Vulnerability and Information Security Investment: An Empirical Analysis of Ministries in Korea

SANGMIN PARK, TAE-SUNG KIM

***Abstract*—**This paper focuses on the relation between information security workforce and information security investment budgets. Organizations are currently interconnected via platforms, such as inter-organizational networks, because their needs have increased with regard to supporting Big Data and Cloud services. Studies define the relation between information security investment measures and vulnerability as a network linkage. However, measuring vulnerability as a network linkage is difficult because organizations presently have good inter-organizational network connections. To address these issues, we propose that vulnerability be measured as the size of an information security workforce (i.e., number of employees). In so doing, we identify the relation between vulnerability and information security investment. The results of this study can be used as bases for relating information security investments to a fixed number of information security investments. We believe the application of our findings will afford organizations a competitive advantage in information security investment and effective decision making.

***Keywords*—**government organization, information security economics, security investment vulnerability, vulnerability measurement.

I. Introduction

THIS document is concerned with the relation between vulnerability and information security. Gordon and Loeb (2002) theoretically analyzed vulnerability and information security investments and Tanaka, Matsuura, and Sudoh (2005) empirically examined vulnerability and information security investment in e-local governments in Japan.

We focus on the relation between information security investment budgets and the vulnerability presented by the size of a security workforce to support effective information security investment decision making. Decision making on information security investment is generally conducted before risk management and analysis. Takacs and Edit (2011) and Toma, Chirita, and Sarpe (2011) argue that risk analysis requires considerable time and effort. Thus, the current work proposes an effective decision making method for information security investment, in which minor management factors are used. These factors include fixed sizes of organizational workforces and information security workforces. Our empirical analysis is based on the ministries, municipal governments, and metropolitan cities in Korea.

The rest of the paper is organized as follows. Section 2 presents the literature review. In Section 3, we propose the method for analyzing information security investment and vulnerability in government organizations. In Section 4, we discuss our research results, derived by linear regression. Section 5 provides the conclusion and discussion of future works.

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0025512). This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2013S1A5A2A01017485). This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the "Employment Contract based Master's Degree Program for Information Security" supervised by the KISA (Korea Internet Security Agency) (H2101-13-1001).

Sangmin Park is with the Department of Information Security Management of Chungbuk National University, Chungbuk, South Korea (e-mail: parks@chungbuk.ac.kr).

Tae-Sung Kim is with the Department of Management Information Systems (Big Data Service Model Optimization Team, BK21 Plus), Chungbuk National University, 12 Gaeshin-dong, Heungduk-gu, Cheongju, Chungbuk 361-763, South Korea (corresponding author.. phone: +82-43-261-3343; fax: +82-43-273-2355; e-mail: kimts@cbnu.ac.kr).

II. Literature Review

Research on the economic issues that arise from information security has been a recent phenomenon [15]. Information security studies are divided into three streams: technical, behavioral, and economic [6]. In the early 2000s, information security investment studies progressed not only technically and behaviorally, but also in terms of economics (e.g., Anderson (2001), Camp and Wolfram (2000), Gordon and Loeb (2002), Tanaka, Matsuura and Sudoh (2005)) [14].

The information security economics studies that we review are those of Gordon and Loeb (2002), Tanaka, Matsuura, and Sudoh (2005), and Shim.

Gordon and Loeb (2002) theoretically investigated the relationship between vulnerability and information security investment on the basis of certain assumptions related to security breach probability functions. The authors found that organizations may either increase security investment or initially increase and then decrease such investment.

For Class I (i.e., companies with increasing security investment), security breach probability functions exhibit a positive linear relationship with vulnerability level; for Class II (i.e., companies with initially increasing and then decreasing security investment), the breach probability functions of information security generate a very low reduction in expected loss for low and very high vulnerability levels. For such levels, an increase in security investment only moderately reduces

expected loss. At medium-to-high vulnerability, however, an increase in security investment effectively minimizes expected loss. Under Class II, low or very high vulnerability results in minimal expected benefits from security investment. Therefore, the optimal information security investment is initially an increasing function before it becomes a decreasing function of vulnerability level. According to our results, the optimal amount for investment in information security should not exceed 37% ($\approx 1/e$).

Through an empirical study of municipal governments in Japan, Tanaka, Matsuura, and Sudoh (2005) revealed the link between vulnerability as a network sharing level and information security investment. The authors assumed that the vulnerability level of a firm that uses a closed LAN is low given that the firm's network is closed and no information is shared with other entities. Firms with this type of network, therefore, usually have strong control over potential vulnerabilities and do not need to worry much about intrusions from outside attackers through a network.

