THE EFFECT OF COLLECTIVE EFFICACY AND NETWORK DEPENDENCE ON MANAGERS' INFORMATION SECURITY RISK PERCEPTION

Completed Research Paper

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

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

Young Kwark
University of Texas at Dallas
Richardson, Texas, USA
youngk082@utdallas.edu

Abstract

Achieving a high level of information security for organizations is difficult due to both technical and managerial reasons. Information technology is getting more sophisticated and thus organizational information systems are becoming more complex. Accordingly, attackers find more intrusion opportunities caused by increased system vulnerabilities. In addition to technical reasons, there are managerial difficulties. Security of organizational information systems requires awareness, commitment, and efforts from not only security specialists and top management but also individual users. That is, it requires the whole group members' efforts. Further, interconnectedness of organizational information systems makes security more difficult. Using a group-level collective efficacy in information security and network dependence as main constructs, we propose an organizational information security risk perception model and validate it using empirical data collected from executive-level information systems managers in the U.S. While there was a concern about IS managers' correct perception of risk caused or amplified by network dependence of information systems, we find that IS managers are aware of such security risk. We provide theoretical contributions of the study and discuss practical implications of the findings for information systems managers.

Keywords: Information Security, network dependence, interdependent risk, collective efficacy

Introduction

Achieving a high level of information security for firms and organizations is difficult for a number of reasons. Information technology is getting more sophisticated and thus organizational information systems are becoming more complex. While technical and technological development and sophistication contribute to the increase of organizational information systems' capability, attackers find more intrusion opportunities caused by increased system vulnerabilities. In addition to the technical reasons, there are managerial reasons of difficulty in security. First, security of organizational information systems requires awareness, commitment, and efforts from not only security specialists and top management but also individual users. For instance, a user's simple mistake of releasing his password can nullify his firm's strong technical security measures of data encryption, intrusion protection, firewall, strong password scheme, and others. Second, many organizational information systems nowadays are interconnected with business partners' systems and even with the public network. Thus, a firm's security of systems depends on others' security efforts as well as its own. This notion of security interdependence is a potentially significant source of risk (Kunreuther and Heal 2003).

Proper understanding of risk is a major determinant of intention to perform security actions (Crockford 1980). Focusing on managerial aspects of organizational information security, in this paper, we would like to explore if information systems (IS) managers have a correct view of security risks (Goodhue and Straub 1991; Hu and Dinev 2005; Loch et al. 1992; Straub and Welke 1998), in particular, risks due to interconnectedness of information systems (i.e., network dependence) (Kunreuther and Heal 2003; Loch et al. 1992). We propose a research model that includes an organization-level domain-specific self-efficacy construct and examine its impact on organization-level information security risk perception from IS managers' viewpoint. Self-efficacy is "people's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances" (Bandura 1986a, p. 391). Its concept can be extended to a group level, referring as *collective efficacy* or *group efficacy*, which is defined as a group's shared belief in their capability to perform a specific task (Bandura 2000; Goddard et al. 2004). Collective efficacy is an important group-level resource that provides the construal of collective ability to cope with uncertainties and to contribute a productive group climate. Although the concept of self-efficacy has been widely studied, its effect on risk perceptions at the group level in the information security domain has not been investigated by prior research. Because security of organizational information systems requires the whole organization's (i.e., technical staff's, managers', and end-users') efforts, the use of collective efficacy seems desirable. Along with the new enhanced concept of collective efficacy as an independent construct in our study, we add perceived *network dependence* of information systems as another independent construct and divide IS managers' information security risk perception into two separated elements (i.e., risk perception on own organization and risk perception from partners).

We validate the proposed research model using empirical data collected from executive-level information systems managers in the U.S. The results of the analysis are interpreted. Conclusively, we provide theoretical contributions of the study and discuss practical implications of the findings for information systems managers.

