Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, July 2021:3324- 3331

Research Article

The Effect of Establishing Security System for SMEs in ICT on Improving Security Awareness and Preventing Security Incidents

Eun-Joung Kim[1], Inchae Park*[2]

[1] Ph.D. student, Dept.Of Knowledge Service & Consulting, Hansung University, Seoul, Korea

*[2] Assistant professor, Division of Smart Management Engineering, Hansung University, Seoul, Korea

fogin99@hotmail.com[1], ipark@hansung.ac.kr*[2]

Corresponding author*: mobile Phone: +82-010-5485-4559, ipark@hansung.ac.kr

Abstract:

Background/Objectives: This study aims to present the effect of the establishment of a security system of SMEs in ICT on enhancing security awareness and preventing security incidents.

Methods/Statistical analysis: A research model was designed to analyze the effect of security system construction on security awareness and security incidents. Through theoretical literature survey, several variables of security training, security policy, and security infrastructure were derived for the security system. An empirical analysis was conducted using the structural equation, validity and reliability analysis with the collected 103 data for employees of SMEs in the ICT field through a questionnaire consisting of a 5-point Likert scale.

Findings: The establishment of a security system through periodic corporate security training, security policy, and security infrastructure has a statistically significant impact on improving organizational security awareness and preventing security incidents. Security training has shown a higher impact on security infrastructure and security policy than on improving security awareness. This is found to have a substantially high impact on security awareness and security incident prevention because security training is already performed in ICT of SMEs, and the introduced security infrastructure is operated by applying security policies.

Improvements/Applications: In order to improve the security awareness of SMEs in ICT, it is necessary to study various influential factors, such as the participation of management, and regulatory factors.

Keywords: Security incident prevention, Security awareness, Security training, Security policy, Security infrastructure

1. Introduction

According to the Ministry of SMEs(Small and Medium Enterprise), the five-year survival rate of domestic SMEs stood at 29.2%, far below the average survival rate of 41.7% in major OECD countries. France (48.2 percent) and the United Kingdom (43.6 percent) are significantly lower than those of OECD member countries. Among the reasons, the threat to survival has increased due to the leakage of key technologies and security incidents. Various preparations are needed for companies based on ICT technology to improve their security awareness and establish a security system to strengthen the security environment. It was intended to study how SME's based on ICT technology should prepare in terms of security to overcome chasm and strengthen their viability. In order to find out what to prepare to improve security awareness and prevent security incidents, we wanted to study the impact of the establishment of a SME's security system in ICT on improving organizational security awareness and preventing security incidents.

During security activities, security training importantly suggested the relationship between organizational security efforts and security interests of organizers in order to enhance compliance with information security[1,2]. In order to enhance the effectiveness of security training, activities to enhance the effectiveness of security training were emphasized according to whether or not security training was completed, contents, and level of security awareness of those subject to training[3]. In the case of appropriate security training and training on the organization's information resources, we also find that the information security compliance intentions of the members have a significant impact on education and training[4]. Within the same enterprise, the content of factors that affect performance in the growth process or the extent of their importance may vary. It investigated how management factors such as security policies, which are important to managers, are changing by stage of organizational growth[5,6]. It established step-by-step procedures for establishing SMEs' own industrial security activities and presented security activities that SMEs can realize as security measures to prevent industrial technology leakage. It was suggested that it is important to establish security policies by evaluating the importance of security control items for the industrial security of SMEs[7,8].

In order to establish a stable corporate security culture, the organization's security awareness, especially its vision and strategy based on executive entrepreneurship, must be preceded to positively affect its members' management performance and security awareness[9]. To find mechanisms to increase organizational commitment to information security compliance, we conducted research that security policy objectives setting positively affects organizational members' level of awareness of security-related fairness and fairness positively affects compliance objectives[10-12]. Although effective policy measures for corporate survival and growth are needed, it is necessary to overcome the difficulties of growth through internal competencies and strategies, it was studied to provide innovative technology support systems for each stage of growth to strengthen technological competitiveness in the long run[13-16].

2. Materials and Methods

2.1. Collecting data

This study conducted a survey of SMEs, laboratory executives and consultants in the ICT field to measure the impact of establishing a corporate security system on improving security awareness and preventing security incidents. The data were collected from 103 people through a questionnaire consisting of a 5-point Likert scale.

2.2. Research model

Based on theoretical literature survey, research model is designed and several variables are derived as shown in Figure 1.