Firms that rely on regional networks have medium-to-high exposure to vulnerabilities because they share information with authorized users through dedicated networks. Given that information sharing in these companies is restricted to certain operational boundaries, they can manage the vulnerability of information security to a satisfactory extent. Finally, the vulnerability level of firms connected through inter-organizational networks can be regarded as very high (Figure. 2).

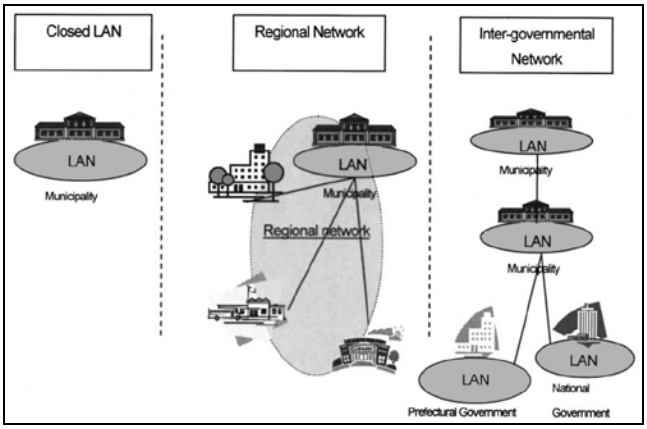

Figure. 2. Three network types as a vulnerability leveling (Adopted from Tanaka, Matsuura, and Sudoh (2005))

Shim used 2007 and 2008 data from the Korean Information Security Surveys conducted by the Korea Internet and Security Agency and argue that firms managing highly confidential information increase their level of security investments as vulnerability increases, whereas firms with less confidential information first increase then decrease investment as vulnerability rises [15].

Shim used private customer information as a proxy for confidential information and divided the data on the basis of whether a firm collects private information from customers through its website. This categorization reflects the assumption that firms collect private information units.

III. RESEARCH METHODOLOGY

The present research expands previous studies by conducting a theoretical analysis of Gordon and Loeb's (2002) study, as well as an empirical analysis of Tanaka, Matsuura, and Sudoh (2005) and Shim's frameworks. We retain the main concepts of Gordon and Loeb (2002) and Tanaka, Matsuura, and Sudoh (2005), and then use the research frameworks of Tanaka, Matsuura, and Sudoh (2005) and Shim.

Organizations are currently interconnected through platforms, such as inter-organizational networks, more popularly known as the Internet. Zarei (2011) states that the Internet is a public network of computers that facilitates data/information flow and to which users have unrestricted access. Given this backdrop, companies have exhibited increasing demand for technologies that enable support for Big Data and Cloud services [4].

In this context, Korean governments presented "Government 3.0," a new government paradigm that comprises three domains: a service government, a transparent government, and a competent government [9]. All the government organizations of Korea avail of the services of the National Computing and Information Agency, which is a government integrated data center that can support high-quality and high-security IT operations [7].

Given these circumstances, the research of Tanaka, Matsuura, and Sudoh (2005) is difficult to apply to the context of Korean governmental organizations. First, measuring vulnerability level on the basis of network linkage may be unsuitable under the conditions that characterize Korean government networks. Second, collecting data on network connection status is difficult to accomplish because such data are classified. These issues have given rise to concerns over effective support for decision making.

In this research, we identify the relationship between vulnerability and information security investment with a sample of 17 ministries. This study also aims to determine a usable measurement for vulnerability level.

A. Variable Selection

As previously stated, data are collected from 17 ministries. In 2000, e-government projects were developed to realize more citizen-centered Japanese [18] and Korean governments; this goal is expected to be accomplished by initiating national, people-centered government projects, such as Government 3.0, an endeavor that has been in place in Korea since 2013 [10].

Information security is an important national issue. The Big Data project in Korea emphasizes the importance of information security [16]. We believe such significance is growing and therefore devote research to defining the relationship between information security investment and vulnerability. In particular, we intend to elucidate this relationship in terms of effective information security investment by Korean government organizations.

Government organizations and the 17 ministries have various divisions [7]. We exclude branch organizations of governmental organizations to manage the scope of the

research. Most government organizations have information security divisions in their headquarters.

