Self-efficacy in information security: Its influence on end users’ information security practice behavior

Hyeun-Suk Rhee, Cheongtag Kim, Young U. Ryu

Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT), USA
Department of Psychology, College of Social Science, Seoul National University, Seoul 151-742, Republic of Korea
School of Management, The University of Texas at Dallas, Richardson, TX 75083-0688, USA

Abstract

The ultimate success of information security depends on appropriate information security practice behaviors by the end users. Based on social cognitive theory, this study models and tests relationships among self-efficacy in information security, security practice behavior and motivation to strengthen security efforts. This study also explores antecedents to individuals’ self-efficacy beliefs in information security. Results provide support for the many hypothesized relationships. This study provides an initial step toward understanding of the applicability of social cognitive theory in a new domain of information security. The results suggest that simply listing what not to do and penalties associated with a wrong doing in the users’ information security policy alone will have a limited impact on effective implementation of security measures. The findings may help information security professionals design security awareness programs that more effectively increase the self-efficacy in information security.

1. Introduction

The increasing sophistication of information security threats and the ever-growing body of regulation has made information security a critical function within many sectors of business. Organizations devote significant resources to control threats imposed on their information security by securing their network using a combination of anti-virus/anti-spyware software, firewalls, intrusion detection and prevention systems, and content filtering software. However, this technical layer of defense to an organization’s security can succumb to human failure. A laptop is left carelessly behind in a public area such as an Internet cafe. Through manipulation of social engineering, naïve users often reveal their passwords and e-mail the company directory or other sensitive and classified information (Winkler and Hayden, 2005). American Express warned their customers of a phishing scheme that presents itself as a security measure by the company and asks for social security number, mother’s maiden name, and date of birth (Washkuch, 2006). Numerous other studies provide similar evidence (e.g., see Albrechtsen, 2007). For the past several years, malicious codes have been listed as one of dominating threats to information security (Power, 2008). Spyware is a type of malicious code intended to help an unauthorized entity break into users’ computers to divulge private information (Thompson, 2005). It is a deliberate software attack that imposes substantial risk to both individual and organizational information security. Its primary means of accessing a system is a user’s accidental or careless activation of a virus or a worm from an e-mail or a web site download (Whitman, 2003). Although the use of an anti-spyware program can effectively shield from such an attack, the
adoption rate of such software by end users is as low as 10 percent (Lee and Kozar, 2005). Even, an installed anti-spyware program can be outdated losing its effectiveness if its detection database is not regularly updated. An estimate reports that more than half of all security breaches are due to social engineering and end users’ careless behavior (Mackenzie, 2006).

These examples suggest that no matter how effective the technical layer of security, the security posture ultimately depends on appropriate end user behavior. However, information security has traditionally been treated as a technical problem, resulting in information security teams being staffed solely with technicians (Collette and Gentile, 2006). This skewed perspective of information security has resulted in overlooking the human factor issue, often referred to as the weakest point of a security chain (Angel, 1993). Concerns about this lack of consideration of the human factor in security programs have been raised in academic research (e.g., Bishop et al., 1997; Dhillon and Backhouse, 2000; Lee and Kozar, 2005; Spruit, 1995; Straub, 1990; Straub and Welke, 1998) as well as field studies (BERR, 2008; Ernst and Young, 2008). Some researchers in IS studied the human agent issue in the context of information security. For example, drawing upon criminology theory of general deterrence, Straub (1990) investigated the extent to which the severity and certainty of sanctions could influence computer abuse. Loch and Conger (1996) addressed attitudinal variables and social norms on ethical computer usage behavior. The main focus of these works is on how to deter an individual behavior, which is counterproductive to information security. The foundational assumption made by this line of research is that human agents have malicious intentions. Therefore, an external deterrent, such as punishment, needs to be introduced (Stanton et al., 2005). However, as evidenced above, there are many naïve user behaviors that are not intended but may cause detrimental effects on information security. In order to design a more effective security program for this group of users, understanding the factors that promote good end user behavior (i.e., control-enhancing behavior) is important. While there are some research efforts which address deterring bad end user behavior, little work has been done to promote good end user behavior in information security (Stanton et al., 2005; Whitman, 2003).

To address this need, we use social cognitive theory and explore its viability as a framework for understanding factors influencing end users’ control-enhancing behavior. Social cognitive theory is concerned with how perceptions of self-efficacy affect peoples’ motivation and action (Bandura, 1986). Self-efficacy is people’s belief in their abilities to mobilize the motivation, cognitive resources, and courses of action needed to exercise control over given events (Ozer and Bandura, 1990). The theory appears to be particularly well suited to studying individual behavior in the domain of information security, because self-regulated behavior in terms of using information and information systems seems critically important for ensuring information security. Self-efficacy has been argued as the most focal or pervasive mechanism of human agency which motivates and regulates individual behavior (Bandura and Jourden, 1991).