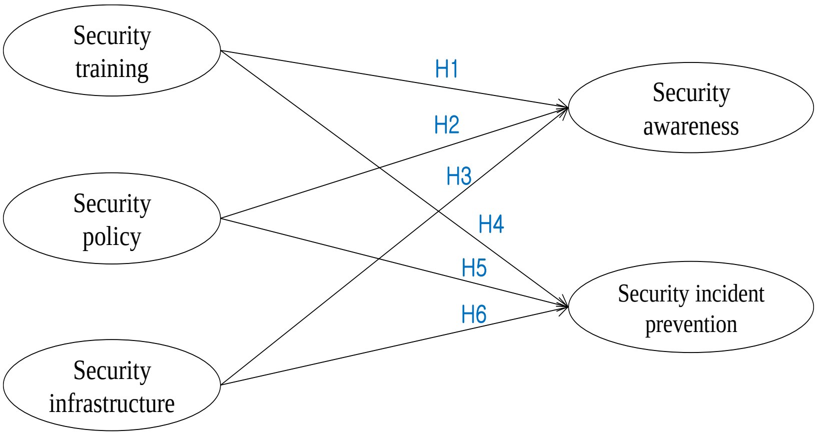

Figure 1. Research Model

2.3. Research Hypothesis

Based on the research model in [Figure 1], we establish a hypothesis about the relationship between security activities and security awareness improvement in the enterprise. In order to determine whether security awareness improvement by security activities is effective, not only security awareness improvement but also hypotheses on whether security activities affect the prevention of real security incidents.

H1: Security training will have a positive impact on improving organizational security awareness.

H2: Security policies will have a positive impact on improving organizational security awareness.

H3: Security infrastructure will have a positive impact on improving organizational security awareness.

H4: Security training will have a positive impact on the security incident prevention in businesses.

H5: Security policies will have a positive impact on the security incident prevention in businesses.

H6: The security infrastructure will have a positive impact on the security incident prevention in businesses.

2.4. Operational Definition of Variables

Based on relevant studies, this work identifies security training, security policies, and security infrastructure as variables as security factors for improving a firm's security awareness. We also want to identify the impact of this study by identifying security awareness and security incident prevention as variables. The variable definitions and questionnaire configurations of measurement variables are as shown in Table 1.

Table 1: Operational definition of variables

Measurement variables	Operational definitions	Configure Questionnaires
Security training	- Security training for members of the organization periodically based on security policies within the enterprise	7 questions
Security policy	- Security objectives to protect corporate assets and security policies to support administrative, physical and technical security	3 questions

Measurement variables	Operational definitions	Configure Questionnaires
Security infrastructure	- Security infrastructure built by introducing security products such as firewall, NAC, IDS, etc.	4 questions
Security awareness	- The voluntary behavior and sense of responsibility of the members of the organization for the security of the enterprise	5 questions
Security incident prevention	- Measures for responding to security incidents, such as leakage of core technologies and hacking incidents, and the effect of preventing security incidents	4 questions

3. Results and Discussion

3.1. Statistical analysis results

A structural equation model is utilized to verify the impact of the security system construction on improving security awareness and preventing security incidents. The research model examined the causal relationship between security training, security policy, and security infrastructure, which are independent variables, and security training, security policy, and security infrastructure with security incident prevention.

3.1.1. Validity and reliability analysis

Table 2 above shows the results of a review of the reliability and validity of the measurement data. The reliability is found to be 0.7 or higher by checking the Cronbach's α value of the latent variable. The concentration validity was found to be 0.5 or higher, the conceptual reliability (CR) was 0.7 or higher, and the standard variance extraction value (AVE) was 0.5 or higher, meeting the criteria. Furthermore, factor analysis determines that the KMO value is 0.879 and is suitable.

Table 2: Result of Validity and Reliability analysis

Evaluation items		Estimate	S.E	p	AVE	CR	Cronbach α
Security training (ET)	ET1	0.799			0.726	0.941	0.941
	ET2	0.828	0.086	***			
	ET3	0.834	0.102	***			
	ET4	0.865	0.113	***			
	ET5	0.894		***			
	ET6	0.916	0.094	***			
Security policy (EP)	EP1	0.832	0.109		0.826	0.959	0.916
	EP2	0.774		***			
	EP3	0.741	0.087	***			
	EP4	0.945	0.091				
	EP5	0.893	0.076				