Literature Review

Self-efficacy and Collective Efficacy

Since Bandura (1977) introduced the concept of self-efficacy, it has been viewed as the foundation of human agency in social cognitive theory. Self-efficacy, "belief in one's capacity to execute the courses of action required to produce given attainments in specific situations or contexts" (Bandura 1997), is necessary motivation to manage given situational tasks (Wood and Bandura 1989). Hence, though the judgment on efficacy is not necessarily accurate assessments of individual's capacity, it is important that such judgment may lead to courses of actions (Bandura 1997). The importance of self-efficacy has been found as its role in human functioning (i.e., students' achievement and their efficacy) (Bouffard-Bouchard et al. 1991; Polonchek and Miller 1999).

In many circumstances, the outcome in performance of task can be achieved through interdependent efforts among group members. Bandura (1986b) proposed the concept of collective efficacy as an extension of self-efficacy to a group level. Collective efficacy is defined as a shared belief in the group's collective power to produce desired outcome (Gibson 1999). Collective efficacy is rooted in self-efficacy, which influences what people choose to do as a group (Bandura 1982). The choices of individuals and organizations are influenced by how strong their efficacy is.

It is not uncommon that a group with talented members performs poorly; hence, collective efficacy is not a simple sum of individuals' efficacy (Bandura 2000). The predictive role of collective efficacy in the group performance has been found in several contexts (Goddard et al. 2004; Hodges and Carron1992; Lichacz and Partington 1996; Little and Madigan1997; Sampson et al. 1997).

Since self-efficacy is about own judgment of capability, one of issues in self-efficacy studies is the bias of self-enhancement in measurement level. It is true that people have a general tendency to evaluate themselves more favorably than others (Alicke and Govorun 2005; Alicke et al. 1995; Rhee et al. 2005), to describe their own personalities in highly favorable terms (Brown 1986), and to express optimism about the future (Heckhausen and Krueger 1993). These egocentric judgment patterns are well known as self-enhancement bias. Although the research on self-efficacy and collective efficacy has been conducted in many studies (e.g., Agarwal and Karahanna 2000; Compeau and Higgins 1995; Marakas et al. 1998; Venkatesh and Davis 1996), surprisingly, very limited studies have dealt with this important measurement bias in the efficacy literature.

Self-efficacy/Collective Efficacy and Risk Perception in Information Security

A number of studies (Hsiu-Fen 2006; Kwon et al. 2007; Rhee et al. 2009; Scholz et al. 2002; Staples et al. 1999) support the strong negative relationship between self-efficacy and risk perception. Individuals with higher self-efficacy may perceive less risk. In a group level, high efficacy for the group ability to produce desired outcome is less likely to lead to a shared belief toward a failure. As indicated by prior studies in organizational information technology adoption, senior managers' decision often critically hinges on their beliefs on their organizations' capability (e.g., Chau and Tam 1997), which may present the organizations' collective efficacy.

In the information security domain, self-efficacy has been studied as an underlying construct for a specific information security task in several contexts. For example, regarding employees' compliance, Bulgurcu et al. (2010) define self-efficacy as an individual employee's judgment of personal skills and competency about fulfilling the requirements of the ISP (information security policy). They show that an employee's intention to comply with the ISP is significantly influenced by self-efficacy, attitude, and normative beliefs. They report the significant impact of outcome beliefs on beliefs about overall assessment of consequences, and thus on employee's attitude. Dinev and Hu (2007) find that, differently from the context of positive technologies, perceived ease of use and self-efficacy are not strong determinants of the individual users' attitudes towards behavior in response to the negative technologies such as cyber-attacks, viruses and spyware. They indicate the level of computer technical skills/knowledge of the threat affects the magnitude of the relationships associated with self-efficacy, ease of use, and perceived usefulness. In a cross-cultural study drawn upon the theory of planned behavior (Ajzen 2002), Dinev et al. (2009) report the significant relationship between self-efficacy and perceived behavior control in South Korea compared with the insignificant relationship in the U.S. They explain the reason of insignificance in the U.S. from the knowledge differences rather than from cultural differences.

