http://dx.doi.org/10.14400/JDC.2014.12.2.27

정보보안 인식 교육의 효과에 대한 연구

임명성*
삼육대학교 경영학과*

Why Security Awareness Education is not Effective?

Myung-Seong Yim*
Dept. of Business Administration, Sahmyook University*

요 약 많은 조직들이 여전히 정보보안 수준을 향상시키기 위해 공식적/비공식적 통제 메커니즘(예. 정책, 절차, 조직 문화)의 향상에 상당한 노력을 쏟고 있으나, 이러한 메커니즘의 영향과 효과에 대한 연구는 아직 초기 수준이다. 보안 정책의 실행가능성을 높이기 위한 가장 확실한 방법 중 하나는 준수자들로 하여금 정책을 이해하고 필수요소로 받아들이게 하는 것이다. 하지만 조직 구성원들의 보안에 관한 지식 및 인지의 부족은 여전히 주요한 문제이다. 그동안 많은 연구에서 보안 지식과 인지를 높이기 위해 보안인식 교육의 수행을 주장하였으나 많은 연구에서 제시된 결과는 일관되지 않는다. 따라서 본 연구는 왜 보안인식 교육이 효과적이지 못한지 그 의문에 대한 해답을 찾기 위해 수행되었다.

주제어 : 보안 인식 교육, 정보 보안, 보안 대책

Abstract While organizations are making a considerable effort to leverage formal and informal control mechanisms (e.g., policies, procedures, organizational culture) to improve security, their impact and effectiveness is under scrutiny as employees seldom comply with information security procedures. The best way to ensure the viability of a security policy is to make sure users understand it and accept necessary precautions. From an organization's perspective, a lack of security knowledge and awareness on the part of employees is a major problem. However, previous studies suggest that effect of security awareness education is inconsistent. Thus, this study is to find the answer why security awareness education is not effective. Conclusions and implications are discussed.

Key Words : Security Awareness Education, Information Security, Security Countermeasures

1. Introduction

Information Security is a serious concern for both businesses and society as a whole [7]. The information security stakeholders are the biggest danger to an organization's IT(information technology) systems [31]. User noncompliance with information systems (IS) security policies is increasingly cited as a key IS security problem in organizations [24]. Therefore, security compliance is not possible without addressing the human issues of information security with proper awareness and training [31]. Information security

Received 4 December 2013, Revised 13 January 2014
Accepted 20 February 2014
Corresponding Author: Myung-Seong Yim(Sahmyook University)
Email: msyim@syu.ac.kr

ISSN: 1738-1916

awareness refers to the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly [18]. In general, awareness can be enhanced through training. Therefore, despite an increased perception of the importance of security awareness, there is a lack of adequate security awareness in practice [32]. From a organization's perspective, a lack of security knowledge and awareness on the part of employees is a major problem [4]. Information security threats can originate internally or externally by human or non-human perpetrators [4]. The success of information security depends on the effective behavior of users. Improving basic knowledge and judgment about sharing information can help prevent human errors and careless, but few companies have adequate information security training programs in place to improve security awareness [4]. However, previous studies suggest that effect of security awareness education is inconsistent. Thus, this study is to find the answer why security awareness education is not effective.

2. Literature Review

Security awareness education focus on raising employees' awareness of their responsibilities regarding their organizations' information resources and the consequences of abusing them, providing the necessary skills to help fulfill these responsibilities [9]. Thus, the purpose of a security awareness education is to increase awareness and facilitate understanding through training, they explicitly differentiate all terms at the end [31]. The concept of awareness is indicated as a critical factor for improving information security. Moreover, to successfully accomplish strong information security awareness programs, it is essential to have both a commitment to spend the time and effort into promoting the program. D'Arcy and Hovav (2007) suggest that educating users is an effective way to deter IS security problems. In addition, awareness education alerts users to known vulnerabilities and exploits. Security awareness educations are often implemented using newsletters, posters, trinkets, and web sites [4].

3. Research Model and Hypotheses

Based on the above-mentioned literature review and hypotheses, we proposed the research model depicted in Figure 1. H = hypothesis and the number following each H denotes the corresponding hypothesis number.

Security awareness programs reinforce acceptable usage guidelines and emphasize the potential consequences for misuse [8]. Such programs include ongoing efforts to (1) provide employees with general knowledge of the information security environment, along with the skills necessary to perform any required security procedures, (2) emphasize recent actions against employees for security policy violations, and (3) raise employee awareness of their responsibilities regarding organizational information resources [8]. This leads to the following hypotheses:

Hypothesis 1a. Security awareness program will negatively affect likelihood of information security breach.

