Considering Qualitative and Quantitative Factors to Select Information Security Countermeasures

CHEOL HWAN JANG, TAE-SUNG KIM

Abstract**—**The Threat of information security breaches is increasing. Large organizations have been targeted and have lost confidential customer information. Organizations have recognized the importance of information security investments. However, many organizations lack adequate investment in information security. In this paper, we derive the factors that affect investment in information security, provide a research model in accordance with information security decision factors and analyze the selecting priority of information security countermeasures using AHP decision model. According to the findings of this study, qualitative investment decision factors presented higher significance relatively and regulatory represented a relatively higher weight in the information security investment decision factors.

Keywords—Information Security Investment, Information Security Countermeasures, AHP

I. Introduction

IN 2011, several large companies were subject to attacks and these information security breaches were discussed in public. The companies lost personal data, including credit card information [12].

In both foreign as well as domestic companies, and particularly for financial companies and telecommunications companies that hold large amounts of personal data including credit card information, hacking attacks are increasing. As a result, information security laws and policies have been strengthened, and concern for the protection of company information has increased.

Companies have recognized the importance of information security investment and there is more interest in information security. In practice, companies lack adequate investment in information security.

In particular, results of information security investment have not occurred within the short term [18]. So, organizations are negative to invest in information security.

Most of the studies related to information security investment are about the optimal level of information security investment, information security investment performance and information security countermeasures. Many studies are related to information security investment research to analyze the economic costs and benefits. Table 1 shows relative researches.

In situations, if we want to improve to an appropriate level of information security investment, economic aspects of the research as well as the factors affecting information security investment analysis needs to.

We find that companies that have decided to invest in information security use standards and purpose for efficient information security investment. Also, we select information security countermeasures that based on each of the investment purpose and standards of information security. These lead to more efficient information security investment.

Therefore, in this paper, we derive criteria to consider when we invest in information security and we perform an information security investment countermeasures priority analysis. The aim of this paper is to provide a model for selecting rational information security countermeasures according to investment objectives or standards for information security.

Table 1. Researches of information security investment

Division	Type	Contents
Information security investment research	Optimal level of information security investment	Research of models that suggest the optimum level of information security investment
	Information security investment performance	Research of the various ways in which to evaluate the costs and benefits of information security investment
	Information security countermeasures	Research of information security countermeasure according to threat of information security

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).

Cheol Hwan Jang is with the Department of Information Security Management, Chungbuk National University, 12 Gaesing-dong, Heungduk-gu, Cheongju, Chungbuk 361-763, South Korea.

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

A. Information Security Investment Decision Factors

Very little research has been done on decisions about investment in information security or investment purpose.

So, we consider the decision factors of investment in information systems. Previous researches on this viewed that information security investment was part of IT investment.

In this aspect, we can see that IT investment decision factors are related to information security investment determinants. These factors apply to the information security decision factors. We review affecting factors that information systems such as the business environment (competition, linking strategy), information technology (technical risk, support of management information), economics (return on investment, input costs), organization (size of organization, support of administration) [9]. Through this review, we determined that there are quantitative factors, qualitative factors and strategic factors.

And, decision of information security investment of enterprise can be prevented in an appropriate investment security incidents deemed risk. Also, if companies were adding information security countermeasure their external business and services, it is considering the positive effect on the profitability of these companies [20].

Through this, the investment factors were confirmed by a consideration of the outcome factors and risk factors. Such as consideration of the characteristics of the decision of investment, in this paper was composed of factors that can be applied to risk factors, performance factors and quantitative factors, qualitative factors, strategic factors.

First, quantitative investment decision factors can be expressed by measuring a numerical objective, it allows that recognizes the need to investment in information security. In previous studies, these were described with terms such as loss of business from denial of service attack (DOS), faulty decisions based on altered data [26] and lost productivity [8], [11].

Based on this, in this paper, we have discussed quantitative investment in terms of productivity, profitability, input costs. Qualitative investment decision factors cannot be expressed by measuring numerical objectives. However, these factors affect investment decisions in the same manner as quantitative factors. In previous studies, these are described with terms such as reputation, regulatory penalties and stock market price [5], [19].

Finally, there are strategic investment decision factors, which relate to performance and the positive effects that companies obtain from information security investment. These include customer satisfaction index [6] and competitive advantage [4].