Rhee et al. (2009) study self-efficacy in the context of information security regarding the influence of self-efficacy on individual users' management against information security risk and their intentions whether to increase efforts for security. They report individuals with high self-efficacy in information security show more usage in security software and show more security care behavior related to computer/Internet usage. More importantly, individuals with high self-efficacy present intention to continue and increase the efforts for security. Their findings confirm self-efficacy as an important construct in individuals' information security practices, which is consistent with previous works that show self-efficacy motivates an individual to make an continuous effort (e.g., Agarwal and Karahanna 2000; Compeau and Higgins 1995; Thatcher and Perrewe 2002)

Some studies have empirically investigated factors that affect the anti-malware software adoption based on the protection motivation theory. In general, they show that the severity of threat or perceived vulnerability increases the intention to adopt the anti-malware software, and the ability to conduct a recommended action using the software leads to more intention to adopt the software (Lee et al. 2008; Lee and Larsen 2009; Zhang and McDowell 2009).

Some other studies have noted the importance of managers' vigilance about the information security (Goodhue and Straub 1991; Hu and Dinev 2005; Loch et al. 1992; Straub and Welke 1998). Straub and Welke (1998) raise the issues of managers' naive response to the challenges by the threat (Loch et al. 1992) and point the lack of managers' knowledge for effective control. They show the theoretical background for the effective countermeasure and suggest a managerial guideline for coping with system risk by empirically identifying an approach that can effectively deal with the security risk. They identify how managers should cope with system risk more effectively by conducting

qualitative studies in two information services Fortune 500 firms. Despite the importance of managers' vigilance regarding 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 the managers' perceived risk. Moreover, to our best knowledge, no study has been conducted about the effect of collective efficacy on the high-level managers' perceived risk in the domain of information security.

Interdependent Security

The interdependent security issue has been recently raised (Kunreuther and Heal 2003), because of the increased interconnectivity among business firms. Kunreuther and Hall (2003) argue the organization should make investment decision to protect it from information security risk depending on how others manage their security risks as well as how it manages its own risks. It is similar to the financial contagion issues in which 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). Therefore, the managers' perception of the risk from their partners is critical since managers' perceived risk from partners influences managers' own risk perception due to the cross-effect between one's incentive induced by the perceived risk and the others' behavior (Kunreuther and Heal 2003). Due to the novelty of the interdependent security issue, only limited studies have empirically investigated the perceived interdependent security risk from partners.

The proceedings are formatted for standard US letter paper (8.5 x 11 inches or 21.6 x 28 cm). The page margins, excluding headers and footers are 1 in. (2.5 cm) all around. All final publications will be formatted and displayed in US letter size. Margins should be full justified, not ragged right (use the `Normal` style). Beware, especially when using this template on a Macintosh, as Word may change these dimensions in unexpected ways.

Research Model and Hypothesis

The risk components model of (Crockford 1980), which provides a conceptual framework for generic risk management, includes risk controlling factors that are internal (e.g., security controllability) or external (e.g., network dependence) features reducing (inhibiting) or increasing (amplifying) the probability of threat manifestation and the severity of damages caused by threat. In information technology risk management frameworks (GAO 1999; Stoneburner et al. 2002), such risk inhibiting factors correspond to the risk management elements of defining security policies, defining technical architecture, management deployment of security measures, and consistent monitoring and control of the overall security infrastructure. On the other hand, increased connectivity or network dependence has been viewed as a security risk amplifying factor, due to the openness of distributed systems and the existence of more potential security attack points than centralized systems (Kunreuther and Heal 2003; Loch et al. 1992). In this study, we propose a research model of information security risk management addressing these risk inhibiting and amplifying factors and hypothesize the relationships between these factors and information security risk perceptions from IS managers' perspective. A graphical form of nomological network with hypotheses is illustrated in Figure 1.