Hypothesis 1b. Security awareness program will positively affect self efficacy.

Hypothesis 1c. Security awareness program will positively affect perceived severity.

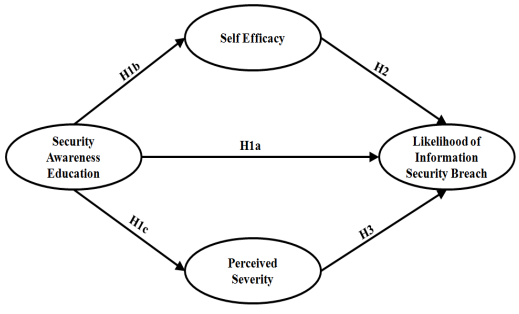
Self-efficacy refers to the belief in one's ability to organize and execute a particular course of action [2]. According to Bandura (1986), self-efficacy is thought to regulate behaviors by influencing the expected outcomes from the behavior. Thus,

Hypothesis 2. Self efficacy will negatively affect likelihood of information security breach.

Severity or certainty of formal sanction is important factors that determine the effectiveness of a sanction. Sanctions come from the General Deterrence Theory (GDT). Straub and Welke (1998) suggest that certainty, severity, and celerity of punishment affect people's decision on whether they commit a crime or not, thereby reducing the incidence of such behavior. According to Siponen et al. (2012), sanctions are explicit penalties imposed for certain forms of misconduct. They also suggest that the more forceful or effective the sanction, the greater the deterrence of undesirable behavior. Sanctions are effective if people feel that they will definitely be punished for their crime or anti-social acts and the punishment will be harsh [17]. D'Arcy et al. (2009) found that the severity of sanctions has a significant negative effect on users' intentions to commit computer abuse. Thus, the following hypothesis is formulated:

Hypothesis 3. Perceived severity will negatively affect likelihood of information security breach.

The resulting research model used in this paper is depicted in Figure 1. In this model, likelihood of information security breach is determined by three factors: security awareness education, self-efficacy, and perceived severity.



[Fig. 1] Proposed Model

〈Table 1〉 Descriptive Statistics of Survey Respondents

		Frequency	Ratio
Gender	Male	121	71.6
	Female	46	27.2
	Non-response	2	1.2
Age	18-24 yrs	3	1.8
	25-34 yrs	78	46.2
	35-44 yrs	74	43.8
	45-54 yrs	14	8.3
Education Level	High School	1	0.6
	Two-year college	15	9.5
	Bachelor's degree	114	67.5
	Master's degree	29	17.2
	Doctorial degree	5	3.0
Current Position	Technical	50	29.6
	Administrative/Clerical	51	30.2
	Professional Staff	19	11.2
	Middle Manager	45	29.6
	Senior Manager	1	0.6
	Other	3	1.8
	Total	169	100

4. Analysis

To test the research model proposed in this paper, this study uses a survey instrument for data collection. Self administered surveys that provide anonymity are a well suited method of inquiry since they can offer privacy to the respondent and are recommended where possibly sensitive answers are sought. In this research, we draw upon the well accepted methods and instruments used in recent security literature. To reduce problems with the reliability and validity of questionnaire, whenever possible it is advisable to adopt survey instruments from earlier validated studies.

4.1 Data Collection

200 questionnaires were distributed across five organizations in Korea. These organizations were selected largely due to their willingness to cooperate with this research due to the contacts of author. Since the survey was anonymous it was not possible to identify non-responders and encourage them to complete the questionnaires. In the end, 174 (87%)