B. Information Security Countermeasures

Research on information security countermeasures was done by dividing the administrative aspects and technical aspects. Research on the information security countermeasures forms a main research covering the technical aspects.

There are studies dealing with information security countermeasures through information security products and

Table 2. Factors and Countermeasures

Division	Type	Description	Reference
Information Security Investment Decision Factors	Quantitative Investment Decision Factors	Productivity, profitability and input costs	Gordon and Loeb(2002) Sonnenreich, Albanese, Stout (2006)
	Qualitative Investment Decision Factors	Reputation, regulatory penalties, stock market price	Kim, Lee, In (2008) Butler (2002)
	Strategic Investment Decision Factors	Customer satisfaction index, competitive advantage	Blight (1997) Parker (1997)
Information Security Countermeasures	Information Security Policy	Formulation of information security policy and periodic review of information security policy	D`Arcy, Hovav, Galletta (2008) Aggarwal, Kanhere, Kanhere, Bajoria (2005) Lee, Jang (2009)
	SETA Program	Security education, training, and awareness program	Liu, Tanaka, Matsuura (2008)
	Information Security Products	Access control information systems and installation information security products	Liu, Tanaka, Matsuura (2008) Ram, Park, Chandrasekar (2008)
	Monitoring/Auditing	Regular monitoring or auditing by internal/external experts	Liu, Tanaka, Matsuura (2008)
	Cyber Insurance	To cover losses and liabilities from information security breaches	Baer and Parkinson (2007) Böhme (2005)

technologies such as firewall, intrusion detection systems (IDS), antivirus products, virtual private networks (VPN), encryption, public key infrastructure (PKI), business continuity contract, operating system patches, password policies and periodic changes, network user accounts, uninterruptible power supplies, wireless security, disaster recovery plan, e-mail virus scan protection, malware/spyware inspection, distributed automated virus scan, automatic patching and updating, sniffer/network analyzer, HTTPs protocols, escrow and authentication, secure server, smart card, authentication policy servers, e-mail content inspection, vulnerability assessment, line encryption, onion router, traffic padding, data segregation, system activity monitor, power surge protectors, security evaluation systems, data backup systems etc [1],[14],[19],[21],[23].

In addition, research on information security countermeasures was done by dividing IT-related efforts (software, hardware, data, network) and non-IT related efforts (physical, personnel, regulations/legality) [16].

In research dealing with information security countermeasures from the administrative aspect, research was done by dividing information security management system (ISMS) [2],[13],[25], information security policy, security education, training and awareness program (SETA program) [7],[24].

In addition, there was research to deal with emergency action plans (EAPs) corresponding to information security breaches.

Domain of information security is divided into physical security, technical security and administrative security.

In this paper, we derive information security countermeasures that can be applied to comprehensive. In addition, we consider the factors that could be proactive and reactive information security countermeasures.

For this reason, we have deemed information security countermeasures cyber insurance against information security breaches [17],[27]. Table 2 lists the information security investment decision factors and information security countermeasures used.

III. AHP Decision model

A. AHP overview

The AHP, develop by Saaty is designed to solve complex multi-criteria decision problems. The AHP is aimed at aimed at integrating different measures into a single overall score for ranking decision alternatives. This is an eigenvalue approach to pair-wise comparisons.

It provides a methodology to calibrate the numeric scale for the measurement of quantitative as well as qualitative performance. The scale ranges from 1/9 for ‘least valued’, to 1 for ‘equal’, and to 9 for ‘absolutely more important than’, covering the entire spectrum of the comparison. Table 3 shows Judgement scores for the important/preference of criteria using AHP.

AHP helps to incorporate a group consensus. Generally, this consists of a questionnaire for the comparison of each element and a geometric mean to arrive at a final solution.

The hierarchy method used in AHP has various advantages [22]. AHP has been applied to a wide variety of decisions [3],[15],[10].

Table 3. Judgement scores for the important/preference of criteria using AHP

Verbal Judgement	Numerical rating
Extremely important/preferred	9
Very strongly to Extremely important/preferred	8
Very strongly important/preferred	7
Strongly to very strongly important/preferred	6
Strongly important/preferred	5
Moderately to strongly important/preferred	4
Moderately important/preferred	3
Equally to moderately important/preferred	2
Equally to important/preferred	1

B. AHP hierarchy

In our paper, we explain the prioritized selection of information security countermeasures based on the information security investment decision factors using AHP decision model.