The variable used, information security workforce, is defined by the National Institute of Standards and Technology (NIST) in 1998 as follows: "An IT security professional is one who integrates the principles of the IT security field in a forward-looking manner to keep up with technology trends and their evolving security implications" [12]. We apply this definition, regarding information security workforce as the group of people accomplishing information security work in their organizations. We exclude employees whose responsibilities exceed the job description and its boundaries, such as staff working on national security project, security policy, or information security administration. Public servants who belong to an information security department but who do not render information security work are also excluded from the definition.

B. Vulnerability Measurement, Variables, and Data

Mnerie, Slavich, Crisan, Herman, and Untaru (2011) argue that no system where potential injury or illness exists is totally excluded from danger; "residual" risk is a constant problem because of the unpredictability of human action and/or the malfunctioning of technical systems.

Budgets are represented as the monetary figure required to achieve a presented policy; a budget constitutes a specific plan for achieving that policy [8]. That is, all activities needed to execute the policy are presented in the budget. Confirming the realization of policies on government information security policy necessitates a clear-cut delineation of information security budgets.

The total information technology budget allotted to a firm's information security activities was used as a dependent variable in Gordon, Loeb, Lucyshyn, and Richardson (2004).

Information security budgets, however, are carefully supervised and are confidential. Such confidentiality prevents access to this information. To resolve this problem, we calculate the information budget and information security budget on the basis of the budget for annual expenditures in 2012. In the calculation, we use the information security budget ratio as a measure.

Gordon and Loeb (2002) argue that the level of information security investment differs depending on the characteristics of each organization's investment preferences. Information security characteristics are categorized as Class I, increasing security investment, and Class II, initially increasing and then decreasing security investment. We assume that the organizations in Korea belong to Class II because the information security investment in the country is characterized by fluctuations; that is, it has repeatedly increased and decreased [11]. Treating the organizations as Class II types enables more realistic research.

To measure vulnerability levels, we propose a vulnerability level index (VLI), which is calculated as follows:

$$VLI_a = ISW_a / FOW_a, \qquad (1)$$

where

※ ISW: the number of employees in the information security workforce of an organization;

※ FOW: a fixed size (population) of an organizational workforce.

Calculating the VLI of each organization entails computing the mean of the VLI and the standard deviation of an entire organizational set. We assume that the VLI follows a nominal distribution. The VLI level is determined by referring to empirical research (mean $\pm$ 3σ) in defining outliers.

The vulnerability criteria used are as follows (Fig. 1):

- Medium: mean – 1σ < VLI_a < mean + 1σ
- Low: VLI_a > mean +1σ
- High: VLI_a < mean – 1σ

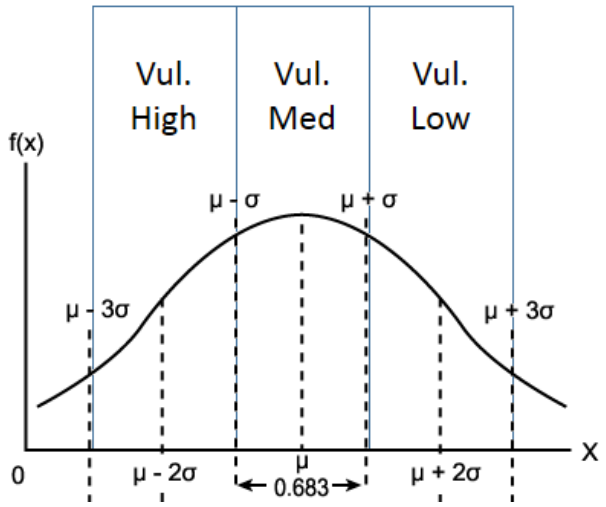

Fig. 1 Proposed measurement of vulnerability level (modified image from http://www.aistudy.co.kr/math/normal_lee.htm)

We determine organizational size from a fixed number of organizations.

If an organization is large, the budget for operations is also large. An issue that requires addressing is that a certain bias occurs in determining organizational size. We eliminate the possibility of such bias, but organizational size remains a variable necessary for guaranteeing the reliability of the study.

Organizational type is a variable intended to classify specific groups, such as ministries, municipal governments, and metropolitan cities. The organizations share common ground, but essentially differ in terms of operations. We therefore analyze the intensity of the relationship between vulnerability and information security investment, and then compare the characteristics of the organizations. This goal requires an organization-type variable on Table. 1.