Evaluation items		Estimate	S.E	p	AVE	CR	Cronbach α
Security infrastructure (ES)	ES1	0.891			0.769	0.930	0.878
	ES2	0.799	0.075	***			
	ES3	0.754	0.087	***			
	ES4	0.743		***			
Security awareness (SA)	EA1	0.833	0.093		0.845	0.942	0.900
	EA2	0.886	0.084	***			
	EA3	0.889	0.098	***			
Security incident prevention (SP)	ST1	0.924	0.103		0.841	0.940	0.890
	ST2	0.895	0.093	***			
	ST3	0.759	0.077	***			

*P< .05, **p< .01, ***p< .001

3.1.2. Correlation analysis

To evaluate the discriminant validity, mean variance extraction and comparative verification of correlation coefficients between variables were performed. As seen in Table 3, the square root value of the mean variance extraction (AVE) value of each component is found to be greater than the correlation coefficient value between the different vertical and horizontal component concepts, showing that discriminative validity is appropriate.

Table 3: Summary of Correlation Analysis Results

Model	Security training	Security policy	Security infrastructure
Security training	(0.853)		
Security policy	0.445	(0.908)	
Security infrastructure	0.428	0.79	(0.879)

( ) AVE square root

3.2. Hypothesis verification

3.2.1. Structural Equation Modeling

The structural model analysis results of estimating the path coefficient of the research model are as shown in Figure 2 and Table 4. For path coefficient analysis, standardization coefficients, t-value, p-value, and R^2 values were identified.

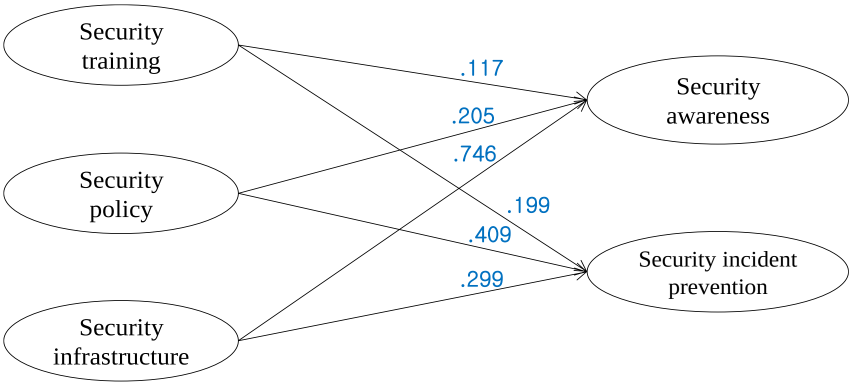

Figure 2. Structural Equation Modeling

Table 4: Summary of Hypothesis Tests

the Hypothesis	path-coefficient	t-value	p-value	VIF	R^2
H1(ET→SA)	0.117	2.088	0.037	accept	0.948
H2(EP→SA)	0.205	2.145	0.032	accept	
H3(ES→SA)	0.746	6.938	0.001	accept	
H4(ET→SP)	0.199	2.397	0.017	accept	0.612
H5(EP→SP)	0.409	2.992	0.003	accept	
H6(ES→SP)	0.299	2.228	0.026	accept	

First, security training will have a positive impact on improving organizational security awareness (β=0.117, p=0.037)

Second, security policies will have a positive impact on improving organizational security awareness (β=0.205, p=0.032).

Thirdly, the security infrastructure will have a positive impact on improving the organization's security awareness (β=0.746, p=0.001)

Fourth, security training will have a positive effect on the security incident prevention in the enterprise (β=0.199, p=0.017)

Fifth, security policies will have a positive effect on the security incident prevention in the enterprise (β=0.409, p=0.003).

Sixth, the security infrastructure will have a positive impact on the security incident prevention in the enterprise (β=0.299, p=0.026)

3.2.2. Analysis and Results

Hypothesis 1-4 are all statistically significant as p values are below 0.05, confirming that all of the research hypotheses have been adopted. Furthermore, we find that R^2 has a 0.948 explanatory power in security awareness and 0.612 in security incident prevention.

Looking at the results of the path coefficient analysis in detail, the security infrastructure was the highest with the standardization coefficient of 0.746, and it was shown that it affects security policies and security training. The prevention of security incidents by companies showed the highest security policy with a standardization factor of 0.409, followed by security infrastructure and security training.

As shown in the results, establishing a company's security system through security training, security policies, and security infrastructure has a significant impact on improving organizational security awareness and preventing corporate security incidents. However, there were many prior studies that believed that security training affected the improvement of security awareness in previous studies, [2,3,10], but the results of this study showed a higher impact on security infrastructure and security policies. This is found to have a substantially high impact on security awareness and security incident prevention because security training is already performed in ICT of SMEs, and the introduced security infrastructure is operated by applying security policies.