〈Table 2〉 Exploratory Factor Analysis

	Factor				Communality
	1	2	3	4	
ATP1	**.827**	-.009	.075	.006	.647
ATP2	**.780**	.092	-.035	-.015	.678
ATP3	**.886**	.075	.007	-.007	.824
ATP4	**.859**	.001	-.017	-.017	.754
ATP5	**.916**	-.025	.083	-.016	.797
ATP6	**.926**	-.081	-.019	-.010	.840
ATP7	**.769**	-.015	-.140	.048	.651
PBC4	.002	**.908**	.042	.008	.814
PBC5	.005	**.924**	.034	-.016	.851
PBC6	.017	**.928**	.025	-.026	.867
PBC7	.009	**.871**	-.013	.027	.764
PBC8	-.012	**.867**	-.069	.051	.765
Likelihood_1	-.002	.049	-.027	**.972**	.931
Likelihood_2	-.013	.006	.014	**.951**	.915
PunCert	.057	-.090	**-.885**	.060	.776
PunSev	-.035	.011	**-.973**	.052	.913
PunCer	.033	.156	**-.574**	-.284	.559
Eigenvalue	6.658	3.572	2.200	1.653	
% of Variance	39.165	21.011	12.939	9.726	
Cumulative %	39.165	60.176	73.115	82.840	
KMO and Bartlett's Test					
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.				.839	
Bartlett's Test of Sphericity		Approx. Chi-Square		2877.879	
		Degree of Freedom		136	
		Significance		.000	

Extraction Method: Principal Axis Factoring.

Rotation Method: Oblimin with Kaiser Normalization.

surveys were returned, and 169 (84.5%) were deemed as complete and usable.

To establish factorial validity and reliability for our model, we followed validation procedures.

4.2 Factor Analysis

To examine the suitability of the data for factor analysis, Kaiser - Meyer - Oklin's (KMO) sampling adequacy test and Bartlett's sphericity test were performed. The results of this analysis appear in Table 2. The Bartlett's test of sphericity is significant with chi square=2877.879 ($p<0.001$), evaluation of the correlation matrix through the KMO was 0.839, which is above the recommended value of 0.6 [12]. Thus, factor analysis was appropriate for the data.

We conducted an exploratory factor analysis to examine the structure of the instrument using an Oblimin with Kaiser normalization to aid interpretation of the results. Results showed that all 17 items had the recommended .50 communalities and factor loading ranging from -0.574 to .972 without any cross loading onto other factors [12]. Variables that cross-load (load highly on two or more factors) are usually deleted [12]. Hence, there was no need to remove any item from the scale. The final scale has 4 factors, accounting for 82.840% of the variance. All factors had Eigenvalues greater than 1 showed an appropriate factor structure.

Table 3 represents the cross-loadings of measurement items on latent constructs. The loadings should be estimated at the true value of 0.70 [16]. In this study, all PLS factor loadings exceed the recommended level of 0.70. These loadings showed a

〈Table 3〉 PLS Cross-Loading Analysis

	Likelihood	Education	Self-Efficacy	Severity
Likelihood_1	**0.978**	-0.200	-0.009	-0.273
Likelihood_2	**0.982**	-0.228	-0.059	-0.315
ATP1	-0.160	**0.830**	0.185	0.193
ATP2	-0.198	**0.857**	0.291	0.314
ATP3	-0.202	**0.919**	0.293	0.305
ATP4	-0.211	**0.892**	0.221	0.292
ATP5	-0.206	**0.892**	0.201	0.210
ATP6	-0.218	**0.911**	0.164	0.299
ATP7	-0.147	**0.834**	0.201	0.370
PBC4	-0.023	0.227	**0.920**	0.149
PBC5	-0.042	0.241	**0.933**	0.183
PBC6	-0.063	0.259	**0.942**	0.186
PBC7	-0.027	0.235	**0.907**	0.169
PBC8	-0.006	0.226	**0.900**	0.214
PunCer	-0.410	0.313	0.261	**0.888**
PunCert	-0.136	0.288	0.052	**0.851**
PunSev	-0.141	0.250	0.140	**0.891**

clear discriminant and convergent validity for all constructs. Convergent validity can be satisfied if item loadings are 0.60 or higher [11]. Discriminant validity is demonstrated when an item more highly loads on its intended construct than on any other construct [11].

4.3 Common Method Bias Test

Because we relied on self-report questionnaire data, common-method bias (CMB) may be of concern. The problem of CMB has being given more and more attention in the field of psychology. Common Method Variance (CMV) refers to the amount of spurious correlations shared among variables in a study due to this common method used in collecting data, and examples include archival biases, key-informant prejudices or limitations, halo effects, social desirability, and acquiescence [1][20]. It stems from the systematic error variance shared among measured variables as a function of using the same method to collect all the data. Thus, CMV can be a potential source of bias in survey research.