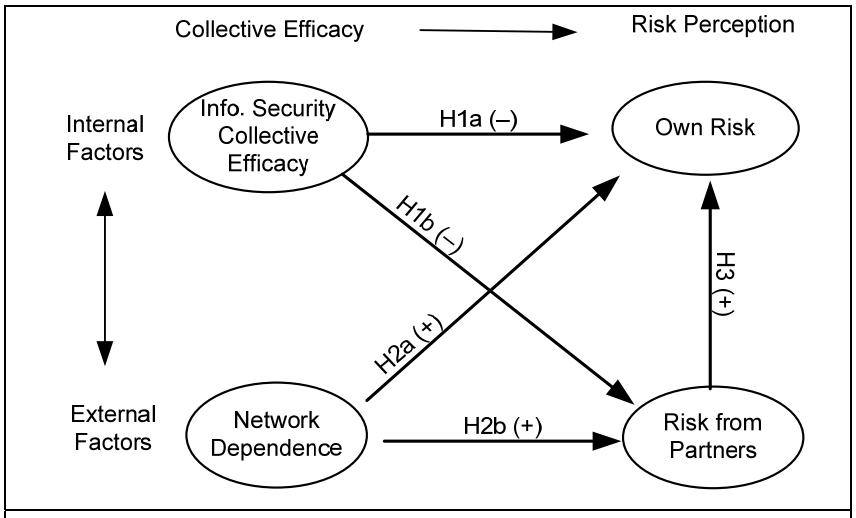

Figure 1. The Research Model

Collective efficacy refers to an optimistic sense of group competence which increases a group's efforts to promote accomplishment in challenging circumstances (Bandura 2000). Adopting the concept of *collective efficacy* in the domain of information security, we use a domain-specific *information security collective efficacy* as an extended concept of self-efficacy to an organizational level in the context of information security. A number of efficacy studies (Kwon et al. 2007; Rhee et al. 2009) support the strong negative relationship between efficacy and risk perception. In the context of information security, it is expected that the higher degree of perceived information security collective efficacy leads to the lower degree of perceived information security risk. This strong negative relationship will be true in the relationship between information security risk perceptions and information security collective efficacy. In other words, information security mangers with higher belief on information security collective efficacy are more likely to perceive lower own information security risk. Thus, we propose:

H1a: Information security collective efficacy is negatively associated with own information security risk perception.

A firm's information security control and risk management cover not only its own network systems but also other networks connected to its systems (GAO 1999; Stoneburner et al. 2002). That is, risks originating from interconnected systems of business partners can be moderated with a high level of security controllability. In other words, when IS managers perceive a higher level of their firms' capability to control information security risks, their perception of risks from partners would be likely low. Therefore, we propose the following hypothesis:

H1b: Information security collective efficacy is negatively associated with information security risk from partners.

Network dependence refers to the degree of information sharing and mutual control of computer network systems within a distributed organization and between the organization and its partners. Increased connectivity has been viewed as a factor amplifying security risk (Loch et al. 1992). In fact, previous surveys and reports confirmed the connectivity as the most frequent point of security attacks and warned of risks associated with interconnected computer systems. Further, recent studies on interdependent security (Kunreuther and Heal 2003) indicate that threats are easily manifested among computer systems linked through trusted networks. It is reasonable to assume that when an organization has a high level of network interdependence with its partners, its risk depends on security protection actions of partners as well as its own. From these, we propose the following hypotheses:

H2a: Network dependence has positive effect on the information security risk from self.

H2b: Network dependence has positive effect on the information security risk from partners.

A firm's own information security risk is at least partially depends on the vulnerabilities of partner firms. Therefore, it would be a logical expectation that the higher level of information security risk from partners is perceived, the

greater degree of own risk perception associated with information security. Based on the arguments above, we propose that:

H3: Information security risk from partners has a positive effect on the information security risk from self.