In this paper, we are particularly interested in exploring (1) the degree to which self-efficacy predicts current security practice behavior (i.e., the use of security technology and security conscious care behavior); (2) the extent to which self-efficacy predicts motivation (i.e., intentions to continue and to strengthen their information security practices); and (3) the extent to which self-efficacy is related to previous relevant experiences and perceived general controllability of information security threats.

Because of the importance of end-user behavior for overall security, understanding factors influencing control-enhancing behavior could provide helpful benefits for information security professionals, managers, and auditors with an interest in assessing the effectiveness of an information security program. Furthermore, such an understanding helps in designing more focused training programs. This paper also extends the current understanding of self-efficacy in a new domain, information security.

The paper is organized as follows. In the next section, we discuss the concept of self-efficacy in information security. This is followed by a description of the research model and its hypotheses. The research method is then presented, followed by a discussion of the analysis and results. Finally, we discuss our findings and suggest future research and managerial implications.

2. Conceptual background

2.1. Self-efficacy in information security

Self-efficacy is an important construct of social cognitive theory. It is a form of self-evaluation which is a proximal determinant of individual behavior (Bandura, 1986). People with a high level of self-efficacy have a stronger form of self conviction about their ability to mobilize motivation, cognitive resources, and courses of action needed to successfully execute a task (Stajkovic and Luthans, 1998). Self-efficacy influences the amount of effort, self regulation, and the initiation and persistence of coping efforts in the face of obstacles (Bandura, 1986). The empirical validity of this argument has been documented in a variety of research contexts (for reviews, see Bandura, 1997; Gecas, 1989; Gist, 1992).

Derived from the general concept of self-efficacy (SE), computer self-efficacy (CSE) was first discussed by Davis et al. (1989) and Gist et al. (1989). It is defined as an individual judgment of one’s capability to use a computer (Compeau and Higgins, 1995). CSE has been related to various end user computing behavior, such as software learning (e.g., Gist et al., 1989; Potosky, 2002), adoption of an information system (e.g., Compeau and Higgins, 1995; Ellen et al., 1991; Venkatesh et al., 2003), participation in systems development (Huntton and Beeler, 1997), as well as ethical computer usage (Kuo and Hsu, 2001). For a detailed review of CSE, see Compeau et al. (2006) and Marakas et al. (1998).

Self-efficacy researchers emphasize that, in order to increase the predictability of SE in performance, the domain specificity of SE should be considered. Bandura (1997) cautions against the use of contextless measures of SE. Consistent with this domain-specific argument, Marakas et al. (1998) explicate the concept of CSE by considering both the general and task specific levels. Task specific self-efficacy is related to the
efficacy belief in performing specific computer-related tasks within the domain of general computing. General computer self-efficacy is related to the efficacy belief across multiple computer application domains. The importance of considering domain specificity is further discussed by Agarwal et al. (2000) and more recently by Compeau et al. (2006) who argue that the “specific” concept remains relatively unexplored and it is necessary to be more precise in defining the domain of a study. They also argue that, in order to reflect the tasks being performed by users that form the basis of their SE judgments, the researcher needs to adapt the definition of CSE to the task and context of the study.

Following these suggestions, we adapt the general definition of CSE to be more specific to the information security context. Information security refers to the protection of information and the systems that use, store, and transmit information (Whitman and Mattord, 2003). The three key attributes of information security are confidentiality, integrity, and availability (Smith, 1989). Based on these attributes, therefore, we define self-efficacy in information security (SEIS) as a belief in one’s capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability.

2.2. The research model and hypotheses

Extending social cognitive theory to the information security context, we contend that individuals’ beliefs regarding their ability to protect their information and information systems may help explain current security practices and their intention to persist in the current efforts. Fig. 1 illustrates our research model. As shown in the figure, the general controllability perception and previous relevant experiences such as computer and Internet experience, and breach experience influence SEIS. In turn, SEIS is posited to influence current information security practice and intention of strengthening such efforts. Each of the constructs and its relationships is discussed below.