One of the procedures used to test for evidence suggesting the presence, or absence of CMB in a data set is the Harman's one-factor test [23]. Harman's one-factor test is to examine whether CMB may have augmented relationships. In this test, all items are entered into an unrotated principal component analysis with a varimax rotation to determine whether a single factor emerges or a single factor accounts for the majority of the variance. In our test, we found four factors, the largest of which accounted for 39.165 percent of the variance. Since several factors, as opposed to one single factor, were identified, and as the first factor did not account for a large percentage of the variance, we were less concerned about potential problems associated with CMB.

In addition, we are examined the construct correlation matrix (reported in Table 4) to determine whether any constructs correlate extremely highly (more than .90) [22]. In this research, none of the constructs were so highly correlated. This finding also indicates that the level of CMB is minimal.

4.4 Reliability and Validity of Measurement Model

Measurement model assessment involves examining individual indicator reliability, internal consistency reliability, convergent validity, and discriminant validity

〈Table 4〉 Correlation Matrix and Discriminant Validity

	Likelihood	Education	Self-Efficacy	Severity
Likelihood	*0.980*			
Education	-0.219	*0.877*		
Self-Efficacy	-0.036	0.259	*0.921*	
Severity	-0.301	0.330	0.196	*0.877*
Cronbach's α	**0.959**	**0.950**	**0.955**	**0.860**
AVE	**0.960**	**0.769**	**0.847**	**0.769**
CR	**0.980**	**0.959**	**0.965**	**0.909**

Value on the diagonal is the square root of AVE.

[13].

In PLS, individual indicator reliability is assessed by examining the loadings of the measures with their respective construct [16]. In practice, a rule of thumb is to accept items with loadings of 0.7 or more, which implies that there is more shared variance between the construct and its measure than error variance [16]. In addition, items with loadings of less than 0.5 should be dropped [16]. The evidence of high individual item reliability is shown in Table 3. Item loadings ranged from 0.830 to 0.982.

The most common measure of internal consistency reliability is Cronbach's alpha, which provides an estimate for the reliability based on the indicator intercorrelations [15]. Evidence for a high degree of internal consistency was good with Cronbach′s alpha statistic exceeding 0.70 for internal consistency [21]. Cronbach′s alpha values ranged from 0.860 to 0.959 (see Table 4).

Although Cronbach′s alpha is the most widely applied index of internal consistency reliability, there are misconceptions. Cronbach's alpha is limited by the assumption that all indicators are equally reliable (tau-equivalence) [15], and efforts to maximize it can seriously compromise reliability [13]. Thus, it is more appropriate to apply a different measure to assess internal consistency reliability. The composite reliability (CR) takes into account that indicators have different loadings, and can be interpreted in the same way as Cronbach's alpha [15]. CR does not assume tau-equivalence, which prioritizes indicators according to their individual reliability [13]. CR is also superior to Cronbach's alpha since it uses the item loadings obtained within the nomological network [10]. An internal consistency reliability value above 0.7 in early stages of research and values above 0.8 or 0.9 in more advanced stages of research are regarded as satisfactory [21]. In our study, composite reliabilities of constructs ranged between 0.909 and 0.980, which is greater than the recommended threshold of 0.70.

Convergent validity shows the degree to which multiple attempts to measure the same concept are in agreement [1]. Convergent validity was assessed by looking at the average variance extracted (AVE) from the measures. The AVE value should exceed 0.50 to meet convergent validity. If AVE is less than 0.50, the variance due to measurement error is larger than the variance captured by the respective construct, and the validity of the individual indicators, as well as the construct, is questionable [10]. The AVE values for our measurements ranged from 0.769 to 0.960 while the threshold for acceptable convergent validity is 0.5.

AVE can be used to evaluate discriminant validity [10]. Discriminant validity is the degree to which measures of different concepts are distinct [1]. The square root of a given construct's AVE should be larger than any correlation of the given construct with any other construct in the model [5]. Correlations among constructs are reported on the off-diagonals and AVE squared roots are reported on the diagonal (see Table 4). Our results, depicted in Table 4, demonstrate strong discriminant validity.

