acceptance," 7th Annual Conference of the Southern Association for Information Systems2004, pp. 156-161.

Appendix 1. Measurement Items

Constructs	Measurement Items
General InfoSec Control Awareness (1-strongly disagree / 7-strongly agree)	AW1: In general, threats to information security are controllable. AW2: In general, technology is advanced enough to prevent information security threats. AW3: In general, there exist technologies to detect information security attacks.
InfoSec Collective Efficacy (1-not concerned / 7-strongly concerned)	SE1: **Our organization** has the means to control information security threats. SE2: **Our organization** has the ability to execute security practices to avoid information security threats. SE3: **Our organization** has access to necessary resources to protect our information systems. SE4: **Our organization** has elaborate plans to cope with information security threats. SE5: **Our organization** can exercise a course of action to avoid an information security breach.
Vulnerability from Partners (1-extremely low / 7-extremely high)	VP1: The likelihood that the operations in **our organization** will be disrupted due to information security breaches originating from our business partners is VP2: The chance that **our organization** will fall a victim to an information security breach originating from our business partners is VP3: The vulnerability of **our organization** to information security threats originating from our business partners is
InfoSec Vulnerability (1-extremely low / 7-extremely high)	VU1: The risk from information security threats to **our organization** is VU2: The likelihood that the information systems in **our organization** are disrupted due to information security breaches in the next 12 months is VU3: The chance that **our organization** will fall a victim to an information security breach is VU4: The vulnerability of **our organization** to information security threats is