Figure1 shows the structure of our AHP decision model. All layers are described as follows.

First, quantitative investment decision factors have been configured to productivity, input costs and profitability. Secondly, qualitative investment decision factors have been configured to reputation and regulatory.

Finally, strategic investment decision factors have been configured to customer satisfaction index and competitive advantage [Figure 1].

The definition of productivity includes investment factors with business damage (loss of data) and property damage (system interruption).

The definition of profitability is investment factors with a loss of revenue and the rate of operating profits. The definition of reputation includes investment factors with a decrease in corporate image.

The definition of regulatory is investment factors with a regulation or law related to information security. The definition of customer satisfaction index is investment factors with customer satisfaction and improving customer loyalty.

The definition of competitive advantage is investment factors that enhance competitiveness against other companies. We define the factors used in the AHP model.

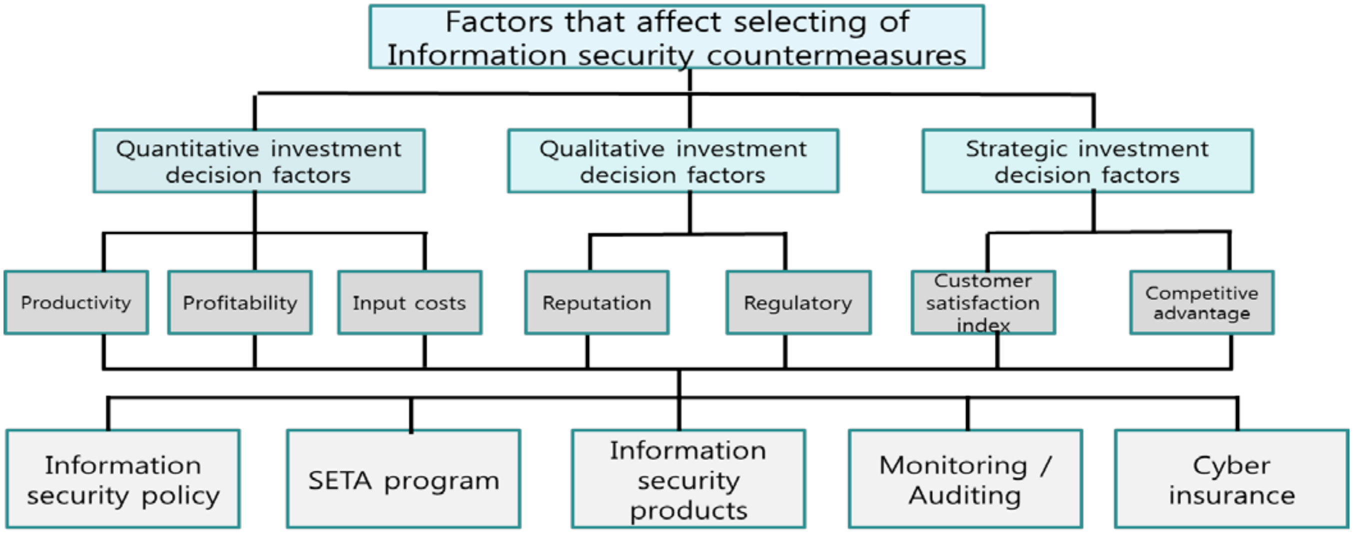
Factors that affect selecting of Information security countermeasures
Quantitative investment decision factors
Qualitative investment decision factors
Strategic investment decision factors
Productivity
Profitability
Input costs
Reputation
Regulatory
Customer satisfaction index
Competitive advantage
Information security policy
SETA program
Information security products
Monitoring / Auditing
Cyber insurance

Fig. 1 AHP hierarchy

C. *Survey Design*

In this study, it is possible to study information security countermeasures based on information security decision factors.

We obtain the advice of a professional before advancing the survey, to confirm the agreement of the hierarchy.

In addition, this study provides factors in selection of information security countermeasures, so we conduct a survey of professional engaged in a separate industry group.