〈Table 5〉 Hypotheses Test

Hypothesized Relationships	Path Coefficient	Standard Error	t-value	p value	Results
H1a. EducationgLikelihood	-0.146	0.087	-1.679	0.094	Not Support
H1b. EducationgSelf-Efficacy	0.259	0.074	3.508***	0.000	Support
H1c. EducationgSeverity	0.330	0.070	4.738***	0.000	Support
H2. Self-EfficacygLikelihood	0.053	0.081	0.656	0.512	Not Support
H3. SeveritygLikelihood	-0.263	0.092	-2.854**	0.005	Support

*p<0.05, **p<0.01, ***p<0.001 (two-tailed)

Construct validity is defined as the extent to which an operationalization measures the concept it is supposed to measure [1]. Without assessing construct validity, the results of theory testing may be ambiguous [1]. Convergent and discriminant validity are two aspects of construct validity [1]. Thus, we can conclude that the construct validity is obtained.

5. Assessment of Structural Model

Partial Least Squares (PLS), a component-based Structural Equation Modeling (SEM) technique, was used to examine the hypothesized paths in the model using the SmartPLS v2.0 M2 [25]. SmartPLS is a software application for the design of structural equation models (SEM) on a graphical user interface (GUI). These models can be measured with the method of PLS-analysis [14].

There are two reasons for choosing to use PLS in this study. First, PLS can be a powerful estimation method of analysis in case of small sample size, strong correlation among the items, missing data and no residual distribution assumption. Especially, sample size can be smaller, with a popular rule of thumb for robust PLS-SEM estimations suggesting that it be equal to the minimum sample size of ten times the maximum number of paths aiming at any construct in the outer model and inner model [3]. Although this rule of thumb does not take into account effect size, reliability, the number of indicators, and other factors known to affect power and can thus be misleading, it nevertheless provides a rough estimate of minimum sample size requirements [13]. Second, PLS path modeling focuses on the prediction of the dependent variables and thus PLS tries to maximize the explained variance (R2) of the dependent variables. Accordingly, PLS is more suited for predictive research models and theory building where prior theoretical knowledge is scare and the emphasis may be more on theory development.

The primary criterion for assessment of structural model is the coefficient of determination (R^2), which represents the amount of explained variance of each endogenous latent variable [13]. Adequate PLS models contain dependent variables with at least 10% of their variance explained [28]. In this research, R2 values ranged from 0.067 to 0.109 of the variance explained, thus demonstrating moderate predictive validity.

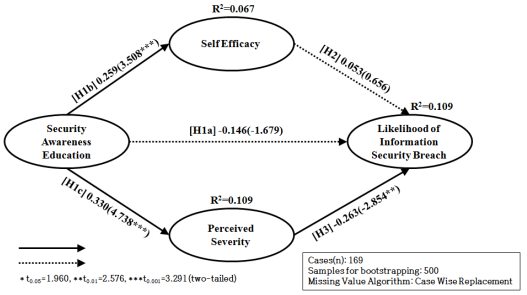
Next, we assessed the model's predictive validity by means of the cross-validated redundancy measure Q2 [13]. This technique is importance for structural model evaluation [5]. Q^2 can assess an individual construct's predictive relevance for the model by omitting selected inner model relationships [13]. We used the blindfolding to obtain cross-validated redundancy measures for each construct. In evaluating Q^2, a value greater than zero indicates the model has good predictive validity [26]. In this study, Q^2 was 0.0677.

Tenenhaus et al. (2005) proposed a global criterion for goodness-of-fit (GoF). This criterion is defined by the geometric mean of the average communality and the model's average R^2 value [13][33]. According to Wetzels et al.(2009), criteria for small, medium, and large effect sizes of GoF are 0.1, 0.25, and 0.36, respectively. We obtained a GoF value of 0.282, which

exceeds the cut-off value of 0.25 for medium effect size.

Standardized path coefficients provide evidence of the structural model's quality, and their significance should be assessed using Bootstrapping technique with 500 resamples [13].

Since each hypothesis corresponded to one such path, support for each hypothesis could be determined based on the sign (positive or negative) and statistical significance for its corresponding path (see Table 5) [17]. Security awareness education was not related to likelihood of information security breach (β=-0.146), thereby not supporting H1a. Security awareness education was positively related to self-efficacy (β =0.259, p<0.001). Therefore, H1b was supported. Security awareness program has positively effect on the perceived severity (β=0.330, p<0.001), thus H1c was supported. Self-efficacy was not related to likelihood of information security breach (β=0.053). Therefore, H2 was not supported. Perceived severity has positively effect on the likelihood of information security breach (β=-0.263, p<0.01), thereby supporting H3.