Security practice can be defined as individuals’ information security risk management behavior involving two aspects: the adoption of security technology and security conscious care behavior related to computer and Internet usage. The former is related to the use of security software and features such as anti-virus software, anti-spyware, and a pop-up blocking function. The latter refers to security compliance behavior in using a computer and the Internet, such as use of a strong password and frequency of making a backup copy. Both dimensions of security practice behavior are important for more effective risk management. Practicing security conscious care behavior together with the adoption of security software should lower vulnerability of information security further than adoption of security software alone.

The influence of CSE on computer usage and adoption has been demonstrated in prior studies. Research on CSE indicated that a significant positive relationship between users’ confidence in their computing skills and usage of information systems (Torkzadeh et al., 1999). For example, Internet self-efficacy has been shown to be a positive influencing factor for Internet usage (Eastin and LaRose, 2000) and use of an e-service (Hsu and Chiu, 2004). In a recent work by Woon et al. (2005), self-efficacy was found to be a significant predictor of using security features on home wireless networks. These studies suggest that variations in self-belief on their efficacy influence the use of information systems.

Furthermore, social cognitive theory also emphasizes the role of self-efficacy on behavior control over potentially threatening events. People with a strong sense of self-efficacy are likely focusing their attention on analyzing and formulating solutions to problems (Bandura and Jourden, 1991). Those with low self-efficacy tend to engage in fewer coping efforts (Gist, 1987). People keep their conduct in line with their personal standards through self-evaluative reaction (Bandura, 1986). Any discrepancies between behavior and personal standards generate self-reactive influences, which serve as motivators and guides for action designed to achieve desired results (Wood and Bandura, 1989). As have been concluded in the above studies, if self-efficacy belief positively influences subsequent behavior and acts upon self-regulatory behavior, we can expect that an individual with a high SEIS is likely to exercise direct control by using necessary security protection systems and following recommended security conscious behavior in order to protect his/her information and information systems. Therefore, the following hypotheses are proposed:

**Hypothesis 1a.** Individuals with higher SEIS use more security protection software.

**Hypothesis 1b.** Individuals with higher SEIS demonstrate more security conscious care behavior.

SE also determines the level of motivation, which is reflected in how much effort people exert and how long they persevere. Those with moderate to high SE tend to engage more frequently in task-related activities and persist longer in coping efforts. This leads to more mastery experience, which in turn enhances SE (Bandura, 1986). In the counseling context, Longo et al. (1992) showed that self-efficacy predicts clients’ intended and actual continuation in counseling. Similarly, in Zhang and Espinoza’s study (1998), the participants with higher CSE beliefs demonstrated greater desire to enroll in computing courses than those with lower CSE beliefs. CSE is expected to affect people’s intention toward future use of computers (Marakas et al., 1998). The influence of SE on effort/persistence is under-researched in MIS (Compeau et al., 2006). While a longitudinal study would be a good research method to examine the influence of SE on the actual persistence of an effort, based on the contention of the theory of planned behavior (Ajzen, 1991), we could argue that intention to exert effort is an indicator of future behavior. Consistent

---

Please cite this article in press as: Rhee H-S et al., Self-efficacy in information security: Its influence on end users’ information security practice behavior, Comput. Secur. (2009), doi:10.1016/j.cose.2009.05.008
with the findings of prior studies, we expect that those with higher SEIS will persist in their effort related to information security practices. Hypothesis 2 states this relationship.

**Hypothesis 2.** Individuals with higher SEIS have stronger intentions to exert more effort to strengthen their information security.

According to social cognitive theory, enactive mastery experience is a primary influencing source of efficacy belief. In general, successful experience increases SE and failure decreases it (Bandura, 1986). Often, in MIS research, enactive mastery is operationalized as past experience and has been measured by using self-reported items of years of computer use or familiarity with certain software. These studies consistently reported computer experience to have a positive influence in shaping CSE (Compeau and Higgins, 1995; Henry and Stone, 1994; Igbaria and Iivari, 1995; Marakas et al., 1998; Potosky, 2002; Staples et al., 1999; Taylor and Todd, 1995). Given that past experience positively affects belief in one’s capability to use a computer, it is reasonable to assume that prior experience with computers and the Internet also increases an individual’s belief in his ability to ensure information security. While successful experience fosters self-efficacy, prior failure weakens subsequent self-efficacy (Compeau and Higgins, 1995). In an information security context, negative experiences such as being a victim of cyber fraud or getting a virus would be considered as a failure. This failed experience may create self doubts and lower individuals’ judgments of their own capabilities (Wood and Bandura, 1989). Based on these arguments, the next two hypotheses posit the relationship between prior experience and SEIS.