Table. 1. Used Variables

Variable	Measure	Description
Dependent Variable	Information security investment budget	Normalized budget by organizational size; 2012 budget for annual information expenditure [15]
Independent Variable	Vulnerability level	Information security workforce; collected from each organization's homepage
	Organizational size	Fixed number of government organizations [7] for measuring vulnerability

The Korean government has 17 ministries with a fixed workforce population, information security workforce population, and 2012 budgets for annual information expenditure. The workforce data are collected from the ministries' homepages and the budgets are taken from the 2012 Public Service Divisional Manual Revenue and Expenditure Budget [14]. The data on the ministries are presented in Table. 2. More information about Korean government is on Appendix. 1.

Table. 2. Ministry of Korean government

Num.	Ministry
1	Ministry of Strategy and Finance
2	Ministry of Security and Public Administration
3	Ministry of Agriculture, Food, and Rural Affairs
4	Ministry of Science, ICT, and Future Planning
5	Ministry of Education
6	Ministry of Justice
7	Ministry of National Defense
8	Ministry of Culture, Sports, and Tourism
9	Ministry of Trade, Industry, and Energy
10	Ministry of Health and Welfare
11	Ministry of Employment and Labor
12	Ministry of Environment
13	Ministry of Land, Infrastructures, and Transport
14	Ministry of Oceans and Fisheries
15	Ministry of Foreign Affairs
16	Ministry of Gender Equality and Family
17	Ministry of Unification

C. Hypotheses

Gordon and Loeb (2002) contend that organizations are rapidly infusing investments into information security activities, especially those with medium-to-high vulnerability levels; organizations characterized by low and very low vulnerability do not engage in security investment activities [6].

On the basis of Gordon and Loeb's (2002) argument, we formulate the following hypotheses:

H1. When the size of the information security workforce in an organization is smaller than the average size of information security workforces (VLI_a > mean), the information security budget is low.

H2. When the size of the information security workforce in an organization is larger than the average size of information security workforces (VLI_a > mean), the information security budget is low.

H3. When the size of the information security workforce in an organization presents medium vulnerability (mean – 1σ < VLI_a< mean + 1σ), the information security budget is high.

We classify the ministries into three groups and verify each group's relationship in terms of information security investment and vulnerability. The groups are G1, G2, and G3, which correspond to H1, H2, and H3, respectively (Table.3).

G1: a group of ministries characterized by high vulnerability (classified as G1 in VLI_a < mean – 1σ).

G2: A group of ministries with medium vulnerability (classified as G2 in mean – 1σ < VLI_a < mean + 1σ).

G3: a group of ministries with low vulnerability (classified as G3 in VLI_a > mean +1σ).

Table. 3. Ministry's groups and hypotheses

	Vulnerability Level	Criteria	Hypothesis
G1	High	VLI_a < mean – 1σ	H1
G2	Medium	mean – 1σ < VLI_a < mean + 1σ	H2
G3	Low	VLI_a > mean +1σ	H3

IV. ANALYSIS RESULTS

The regression equation used is

$$\ln (BIAE) = \alpha + \beta_1(ISW) + \beta_2(FOW) + \gamma \text{ , } (2)$$

where

※BIAE is the 2012 budget for annual information expenditure;

※ISW is an information security workforce in an organization;

※FOW is a fixed size of organizational workforce.

Deducting information security investment is a complicated process because security investment is distributed across many cost indexes [17]. The Korean budget system is operated and organized as an information security budget, which is included in the information budget. Concerns as to whether such budget is recorded arise.

We use BIAE as a proxy value for information security investment. As previously stated, we divide the ministries into three groups using the VLI. We conduct linear regression analysis on each group to ascertain the relationship between information security investment and vulnerability.

Although our sample comprises 17 ministries, we are able to derive data only from 16's because Ministry of Unifications was not support their budget information on public.

As a result, we cannot examine G1 and G3 because these constitute small samples for regression analysis and we cannot derive significant results from the relatively large sample of G2 (Table. 4).

Table. 4. Regression analysis results (first analysis)

	β_1[ISW] (t-value)	β_2[FOW] (t-value)	γ	Adjusted R^2	N
All	-.71 (–.877)	.004 (.682)	19.857	.387	16
G1	.092 (–)	.003 (–)	20.656	-	3
G2	.09 (.474)	.003 (1.262)	19.95	.011	11
G3	.175 (–)	-	18.419	-	2

Significance level ***99.9%, **95%, *90%, ( ): t-value.