[Fig. 2] Results of PLS-SEM Analysis

6. Conclusions and Implications

The purpose of this study is to investigate the effect of the security awareness program on likelihood of information security breach. We found that security awareness program does not directly contribute to reduce the likelihood of information security breach. However, security awareness program reduces the likelihood of information security breach through perceived severity. This finding suggests that security awareness program has to play a role of deterrent countermeasure by reflecting certainty and severity of sanctions. D'Arcy et al. (2009) suggest that security awareness program deters illicit behaviors by reviewing current laws and by emphasizing the likelihood of apprehension and the corresponding penalties for violating the law. In a similar vein, Straub and Welke (1998) assert that security awareness program is initiated to convince potential abusers that the company is serious about security and will not take intentional breaches of this security lightly. Thus, security awareness programs that are running on the company must deliver the messages related to punishment to employees for decreasing the possibility of information security breach. The result can be a foundation for further theoretical research and practical applications in information security field.

Although we drew meaningful conclusions, this study has the following limitations. First, an important limitation of the study lies in sample size. In this study, 169 samples were used to assess the proposed model. However, more samples are required to yield more rigorous research results. Second, this research involves examining the relationships among two or more self-reported measures of constructs of interest. However, survey research based on same-source data can be problematic since same-respondent studies can face concerns about common method variance (CMV)-spurious correlation that arises from using the same method to measure the independent and dependent variables within a relationship [6] [27]. This means that individual's reports of their internal states are collected at the same time as their reports of their past behavior related to those internal states [19]. In this case, CMV may lead to wrong conclusions, the merits of research

designs that do not address CMV have been questioned [6]. In this study, in an attempt to avoid common method and respondent bias, we conducted the Harman's one-factor test to statistically detect or eliminate the presence CMV after the data have been collected. However, this statistical remedy has two problems. First, Harman's single-factor test is a post hoc statistical remedy [6]. Second, Harman's methods factor is the minimum standard or a final resource for addressing CMV because of its inability to detect moderate to small levels of CMV [6]. Consequently, it is difficult to assert that we are free from concern of CMV.

REFERENCES

[1] Bagozzi, R. P., Yi, Y., and Phillips, L. W., Assessing Construct Validity in Organizational Research, Administrative Science Quarterly, vol. 36, pp. 421-458, 1991.

[2] Bandura, A., Social Foundations of Thought and Action: A Social Cognitive Theory, Prentice hall, Englewood Cliffs, NJ., 1986.

[3] Barclay, D. W., Higgins, C. A., and Thompson, R., The Partial Least Squares Approach to Causal Modeling: Personal Computer Adoption and Use as Illustration, Technology Studies, vol. 2, no. 2, pp. 285 - 309, 1995.

[4] Chen, C. C., Shaw, R. S., and Yang, S. C., Mitigating Information Security Awareness: A Case Study of an Information Security Awareness System, Information Technology, Learning, and Performance Journal, vol. 24, no. 1, pp. 1-14, 2006.

[4] Chin, W. W., The Partial Least Squares Approach to Structural Equation Modeling. In G. A. Marcoulides (Ed.), Modern Methods for Business Research. Mahwah, New Jersey: Lawrence Erlbaum Associates, pp. 295 - 336, 1998.

[5] Craighead, C. W., Ketchen, D. J., Dunn, K. S., and Hult, T. M., Addressing Common Method Variance: Guidelines for Survey Research on Information Technology, Operations, and Supply Chain Management, IEEE Transactions on Engineering Management, vol. 58, no. 3, pp. 578-588, 2011.

[6] D'Arcy, J., and Herath, T., A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings, European Journal of Information Systems, vol. 20, pp. 643-658, 2011.

[7] D'Arcy, J., Hovav, A., and Galletta, D., User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, vol. 20, no. 1, pp. 79-98, 2009.

[8] D'Arcy, J., and Hovav, A., Deterring Internal Information Systems Misuse, Communications of the ACM, vol. 50, no. 10, pp. 113-144, 2007.

[9] Fornell, C., and Larcker, D. F., Evaluating Structural Equation Models with Unobservable and Measurement Error, Journal of Marketing Research, vol. 18, pp. 39-50, 1981.

[10] Gefen, D., and Straub, D., A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example, Communications of the Association for Information Systems, vol. 16, pp. 91-109, 2005.

[11] Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., Tatham, R. L., Multivariate Data Analysis, 6th eds., Pearson Education, Inc., Upper Saddle River, New Jersey, 2006.