**Hypothesis 3a.** The greater one’s experience with a computer and the Internet, the higher is the SEIS.

**Hypothesis 3b.** Security incidents lower SEIS.

In addition to prior experience, the belief in the general controllability of information security threats is also expected to influence formation of self-efficacy in information security. The perceived general controllability of information security threats can be defined as an individual’s belief in the availability of technological means and solutions to control information security threats in general. This perception is similar to the “strategy belief” concept, which refers to generalized expectancies about the extent to which certain means or causes are sufficient conditions for the production of outcomes (Skinner, 1995). According to social cognitive researchers (Bandura, 1986; Gurin and Brim, 1984), there are two aspects of the exercise of control. One aspect concerns the level of personal efficacy to effect changes by exerting efforts. The other aspect concerns the controllability of the problem domain. The former constitutes the personal side of the controllability. The latter relates to the level of constraints and opportunities to exercise personal efficacy. In fact, these two aspects are closely related. In a managerial decision-making context, Wood and Bandura (1989) showed that when an organization is viewed as controllable, perceived self-efficacy to manage the organization increases, whereas regarding it as uncontrollable undermines self-beliefs of managerial efficacy. This result suggests that self-efficacy level is limited by the perception on the controllability of determinants (Gist, 1992). Along this vein, in the domain of information security, we expect that an individual’s perception on the existence of means to control threats to information security in general influences efficacy belief at the personal level. Thus Hypothesis 4 is proposed as follows:

**Hypothesis 4.** As one perceives information security threats are controllable, their own self-efficacy on information security also increases.

### 3. Research method

#### 3.1. Subjects

A total of 415 graduate students majoring in business participated in this study. Respondents completed self-report questionnaires. Participations were voluntary. The sample consisted of 265 males and 150 females. The average age was 30.61 (s.d. = 6.27). They had 13 years of computer experience (s.d. = 4.56) and 8.7 years of Internet experience (s.d. = 2.43).

Some authors have noted potential problems related to the generalizability of findings of a study using student subjects to the real-world managers (e.g., Hughes and Gibson, 1991). However, we are not using students as surrogate for managers. Our research interest is in understanding the relationship between the end users’ self-efficacy and their behavior in the context of information security. All the participants are end users. Furthermore, over 70% of the participants are reported as currently working either in a full time or a part time job. The average working experience was 53 months. Therefore, we believe that the graduate students in this research context may serve as useful surrogates of the real-world end users of more direct interest.

#### 3.2. Instrument

The research model involves the seven constructs: computer/Internet experience, security breach incidents, general controllability, self-efficacy in information security, security practice—technology usage, security practice—security conscious care behavior, and intention to strengthen the efforts.

In order to develop a measure for self-efficacy in information security, we reviewed the existing measures in the IS literature (e.g., Compeau and Higgins, 1995; Harrison and Rainer, 1992). Items were adapted from a review of the existing measures to reflect tasks that relate to protecting information and information systems. For example, the participants were asked to rate their confidence on the items of ability of getting help for problems dealing with information security and ability of learning a variety of programs to protect their information and information systems. For computer and Internet experience, two items asking years of computer use and years of Internet use, and other two items...
asking self-reported literacy level on computer and Internet, were used. The questions asking if they have ever had a virus or spyware on their computers and if they have ever been a victim of cyber fraud such as phishing were selected to measure security breach experience. A three-item measure of general controllability was developed based on the conceptual framework of Skinner (1995).

In order to develop a measure for security practice behavior, we used information security guidelines published by various sources (e.g., AOL/NCSA, 2005; Rogers, 2004; Kuhn et al., 2002; Microsoft, 2006; NCSA, 2004). Based on the recommendations by vendors and security centers, questions to measure information security practice—technology aspects were selected. Some of the questions are related to the usage of major protection software such as firewall, encryption, anti-virus, and anti-spyware. Items asking usage of additional security features such as a spam filtering function and a pop-up window blocking function were also selected. The second aspect of information security practice is related to computer and Internet usage behavior. Items such as sending sensitive information via e-mail, frequency of making a backup copy of important files, use of file-sharing software, and use of a strong password (e.g., a combination of upper and lower cases, symbols, and numbers) were selected for this measure.

Behavioral intention measures individuals’ willingness to continue their efforts in order to strengthen their security measures. The four items created to measure this construct are their intentions to enforce stronger security procedures, to learn more about information security, to add additional security measures, and to buy more software to mitigate the threats.

SEIS, general controllability, behavioral intention, and two items asking literacy level of computer/Internet use were measured using a seven-point scale with strongly disagree (or very low) to strongly agree (or very high). In order to assess security practice behavior, categorical response items were given following the AOL/NCSA online safety study (AOL/NCSA, 2005) and the Microsoft home security guideline (Microsoft, 2006).