Research Methodology and Data Collection

Focusing on the domain of information security control and risk from interdependent security perspective, the survey items to measure information security collective efficacy, perceived risk, and risk from others due to network dependence were initially developed based on previous literature, published security survey reports, and interviews with two information security professionals who were chief security officers of a profit firm and a non-profit organization. Two-round pilot tests with information systems professionals and IS major graduate students were conducted to ensure the accuracy of item wordings, the reliability of the scales, and general mechanics of the survey questionnaire including appropriateness of instructions and completion time. Based on the pilot test results, the survey questionnaire was streamlined and finalized.

Several approaches have been proposed to measure collective efficacy, including aggregating individual self-efficacy beliefs, aggregating individuals' perceptions of their group's capability, and having group members' concordant judgment of collective efficacy (Bandura 2000; Goddard et al. 2004). Among them, it was argued that aggregating individual perceptions of group (as opposed to self) better captures the intended meaning (Goddard et al. 2004). However, aggregating individual members' measures of their group's information security collective efficacy is not a simple matter because of their heterogeneity. An organization's information security requires efforts from IS or security managers, computer users, and general managers, and their measures of collective efficacy cannot have equal weights due to differences in their roles and perspectives in their organization's information security. Among these three different groups of members of organizations, we argue that IS managers' measures of their organizations' collective efficacy would be more reliable and accurate than others. Thus, we measure the collective efficacy from IS managers' perspective of group.

Since this study specifically focuses on information security efficacy from IS managers' perspective under the context of the different level of interconnectivity, it is an appropriate approach to collect IS managers' perceived information security collective efficacy and network dependence through survey questionnaires from IT/IS executives (i.e., managers having a title of chief information officer, IT director, or a similar one). For data collection, we selected IS executives of 2027 organizations. In order to encourage subjects' participation and improve the response rate, we carried out two rounds of survey-questionnaire mailing in a period of six weeks and post-card reminding between the two rounds. A total of 222 survey responses were received. Among them, 46 were dropped due to missing data points or multiple answers for a same item. Organizations of responded IS executives were companies and institutes from various for-profit and non-profit sectors including manufacturing, banking, transportation, retail, health-care, various other service sectors, education, and government.

Data Analysis and Results

Structural equation modeling (SEM) approach was used to analyze the data for both the measurement model and structural model. Compare to a conventional regression analysis that ignores the interrelationships between latent constructs measured by multiple measurement items (Bollen 1989), SEM is a statistical methodology that takes a confirmatory (i.e., hypothesis-testing) approach to the analysis of causal relationships among latent construct (i.e., a structural theory). There are two families of SEM techniques: covariance-based techniques (e.g., AMOS) and variance-based techniques (e.g., SmartPLS). In this study, we use both AMOS 19.0 (build 1375) and SmartPLS version 2.0.M3 to test the measurement model and structural model because SmartPLS and AMOS can be regarded as complementary. SmartPLS reports composite reliability (CR) and average variance extracted (AVE) for content validity and discriminant validity. Based on covariance analysis, like LISREL, AMOS is more confirmatory in nature and it provides various overall goodness-of-fit indices to assess model fit for convergent validity.

To ensure the psychometric properties of the instrument, it was tested for reliability and validity of 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. The internal consistency of the measurement models was tested by examining Cronbach's alpha and Fornell's composite reliability. Table 1 shows the summarized reliability indices. The values of the

Cronbach reliability coefficients range from .745 to .957, which are higher than the minimum cutoff score of .7. Composite reliability should be greater than the benchmark of .7 to be considered adequate. The lowest composite reliability is .861, which is a value higher than .7, indicating adequate internal consistency.