To solve this problem, we perform regression analysis again using the entire sample without the division into three groups and use the backward input method for regression analysis (Table.5).

Table. 5. Regression analysis results (second analysis)

	β_1[ISW] (t-value)	β_2[FOW] (t-value)	γ	Adjusted R^2	N
All	-	.004** (3.299)	19.521	.397	16

Significance level ***99.9%, **95%, *90%, ( ): t-value.

The analysis result shows that FOW generates a significant coefficient (3.299) and the adjusted R^2 is 0.397. The regression equation is

$$\ln(\text{BIAE}) = 19.521 + 0.004\ (\text{FOW}). \quad (3)$$

As indicated in the correlation analysis results in Table 6, BIAE is significantly related to FOW (.661). We therefore conclude that FOW and BIAE are significantly related, but that FOW exerts a nonsignificant effect on BIAE.

Table. 6. Results on the correlation between FOW and BIAE

		FOW	BIAE
FOW	Pearson correlation	1	.661**
	Sig (2-tailed)	-	.005
	N	16	16

Significance level ***99.9%, **95%, *90%

V. Conclusion and Future Works

Gordon and Loeb (2002) theoretically studied the relationship between information security investment and vulnerability. In an empirical study, Tanaka, Matsuura, and Sudoh (2005) and Shim defined the relationship between vulnerability as a network linkage and information security investment. Network linkages are currently established via existing inter-organizational entities; thus, recognizing the vulnerability of such linkages is difficult. Given these circumstances, we propose a vulnerability measurement method that uses information security workforce as a variable.

The importance of information security continues to increase. Many organizations, such as government divisions, firms, and research institutions are concerned over how activities related to information security investment can be efficiently implemented. We hope to have provided a meaningful response to this question.

For this work, we collect data from only 17 ministries. For reliability and validity, we intend to collect more data on a fixed number of organizations, the size of information and information security workforces, and the 2012 expenditure budgets of municipal and metropolitan government organizations.

Some limitations are worth noting. First, this research uses a small sample (16 ministries). We endeavored to guarantee the reliability and validity of the derived vulnerability levels, but we cannot draw meaningful results because of the sample size. As a future direction, we will focus on broadening the research scope by adding more government organizations, such as metropolitan cities and municipal governments.

Second, we are concerned over the dependence between information security investment and a fixed organizational size.

The proxy value used in this research (2012 budget for annual information expenditure) may not be completely free from the influence of a fixed number of organizations. The budget of an organization is made up of numerous cost and investment indexes, as well as costs from different domains, including human resources, finance, marketing, and strategy. The results of this study do not extend to these components.

Despite the limitations, however, our findings verify that information security investment and a fixed organizational size are strongly correlated. This result facilitates effective decision making on information security investment and enables comparison with other government organizations. Expanding this result to other domains (such as private companies) will afford certain enterprises a competitive advantage because decision making on the level of information security investment can be made on the basis of competitor decisions. These companies can consider internal and external factors that surround organizations, such as market conditions and government effectiveness.

APPENDIX

Appendix. 1. Information on the 17 Korean ministries of Korea

Number	Ministry	Fixed size of organizational workforce (FOW)	Size of information security workforce (ISW)	ln(budget for annual information expenditure of 2012)
1	Ministry of Strategy and Finance	935	2	23.578
2	Ministry of Security and Public Administration	1160	3	24.329
3	Ministry of Agriculture, Food, and Rural Affairs	525	2	22.377
4	Ministry of Science, ICT, and Future Planning	770	10	23.275
5	Ministry of Education	518	7	24.603
6	Ministry of Justice	640	4	21.620
7	Ministry of National Defense	940	9	23.860
8	Ministry of Culture, Sports, and Tourism	663	8	21.132
9	Ministry of Trade, Industry, and Energy	790	4	21.973
10	Ministry of Health and Welfare	731	5	23.805
11	Ministry of Employment and Labor	531	7	21.035
12	Ministry of Environment	515	6	21.824
13	Ministry of Land, Infrastructures, and Transport	956	5	23.732
14	Ministry of Oceans and Fisheries	509	4	22.003
15	Ministry of Foreign Affairs	845	17	21.400
16	Ministry of Gender Equality and Family	227	4	19.121
17	Ministry of Unification	N/A	N/A	N/A

REFERENCES

[1] Anderson, R., "Why Information security is Hard - An Economic perspective", *Paper presented at the 17th Annual computer security applications conference*, 2001.