Once the item pools were created, we interviewed information security professionals, MIS faculty, and graduate students to clarify the wording of each item and to demonstrate content validity. Items that were reported to be ambiguous were deleted from the pool. This process was followed by a pilot test with a group of graduate students to ensure the initial reliability of the scales and the general mechanics of the questionnaire, such as instructions, completion time, and appropriate wording. Based on the responses received from this pilot study, the questionnaire was revised. This process resulted in eleven items for SEIS, three items for general controllability, four items for computer/Internet experience, three items for security breach experience, eight items for security practice—technology usage, eight items for security practice—care behavior, and four items for behavioral intention. The final set of items used for the study is presented in the Appendix. It is important to clarify the concept of information security to the study participants. Thus, in the survey, we provided a guiding definition of information security.

4. Analysis and results

The research model was tested using partial least squares (PLS). With this method, we first assess the measurement model including the reliability and discriminant validity of the measures. Then, we fit the structural model to test the hypothesized paths between latent constructs. LVPLS version 1.8 (Lohmoller, 1986) was used to fit the model. The standard errors and t statistics were estimated using a bootstrapping procedure with 1000 resampling.

4.1. Measurement model

To assess reliability of the three constructs in the research model (SEIS, general controllability, and intention), composite reliability is calculated. Similar to a Cronbach’s alpha internal consistency reliability estimate, a composite reliability of .7 or greater is considered acceptable (Hair et al., 1998). To evaluate discriminant and convergent validity assessment of the constructs, we examined the correlation of constructs, the factor loadings, and the average variance extracted. For discriminant validity, each indicator’s factor loadings should be higher on own construct than on other constructs in the model, and the average variance shared between the constructs and their indicators should be greater than the variance shared between the constructs themselves.

As reported in Table 1, all three constructs have adequate composite reliabilities. The general controllability construct has somewhat lower composite reliability but close to the acceptable cut off point. Therefore, we decided to keep all the three items. Also the square root of each construct average variance extracted (AVE) (diagonal elements in the correlation of constructs matrix) is greater than the correlation of the construct to other latent variables. The factor structure matrix shown in Table 2 demonstrates discriminant validity of the constructs. The measures of the three constructs satisfied the reliability and validity assessment. Thus, no changes to these constructs were made for testing the structural model.

The assessment of internal consistency for the two measures, computer/Internet experience and breach experience, is not performed, since the indicators of these two latent constructs are not reflective but formative. In such a case, the assessment of internal consistency measure is not needed (Chin, 1998, 2000). The composite scores for security practice variables were calculated based on the scheme developed by the authors together with two information security professionals.

<table>
<thead>
<tr>
<th>Construct</th>
<th>Composite Reliability</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. General controllability</td>
<td>0.697</td>
<td>0.773</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. SEIS</td>
<td>0.965</td>
<td>0.263</td>
<td>0.846</td>
<td></td>
</tr>
<tr>
<td>3. Intention to risk management</td>
<td>0.920</td>
<td>0.179</td>
<td>0.363</td>
<td>0.862</td>
</tr>
</tbody>
</table>

Note: The diagonal elements are AVEs and off-diagonal elements are the correlations among constructs.
4.2. Structural model

The structural model result is presented in Fig. 2. As stated in Hypothesis 1, SEIS significantly influenced users’ current security practice behavior regarding both the use of security software and security conscious care behavior. The path coefficients from SEIS to usage of security protection software and features (β = .565, t = 15.256, p < .001), and to care behavior (β = .368, t = 7.833, p < .001) were statistically significant. These results support Hypotheses 1a and 1b.

SEIS demonstrated a significant positive relationship with intention to strengthen security effort. Users with higher SEIS were more likely to exert high levels of effort to enhance information security (β = .353, t = 7.096, p < .001), thus supporting Hypothesis 2.

Hypotheses 3a and 3b assert that prior relevant experiences would influence formation of SEIS. Prior positive experience operationalized with computer/Internet years of use and self-reported literacy levels demonstrated a statistically significant positive relationship with SEIS (β = .603, t = 15.846, p < .001). In contrast, breach experience had a direct negative effect on SEIS (β = −.088, t = 2.133, p < .05). These results support Hypotheses 3a and 3b.

Hypothesis 4 states that perceived general controllability of information security threat positively influences SEIS. The path coefficient from general controllability perception to SEIS was statistically significant (β = .132, t = 2.616, p < .01).