[12] Hair, J. F., Sarstedt, M., Ringle, C. M., and Mena, J. A., An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research, Journal of the Academy of Marketing Science, vol. 40, pp. 414-433, 2012.

[13] Hansmann, K., and Ringle, C. M., SmartPLS Manual, Universität Hamburg, 2004.

[14] Henseler, J., Ringle, C. M., and Sinkovics, R. R., The Use of Partial Least Squares Path Modeling in International Marketing, Advances in International Marketing, vol. 20, pp. 277-319, 2009.

[15] Hulland, J., Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies, Strategic Management Journal, vol. 20, pp. 195-204, 1999.

[16] Kankanhalli, A., Teo, H. H., Tan, B. C. Y., and Wei, K. K., An Integrative Study of Information Systems Security Effectiveness, International Journal of Information Management, vol. 23, pp. 139-154, 2003.

[17] Kruger, H. A., and Kearney, W. D., A Prototype for Assessing Information Security Awareness, Computers & Security, vol. 25, pp. 289-296, 2006.

[18] Lindell, M. K., and Whitney, D. J., Accounting for Common Method Variance in Cross-Sectional Research Designs, Journal of Applied Psychology, vol. 86, no. 1, pp. 114-121, 2001.

[19] Malhotra, N. K., Kim, S. S., and Patil, A., Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research, Management Science, vol. 52, no. 12, pp. 1865-1883, 2006.

[20] Nunnally, J. C., and Bernstein, I. H., Psychometric Theory, 3rd eds. McGraw-Hill Inc., New York, 1994.

[21] Pavlou, P., Liang, H., and Xue, Y., Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective, MIS Quarterly, vol. 31, no. 1, pp. 105-136, 2007.

[22] Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P., Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies, Journal of Applied Psychology, vol. 88, no. 5, pp. 879-903, 2003.

[23] Puhakainen, P., and Siponen, M., Improving Employees' Compliance through Information Systems Security Training: An Action Research Study, MIS Quarterly, vol. 34, no. 4, pp. 757-778, 2010.

[24] Ringle, C. M., Wende, S., and Will, A., SmartPLS 2.0 (beta), Hamburg, Germany, 2005.

[25] Siponen, M., Vance, A., and Willison, R., New Insights into the Problem of Software Piracy: The Effects of Neutralization, Shame, and Moral Beliefs, Information & Management, vol. 49, pp. 334-341, 2012.

[26] Slater, S. F., and Atuahene-Gima, K., Conducting Survey Research in Strategic Management, vol. 1, Emerald Group Publishing Ltd., pp. 227-249, 2004.

[27] Sosik, J. J., Kahai, S. S., and Piovoso, M. J., Silver Bullet or Voodoo Statistics? A Primer for Using the Partial Least Squares Data Analytic Technique in Group and Organization research, Group and Organization Management, vol. 34, no. 1, pp. 5-36, 2009.

[28] Straub, D. W., and Welke, R. J., Coping with Systems Risk: Security Planning Models for Management Decision-Making, MIS Quarterly, vol. 22, no. 4, pp. 441-469, 1998.

[29] Tenenhaus, M., Vinzi, V. E., Chaterlin, Y. M., and Lauro, C., PLS Path Modeling, Computational Statistics & Data Analysis, vol. 48, no. 1, pp. 159-205, 2005.

[30] Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E., Investigating Information Security Awareness: Research and Practice Gaps, Information Security Journal: A Global Perspective, vol. 17, pp. 207-227, 2008a.

[31] Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E., Process-variance Models in Information Security Awareness Research, Information Management & Computer Security, vol. 16, no. 3, pp. 271-287, 2008b.

[32] Wetzels, M., Odekerken-Schröder, G., and van Oppen, C., Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration, MIS Quarterly, vol. 33, no. 1, pp. 177-195, 2009.

임 명 성(Yim, Myung-Seong)

- 2002년 2월 : 삼육대학교 경영정보학과(경영 학사)
- 2004년 2월 : 한국외국어대학교 경영정보대학원(경영학 석사)
- 2011년 8월 : 서강대학교 경영전문대학원(경영학 박사)
- 2011년 8월 ~ 2012년 2월 : 서강대학교 경영학부 대우교수
- 2012년 3월 ~ 현재 : 삼육대학교 경영학과 조교수
- 관심분야 : 정보보안, 서비스 시스템, 정보 심리학, 연구 방법론
- E-Mail : msyim@syu.ac.kr