[2] Camp, L. J., "The State of Economics of Information Security." *I/S A Journal of Law and Policy in the Information Society*, Vol. 2, No. 2, 2005, pp. 189-205

[3] Camp, L. J., Wolfram, C., "Pricing Security," *Paper presented at the CERT Information Survivability Workshop*, Boston, 2005.

[4] Database industry and market analysis report 2012, *Korea Database Agency*, 2012.

[5] Gordon, L. A., Loeb, M., Lucyshyn, W., Richardson, R., "2004 CSI/FBI Computer Crime and security Survey," *Computer Security Journal*, Vol. 20, No. 3, 2004, pp. 33-51.

[6] Gordon, L. A., Loeb, M., "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, Vol. 5, No. 4, 2002, pp. 438-457.

[7] Government Organization Management Information System, MOSPA (Ministry of Security and Public Administration of Korea), Retrieved on 23. Sep. 2013. Available: org.mospa.go.kr

[8] Kim, G., "Comparison analysis of Information organization and budget in local government; Focused metropolitan council," The Korean Association for Regional Information Society, Vol. 14, No. 2, 2011, pp. 57-83 (in Korean).

[9] Mnerie, D., Slavici, T., Crisan, G, C., Herman, L., Untaru, M., "Risk - security relationship in manufacturing processes." *Recent researches in Sociology, financing, environment and health Sciences*, March. 2011, pp. 247-250.

[10] MOSPA (Ministry of Security and Public Administration of Korea), Retrieved on 23. Sep. 2013. Available: www.mospa.go.kr

[11] Nation Information White Paper 2012, Ministry of Public Administration and Security, Korea Communications Commission, Ministry of Knowledge Economy, 2012.

[12] NIST, "Information Technology Security Training Requirements: A Role-and Performance-based Model," Special Publication 800-16, 1998.

[13] NCIA (National Computing & Information Agency), Homepage, www.ncia.go.kr, retrieved on 23. Sep. 2013.

[14] Public Service Divisional Manual Revenue and Expenditure Budget 2012, Government of the Republic of Korea, 2012.

[15] Shim, W., "Types of Information Vulnerability and IT Security Investment: An empirical Analysis of Businesses in Korea." (Unpublished).

[16] Smart Gov. Promotion plan (proposal), Ministry of Public Administration and Security, March, 2011.

[17] Stevens, B., "The emerging security economy: an introduction. In: OECD", *The Security Economy*, 2004, pp.7-16.

[18] Takacs, M., Edit, T, L., "The AHP Extended fuzzy based risk management". *Recent Researches in Artificial Intelligence, Knowledge Engineering and Data Bases*, Feb. 2011, pp.269-272.

[19] Tanaka, H., Matsuura, K., Sudoh, O., "Vulnerability and Information Security Investment: An empirical analysis of e-local Government in Japan," Journal of Accounting and Public Policy, Vol. 24, 2005, pp. 37-59.

[20] Toma, S, V., Chirita, M., Sarpe, D, A., "Country risk analysis: political and economical factors." *Recent Researches in Applied Economics*, July. 2011, pp. 162-167.

[21] Zarei, S., "Risk Management of Internet Banking." *Recent researches in Artificial Intelligence, Knowledge engineering and Data Bases*, Feb. 2011, pp. 134-139.

Sangmin Park is a master course student at the Department of Management Information Systems at Chungbuk National University. He received his bachelor degree in Science in Business Administration from Chungbuk National University. His research areas include strategy, management and policy issues in information security and business industry. His recent research papers have appeared in Korean journals, such as Journal of Information Technology Applications and Management, Journal of Korea Institute of Information Security and Cryptology.

Tae-Sung Kim is a professor at the Department of Management Information Systems at Chungbuk National University. He received his bachelor, master, and doctoral degrees in Management Science from Korea Advanced Institute of Science and Technology (KAIST). He worked for Electronics and Telecommunications Research Institute (ETRI) as a Senior Researcher for more than three years. Also, he worked as a visiting professor at the Department of Business Information System and Operation Management, the University of North Carolina at Charlotte and a visiting research scholar at the School of Computing, Informatics and Decision Systems Engineering, Arizona State University. His research areas include management and policy issues in telecommunications and information security. His recent research papers have appeared in international journals, such as European Journal of Operational Research, ETRI Journal, Journal of the Operations Research Society, Journal of Intelligent Manufacturing, Operations Research Letters, and Stochastic Analysis and Applications.