In addition to the individual path test, another indication of model fitness can be evaluated by examining the explained variance (i.e., R²) in the endogenous constructs. To evaluate the full model, R² were calculated for self-efficacy in information security, security practice – technology, security practice – care behavior, and intention to strengthen the security effort. The model explained 44.5 percent of the variance in SEIS, 32 percent of the variance in information security practice – technology, 12.5 percent of the variance in information security practice – care behavior, and 13.5 percent of the variance in intention. Overall, the amount of variance explained by the model seems reasonable. SEIS influences both dimensions of end users’ information security practice and intention to strengthen security effort, resulting in the relatively modest R² values.

5. Discussion

Drawing upon social cognitive theory, this study extended the concept of self-efficacy in the context of information security and attempted to empirically test the influence of SEIS on users’ current information security risk management behavior and their intention to strengthen security efforts. We also studied variables influencing the formation of self-efficacy in information security.

The findings of this study provide support for the research model. Individuals with high SEIS used more security software and features. The adoption rate of the major security applications, as well as of additional security tools, was higher with high SEIS individuals. Furthermore, this group of users applied security updates/patches more often than individuals with low SEIS. Of more interest, SEIS influenced not only the use of security software but also the security care behavior related to computer/Internet usage. Individuals with high SEIS made backup copies of important files more frequently, used strong and multiple passwords for different online accounts, checked whether the site encrypts transferred data when sending their personal information, and did not share their computers with other people. In addition, users with high SEIS demonstrated their intention to continue and strengthen these security efforts. With all four items used to measure intention to persist their security efforts, a positive relationship was observed. Consistent with social cognitive perspective on computing behavior (e.g., Agarwal et al., 2000; Compeau and Higgins, 1995; Thatcher and Perrewe, 2002), these results suggest that self-efficacy is an important construct in determining individuals’ information security practices. The results of this study also corroborate the arguments made in the earlier studies that self-efficacy motivates an individual to exert effort continuously.

Hypotheses 3 and 4 address factors that could potentially influence users’ belief in self-efficacy. As shown in the result section, previous general computer/Internet experience influences SEIS. This implies that individuals with more experience in computer/Internet use will have higher levels of self-efficacy on tasks that require protecting their...
information and information systems. This efficacy judgment was also influenced by negative experience. Security incidents such as a virus infection, a spyware attack, and/or being a victim of cyber fraud significantly lowered self-efficacy. It seems that experiencing a direct security breach creates a negative emotional state such as anxiety or stress. This emotional state seems to debilitate individuals’ belief in their efficacy related to information security. The path from general controllability perception to self-efficacy was also significant. Individuals with stronger conviction on the availability of technology and procedures to control threats to information security in general demonstrated higher belief in their abilities to control threats to information security at the personal level. This result confirms the argument made in the earlier study: that personal efficacy level is influenced by belief in the controllability of the problem domain (i.e., in this case, controllability of information security threats in general).

Before discussing the implications of this study, it is important to consider the study’s limitations. In this study, we used self-reported data on years of computer and Internet use and on literacy level as a measure of prior mastery experience. Although prior experience has been consistently reported to be strongly correlated with CSE regardless of the type of measurement used to measure mastery (Compeau et al., 2006), the use of an alternative method of measuring this past experience would provide additional validity of this finding. These measures could include security training and the number of packages learned in the information security context. In addition to the mastery experience, people’s beliefs in their self-efficacy can also be strengthened by other variables such as vicarious learning and social persuasion. It may be valuable to explore the influence of other variables in shaping SEIS.

Social cognitive theory postulates the reciprocal nature of interaction among behavioral, personal, and environmental factors (Bandura, 1986). Individuals with high SEIS exercise information security practices either through adoption of security software or more security conscious care behavior. The practice of this control-enhancing behavior in turn may enhance self-efficacy belief in information security. Compared to other techniques, such as correlation and regression, the PLS analysis method would be useful in predicting causal relationships between the constructs (Compeau and Higgins, 1995). However, the ability to draw interpretations on the causality precedence of the constructs is limited since the data was gathered at the same point in time. Although cross-sectional survey data is widely used in many studies, certainly a longitudinal study incorporating temporal consideration would provide more insight on this causality interpretation.