Table 1. Reliability, Correlation, and Discriminant Validity of Constructs

Constructs	Alpha	CR	AVE	1	2	3	4
1, Relative InfoSec Collective Efficacy	0.893	0.917	0.689	**0.830**			
2. Network Dependency	0.712	0.830	0.627	0.045	**0.791**		
3. Perceived InfoSec Risk	0.855	0.902	0.700	-0.200	0.222	**0.836**	
4. Perceived InfoSec Risk from Partner	0.951	0.968	0.910	-0.193	0.513	0.209	**0.954**

The correlations between the constructs, the average variances extracted (AVE) of each latent construct, are, as shown in Table 1, between .628 and .910, and the square roots of the AVE are between .791 and .954. The square root of the AVE of each constructs is greater than its correlations with other constructs, indicating that the constructs show acceptable convergent validity. The discriminant validity is tested by the factor loadings and cross-loading loading (see Table 2). All factor loadings exceed the minimum level of .5 and cross-loadings are lower than the loadings on the anticipated constructs, suggesting sufficient discriminant validity.

Table 2. Exploratory Factor Analyses

Constructs	Items	Components			
		1	2	3	4
1. InfoSec Relative Collective Efficacy	RCE1	**0.899**	-0.019	-0.202	-0.233
	RCE2	**0.886**	0.044	-0.129	-0.115
	RCE3	**0.877**	0.046	-0.225	-0.164
	RCE4	**0.687**	0.179	-0.016	-0.015
	RCE5	**0.783**	0.073	-0.128	-0.146
2. Network Dependency	ND1	-0.003	**0.874**	0.173	0.176
	ND2	0.048	**0.879**	0.216	0.223
	ND3	0.085	**0.587**	0.121	0.039
3. Perceived InfoSec Risk	PR1	-0.017	0.141	**0.679**	0.293
	PR2	-0.201	0.201	**0.867**	0.456
	PR3	-0.201	0.222	**0.920**	0.491
	PR4	-0.200	0.168	**0.859**	0.442
4. Perceived InfoSec Risk from Partner	PRP1	-0.195	0.230	0.511	**0.953**
	PRP2	-0.184	0.183	0.477	**0.962**
	PRP3	-0.171	0.182	0.478	**0.947**

After confirming the validity of measurement model, we conduct the structural model testing using SmartPLS. The significance of path coefficients is calculated using a boots strap technique with an option of 300 resamples. Figure 2 depicts the results of structural model testing. As shown in Figure 2, all of the five hypotheses are supported at the .05 significance or better levels. The path coefficients from information security collective efficacy to information security risk perception from self (β = –.117, p < .05) and information security risk perception from partners (β = –.202, p < .01) are significant. These results support H1a and H1b. The causal relationships between network dependence and perceived risk from self and perceived risk from partners show statistically significant results (β = .131, p < .01 and β = .281, p < .001), respectively; therefore, H2a and H2b are supported. As we expected, perception on the risk from partners has highly strong positive effect on perception on information security risk (β = .462, p < .001) which supports H3. The structural model explains 29% of the variance in information security risk perception from self and 10% of the variance in information security risk perception from partners.

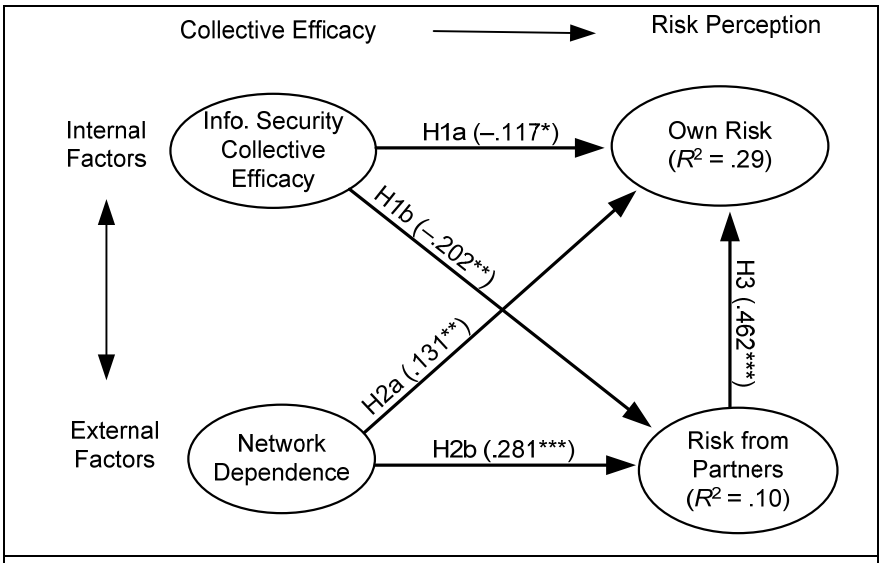

Figure 2. Results of the Structural Model (*p = .05, **p = .01, ***p = .001)