4. Conclusion

This study sought to find meaning in terms of security for companies to improve their survival rate in the increasingly complex era of the Fourth Industrial Revolution. In various aspects, such as security training, security policies, and security infrastructure, the government wanted to study whether establishing a security system could improve the security awareness of organizational members internally and externally prevent security incidents.

Research hypotheses and research models are presented based on prior research, and research hypotheses are validated through structural equation modeling. Empirical analysis found that corporate security awareness was positively affected by security training, security policy establishment, and security infrastructure introduction, and found that corporate security incident prevention was positively affected by security training, security policy establishment, and security infrastructure introduction. In particular, we prove that the introduction of security infrastructure applied with security policies plays an important role in improving security awareness and preventing security incidents for SMEs in ICT.

This results can be expected to help SMEs that want to find successful security-side risk management measures based on the establishment of a security system. However, it is hard to say that the findings represent the characteristics of SMEs in ICT. Therefore, because there may be differences between SMES in ICT, it is necessary to conduct various studies by changing different scope, elements of security activities, etc.In addition, it is expected that analysis studies will be conducted in addition to security training, security policies, and security infrastructure to establish an effective security system, including various factors such as management's participation.

5. Acknowledgment

This research was financially supported by Hansung University.

6. References

1. Hwang IH, Kim DJ, Kim TH, Kim JS. Effect of Security Culture on Security Compliance and Knowledge of Employees. Information Systems Review. 2016 Mar;18(1):1-23.
2. Baek MJ, & Sohn SH. A study on the effect of information security awareness and behavior on the information security performance in small and medium sized organization. Asia Pacific Journal of Small Business. 2011 Jun;33(2):113-132.

3. Park SR, Lee HS, Park HA. Effect of the frequency of security training on the enhancement of employees' consciousness of security in terms of technology protection. Korean Journal of Industrial Security. 2020;10(1):55-79.
4. Noh MS, Lee SY. Explaining Industrial Security of SMEs in Korea: An Ordered Logit Analysis. Korean Public Administration Review. 2010 Sep;44(3):239-259.
5. Lee CW, Seoh CS. A exploratory study on the importance of managerial factors of Korean Ventures through organizational stage. Asia Pacific Journal of Small Business. 2006 Jun;28(2):3-29.
6. Kwak DC, Joo YH, Cho BH. A study on influential factors of survival rates: Focused on youth start-ups. Asia Pacific Journal of Small Business. 2016 Dec;38(4):77-94.
7. Lee, MH. A Study on the Developmental Activation Plan of Local Medium and Small Firms-Focussed on Industrial Security. Korea Local Government Studies. 2013;15(2):141-159.
8. Gong BW. The situation and security measures of industrial technology security management of SMEs. J. Korean Soc. Priv. Secur. 2019;18(1):1-26.
9. Kim KW, Kim MS. An Empirical Analysis of Influence of Corporate Entrepreneurship on Business Performance from the Viewpoint of SMEs' Growth. Asia-Pacific Journal of Business Venturing and Entrepreneurship. 2017;12(5):13-28.
10. Han JY, Kim YJ. Investigating of psychological factors affecting information security compliance intention: Convergent approach to information security and organizational citizenship behavior. Journal of Digital Convergence. 2015 Aug;13(8):133-144.
11. Hwang IH, Kim SW. A Study on the Influence of Organizational Information Security Goal Setting and Justice on Security Policy Compliance Intention. Journal of Digital Convergence. 2018;16(2):117-126.
12. Kim H, Eom SS, Kwon HJ. The impact of the introduction of information security solutions by public organizations on the improvement of information security level. Convergence Security Journal. 2017 Dec;17(5):19-25.
13. Park JB, Kim JH, Yang HB. Factors Affecting the Growth of Corporate Start-ups Focused on Sales Performance and Job Creation. The Asia Pacific journal of Small Business. 2010 Sep;32(3):109-128.
14. Shim YS, Seo JH. A Study on Entrepreneurial Orientation and Startup Performance: Mediating Effect of Strategic Orientation. International Journal of Emerging Multidisciplinary Research. 2019 Dec;3(4):32-40.
15. Oh DH, Kwon YM. Impact on the level of security education by privacy policy of smaller enterprises. Journal of Korean Marketing Association. 2014;1(1):63-64.
16. Hayden L. People-centric security: transforming your enterprise security culture. McGraw Hill Professional. 2015. p. 35.