In this study, we didn’t explicitly investigate how the CSE influences the development of SEIS. Understanding if there is any such an effect, what we call the specialization effect of CSE (i.e., influence of individuals’ beliefs about their capabilities to use computers in general to a self-efficacy belief related to a specific computing domain), would be an interesting extension. Related to this specialization effect, Agarwal et al. (2000) demonstrated general computer self-efficacy influence to a specific software self-efficacy (i.e., Windows 95) and in turn a carryover effect of this specific software self-efficacy to another software self-efficacy (i.e., Lotus 123). In this case, the notion of domain specificity is treated as a software level. However, as Compeau et al. (2006) addressed, equating a software package as a specific domain is a technology-focused approach. Given the increasing interchangeable functionalities between software, a task-driven domain-specific notion should be considered. Thus, future research addressing this specialization effect would be a valuable contribution to the field.

In spite of the limitations noted, the findings of this study provide several important implications for research and practice. This study provides an initial step toward understanding the applicability of social cognitive theory in a new domain of information security. Our results confirm that self-efficacy in information security is a meaningful construct in explaining users’ security practice behavior. From a practical perspective, the findings suggest that information security professionals need to be aware of the role of users’ belief on their efficacy in the information security domain on security practice behavior. They need to design training programs that more effectively foster this efficacy belief. The results of this study suggest that a training program that enhances SEIS can result in a higher level of security practice behavior in terms of both using technology and security conscious care behavior. Therefore, simply listing what not to do and penalties associated with a wrong doing in the users’ information security policy alone will have a limited impact on effective implementation of security measures. The results of this study also indicate that the general controllability perception of information security threats is positively associated with SEIS. Current security awareness training emphasizes the vulnerability related to the various information security threats and what should not be done in order to reduce such vulnerability (e.g., see Rezgui and Marks, 2008). Given the influence of general controllability perception to SEIS, awareness training should also communicate the existence of means and procedures to control information security threats.

In sum, organizations need to increase individual end users’ SEIS using various means. Hypothesis 3a signifies the importance of end users’ general computing literacy. Though not directly relevant to end users’ functional requirements, general knowledge in computer systems, application software, and Internet needs to be enhanced. Security technology understanding and security practice training, as a direct means to increase end users’ SEIS (Hypothesis 4), must be implemented and exercised repeatedly as security technology and required behavior change. Upon security breach incidents, organizations must further enhance their efforts by strengthening awareness training, security behavior modification education, and others as evidenced by the support of Hypothesis 3b.

6. Conclusions

This study has attempted to understand the factors influencing individuals’ information security promoting behavior. Our results demonstrate that self-efficacy in information
security does have substantial explanatory power regarding individuals’ information security practice behavior both in terms of technology use and security conscious care behavior. Moreover, SEIS also influences the intention to continue individuals’ security efforts. The weakness in user practice poses a bigger threat to an organization’s security than any other vulnerability in information security. Thus, the biggest challenge to information security professionals is knowing how to transform users from the biggest vulnerability into the first line of defense (Moore, 2003). By identifying more specific conditions which influence the formation of self-efficacy in information security, we may develop a more effective security program that organizations should be able to use to promote users’ security enhancing behavior.

Appendix.

A guiding definition of information security provided to the participants: Information security refers to protection of information and the systems that use, store, and transmit information. Therefore, information security is about safeguarding information from unauthorized disclosure, assuring information is shared only among authorized entities, preserving information in its original form, and assuring that the systems responsible for storing, processing, and transmitting information are always available when required. The objective of this survey is to study your perception and behavior on information security related to your information and computer (a laptop and/or a computer at home).

SEIS
- I feel confident handling virus infected files.
- I feel confident getting rid of spyware.
- I feel confident understanding terms/words relating to information security.
- I feel confident learning the method to protect my information and information system.
- I feel confident managing files in my computer.
- I feel confident setting the Web browser to different security levels.
- I feel confident using different programs to protect my information and information system.
- I feel confident learning advanced skills to protect my information and information system.
- I feel confident getting help for problems related to my information security.
- I feel confident using the user’s guide when help is needed to protect my information and information system.
- I feel confident updating security patches to the operating system.

General controllability
- In general, threats to information security are controllable.
- In general, technology is advanced enough to prevent information security threats.
- In general, there exist means to control information security threats.

Computer/Internet Experience
- How many years have you used computers? ________ years
- How many years have you used the Internet? ________ years
- How would you evaluate your computing literacy level?
- How would you evaluate your Internet literacy level?

Breach Experience (Please consider don’t know.)
1. Have you ever had a virus on your computer during the last two years?
   - yes
   - no
   - don’t know
2. Have you ever had spyware on your computer during the last two years?
   - yes
   - no
   - don’t know
3. Have you fallen a victim to a cyber fraud such as phishing during the last two years?
   - yes
   - no
   - don’t know

Behavioral intention
- I will enforce stronger security procedures.
- I will add additional security measures to protect my information and my information system.
- I will buy more software to mitigate impacts of information security breaches.
- I will learn more about how to strengthen my information security.