Concluding Remarks

Although a large number of studies in information systems (IS) and behavioral sciences examine the role of self-efficacy at the individual level, little is known of the effect of collective efficacy from senior managers' perspective at the firm level. This study explicitly measures the collective efficacy, the perceived group efficacy responded by the executive managers. This study also models risks amplified by interconnectivity of information systems (Loch et al. 1992) and interdependence of information security risks (Kunreuther and Heal 2003), and test if managers are aware of them.

While there was a concern about IS managers' correct perception of risk caused or amplified by network dependence of information systems (Loch et al. 1992), the results of the study show that IS managers are aware of such security risk. Though many surveys report ever-increasing information security threats manifested by powerful attackers, we view that our finding is encouraging.

Methodologically, the study shows that information security collective efficacy is a strong predictor to reduce not only the level of perceived information security risk from own firm but also that of information security risk from partners. Higher degree of network dependence significantly influences the executive-level manager's information security risk perceptions from own firm as well as from partner firms. Consistent with the arguments of interdependent security literature, perceived information security risk from own firm is significantly induced by the perceived risk of other partner firms.

The unique contributions of this study to the information security literature and self-efficacy literature are multifaceted. First, this study extends the role of collective efficacy from executive managers' perspective in the context of information security. The use of *collective* efficacy (Bandura 2000) in the information security domain is appropriate since a firm's information security requires organizational-level commitments. Second, this study shows that the collective efficacy in information security contributes to the managers' vigilance about the risk from their own organizations and that from their partners. Third, this study tests the network dependence and the managers' perceived risk in the information security. Considering the huge reliance on the interorganizational information systems in business, understanding the effect of the network dependence on the managers' risk perception is essential. We show the network dependence not only increases the perceived risk from the business partners but also allows the managers to perceive the risk on their own organizations' information security. Further, we empirically verify that managers are aware of interdependence of information security risk.

There are several limitations of this study, which should be considered in future research. First, this study used IS executive managers' perception of collective efficacy. Although collective efficacy from executive managers' viewpoint reflects the organizational efficacy better than other individual measures since the IS managers are better informed about the level of control at the organizational level than any other individuals, it is certainly a limitation

of a group-level study. Second, this study also measured managers' perceived risk perceptions as a proxy of organizational-level information security risk and future vulnerability, because of the nature of limited public access of internal reports of information security risk. We believe that there are other ways to directly measure a firm' own information security risk and information security risk from partners (e.g., frequency of incidents in a given time period). Thus, future study will examine effect of other cognitive and non-cognitive factors that affect forming the collective efficacy or the perceived risk from own and from partners. For instance, the past experience of information security breaches compared to the level of IT usage may affect both the collective efficacy and the future vulnerability. Further, how the past breach experience of the partners as well as that of own organizations differently affect the collective efficacy and thus risk perception will be studied. By extending our research to these ways, we will have more complete insights.

References

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), pp. 665–694.

Ajzen, I. 2002. "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1," *Journal of Applied Social Psychology* (32:4), pp. 665–683.

Alicke, M.D., and Govorun, O. 2005. *The Better-Than-Average Effect*. New York: Psychology Press.

Alicke, M.D., Klotz, M.L., Breitenbecher, D.L., Yurak, T.J., and Vredenburg, D.S. 1995. "Personal Contact, Individuation, and the Better-Than-Average Effect," *Journal of Personality and Social Psychology* (68:5), p. 804–825

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

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

Bandura, A. 1982. "Self-Efficacy Mechanism in Human Agency," *American Psychologist* (37:2), p. 122–147.

Bandura, A. 1986a. "The Explanatory and Predictive Scope of Self-Efficacy Theory," *Journal of Social and Clinical Psychology* (4:3), pp. 359–373.

Bandura, A. 1986b. *Social Foundations of Thought and Action. A Social Cognitive Theory*. Englewood Cliffs, NJ: Prentice Hall.

Bandura, A. 2000. "Exercise of Human Agency through Collective Efficacy," *Current Directions in Psychological Science* (9:3), pp. 75–78.

Bollen, K.A. 1989. *Structural Equations with Latent Variables*. New York, NY: Wiley.

Bouffard-Bouchard, T., Parent, S., and Larivee, S. 1991. "Influence of Self-Efficacy on Self-Regulation and Performance among Junior and Senior High-School Age Students," *International Journal of Behavioral Development* (14:2), pp. 153–164.

Brown, J.D. 1986. "Evaluations of Self and Others: Self-Enhancement Biases in Social Judgments," *Social Cognition* (4:4), pp. 353–376.

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.

Chau, P.Y.K., and Tam, K.Y. 1997. "Factors Affecting the Adoption of Open Systems: An Exploratory Study," *MIS Quarterly* (21:1), pp. 1–24.

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.

Crockford, N. 1980. *An Introduction to Risk Management*. Cambridge, MA: Woodhead-Faulkner.

Dinev, T., Goo, J., Hu, Q., and Nam, K. 2009. "User Behaviour Towards Protective Information Technologies: The Role of National Cultural Differences," *Information Systems Journal* (19:4), pp. 391–412.

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), Article 23.

GAO. 1999. "Information Security Risk Assessment: Practices of Leading Organizations," U.S. Government Accountability Office, Washington, DC.

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.

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.
Heckhausen, J., and Krueger, J. 1993. "Developmental Expectations for the Self and Most Other People: Age Grading in Three Functions of Social Comparison," *Developmental Psychology* (29:3), p. 539–548.
Hodges, L., and Carron, A.V. 1992. "Collective Efficacy and Group Performance," *International Journal of Sport Psychology* (23:1), pp. 48–59.
Hsiu-Fen, L. 2006. "Understanding Behavioral Intention to Participate in Virtual Communities," *CyberPsychology & Behavior* (9:5), pp. 540–547.
Hu, Q., and Dinev, T. 2005. "Is Spyware an Internet Nuisance or Public Menace?" *Communications of the ACM* (48:8), pp. 61–66.
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.
Lee, D., Larose, R., and Rifon, N. 2008. "Keeping Our Network Safe: A Model of Online Protection Behaviour," *Behaviour & Information Technology* (27:5), pp. 445–454.
Lee, Y., and Larsen, K.R. 2009. "Threat or Coping Appraisal: Determinants of Smb Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18:2), pp. 177–187.
Lichacz, F.M., and Partington, J.T. 1996. "Collective Efficacy and True Group Performance," *International Journal of Sport Psychology* (27:2), pp. 146–158.
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.
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.
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.
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.
Rhee, H.S., Ryu, Y., and Kim, C.T. 2005. "I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security," in *Proceedings of International Conference on Information Systems*.
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), p. 242–251.
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.
Stoneburner, G., Goguen, A., and Feringa, A. 2002. "Risk Management Guide for Information Technology Systems," NIST special publication 800-30.
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.
Thatcher, J.B., and Perrewe, P.L. 2002. "An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy," *MIS Quarterly* (26:4), pp. 381–396.
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.
Wood, R., and Bandura, A. 1989. "Social Cognitive Theory of Organizational Management," *Academy of Management Review* (14:3), pp. 361–384.
Zhang, L., and McDowell, W.C. 2009. "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords," *Journal of Internet Commerce* (8:3/4), pp. 180–197.