Security Practice—Technology Aspect
1. Do you currently have anti-virus software on your computer?
   - yes
   - no
   - I don’t know whether I have anti-virus software.
   - I don’t know what anti-virus software is.
2. If you have anti-virus software on your computer, how often do you update the virus database?
   - automatically or at least once a week
   - once a month
   - rarely
   - don’t know
3. Do you currently have anti-spyware software on your computer?
   - yes
   - no
   - I don’t know whether I have anti-spyware software.
   - I don’t know what anti-spyware software is.
4. Do you currently use a spam-filtering function in the email software on your computer?
   - yes
   - no
   - I don’t know whether I have a spam-filtering function.
   - I don’t know what the spam-filtering function is.
5. Do you currently use firewall on your computer or in your home network?
   - yes
   - no
   - I don’t know whether I have a firewall.
   - I don’t know what firewall is.
6. How often do you check and apply security updates/patches to the operating system and critical applications on your computer?
   - automatically or at least once a week
   - once a month
   - rarely
   - I don’t know how often I check.
   - I don’t know what security updates/patches are.
7. Do you use a pop-up window blocking function/tool on your computer?
   - yes
   - no
   - I don’t know whether I have a pop-up window blocking function/tool.
   - I don’t know what the pop-up window blocking function/tool is.
8. Do you use any form of wireless encryption feature in your wireless connection?
   - yes
   - no
   - I don’t know whether I use a wireless encryption feature.
   - I don’t know what the wireless encryption feature is.
   - I don’t have wireless connection.
Security Practice—Security Conscious Care Behavior

1. Do you use file-sharing software such as Kazaa and E-Donkey over Internet?
   - yes
   - no
   - I don’t know what file-sharing is.

2. When was the last time you made a backup copy of important files?
   - the last week
   - the last month
   - longer than a month ago
   - none within the last year

3. Do you store sensitive information, such as financial data and medical record, on your computer?
   - yes
   - no

4. Have you sent sensitive information (such as account numbers, passwords, and the social security number) via email?
   - yes
   - no

5. Do you use the same passwords for different online accounts?
   - (almost) always
   - often
   - rarely

6. When sending your personal information on the Internet, do you check whether the site encrypts transferred data?
   - yes
   - no

7. Do you share your computer with other people?
   - yes
   - no

8. Do you use password which is very difficult to guess such as a combination of upper and lower cases, symbols, and numbers?
   - yes
   - no

REFERENCES


Eastin MS, LaRose R. Internet self-efficacy and the psychology of the digital divide. Journal of Computer Mediated Communications 2000;6(1).


Whitman ME. Enemy at the gate: threats to information security. Communications of the ACM August 2003;46(8):91-5.


Hyeon-Suk Rhee is the Director of United Nations Asian Pacific Training Centre for Information and Communication Technology for Development (UN-APCİCT). Prior to UN-APCİCT, She served as a professor for two major universities in the United States of America: Georgia Tech and University of Texas at Dallas. She also served as Chief at the Information Technology Centre for Africa (ITCA). She received PhD from The Ohio State University where she also received several awards including the 1991 President Citation and Teaching Excellence Award. She has published over 30 research articles in various internationally recognized journals and made presentations at conferences in the ICT field. She has served as a chair for a number of national and international conferences.

Cheohtag Kim is a Professor of Psychology and Cognitive Science at the Seoul National University. He received B.A in psychology and M.A in psycholinguistics from Seoul National University, and Ph.D. in quantitative psychology from the Ohio State University. He began his academic career at Seoul National University in 1998 as an Assistant Professor and was promoted to Associate Professor in 2003 and Full Professor in 2008. He was the department chair from 2004 to 2006 and the director of Psychological Institute at Seoul National University from 2006 to 2007. He is the author of more than 30 publications on decision making, psychometrics, mathematical modeling of cognition in Psychological Methods, Journal of Personality and Social Psychology, Multivariate Behavioral Research, and several Korean Journals. His main interests are structural equation model, multilevel model, and test development.
Young U. Ryu is Associate Professor of Information Systems at the School of Management, The University of Texas at Dallas. He holds a Ph.D. degree in Management Science and Information Systems from the McCombs Graduate School of Business, The University of Texas at Austin. He has studied applications of data mining & artificial intelligence technologies and decision science methods to the modeling & analysis of information systems. He currently works on data separation as information classification and machine learning, computer security, and social network analysis.