D. *sample and Method*

This research surveyed current enterprise employees for 2 weeks by utilizing both interviews and online surveys in parallel. In AHP analysis, we adopted a strict standard that the consistency ration should be less that the threshold of 0.10. But for subsequent studies, if AHP is to be applied to social science areas, the threshold could be lifted up to 0.20, considering the fact that the details of each criteria are often failed to be fully delivered.

The surveyed herein were those who had higher understanding of information security investment for their job or those who managed system security or computer management mostly.

An e-mail invitation to complete the online survey was sent to 64 employed professionals, of which 21 responded.

Incomplete or otherwise unusable entries were discarded from data set, leaving 13 usable responses. A summary of the demographic characteristics of respondents is provided in Table 4. For the empirical analysis in this research, Expert Choice was adopted.

Table 4. Characteristics of Respondents

Division		Survey participants	percent
Company size	Small and medium	9	69.2
	Large	4	30.8
Industry	Manufacturing	2	15.4
	Information technology	10	76.9
	Professional, Scientific and Technical services	1	7.7
Position	Assistant manager	4	30.8
	Manager	2	15.4
	Deputy / General manager	5	38.5
	Director	2	15.4
Career	3-5 years	5	38.5
	5-10 years	3	23.1
	10-15 years	3	23.1
	15-20 years	2	15.4

IV. Analysis and Results

Though AHP analysis, we analyzed the relative order of priority of factors affecting information security investment decision making and the order of priority of information security investment countermeasures depending upon each information security investment decision.

First of all, this research has formed a survey with qualitative investment decision factors, quantitative investment decision factors and strategic investment decision factors without adding each factor-specific weight then, combined the lower-class factor weights calculated after the survey to draw upper-class factor-specific weight.

As a result, qualitative investment decision factors are considered to priority of information security investment decision. Table 5 shows the analysis results.

Table 5. Weight of investment decision factors

Criteria	Quantitative investment decision factors	Qualitative investment decision factors	Strategic investment decision factors	Total
Weight (Rank)	0.349 (2)	0.350 (1)	0.301 (3)	1.000

A. *Priority comparison of information security investment decision factors*

As result of relative priority comparison on information security investment decision factors, we found that ‘Regulatory’ showed a weight 0.229, making the highest priority followed by ‘Competitive advantage (0.167)’, ‘Customer satisfaction index (0.134)’, ‘Productivity (0.124)’, ‘Reputation (0.121)’, ‘Profitability (0.115)’, ‘Input costs (0.110)’ in order.

Based on this finding, we view that factors affecting information security investment decision by enterprises are more primarily focused on response to regulatory such as laws and policies on information security.

B. *Priority comparison of information security countermeasures according to investment decision*

This thesis examined the priority of information security countermeasures depending upon information security investment decision factors as follows.

First, under the assumption that ‘productivity’ is regarded as a significant information security investment decision factor, ‘Information security education, training and awareness program (SETA program)’ showed the highest priority with 0.269 weight. Next was ‘Information security policy (0.230)’, ‘Monitoring / Auditing (0.219)’, ‘Information security products (0.217)’ and ‘Cyber insurance (0.065)’. This order of priority demonstrates that enterprises primarily consider information security education, training and awareness program for employees as a countermeasure to information security investment to prepare for possible asset damages such as data loss or work damages like system failure.

Second, under the assumption that ‘Profitability’ is regarded as a significant information security investment decision factor, ‘Information security products’ showed the highest priority with 0.300 weight. Next was ‘Monitoring /Auditing (0.235)’, ‘SETA program (0.198)’, ‘Information security policy (0.175)’, ‘Cyber insurance (0.092)’. This order of priority demonstrates that enterprises are viewed to consider information system access control and information security product purchase and installation to provide against damages to sales turnover amount or sales profit as countermeasure to information security investment.

Third, under the assumption that ‘Input costs’ is regarded as a significant information security investment decision factor, ‘Information security products’ showed the highest priority with 0.282 weight. Next was ‘Monitoring/Auditing (0.232)’, ‘Information security policy (0.199)’, ‘SETA program (0.182)’, ‘Cyber insurance (0.105)’.

It was found in this research that enterprises thing of buying and installing information system access control and information security products as a priority in making information security investment by considering financial aspects such as establishment cost and maintenance cost.

Forth, under the assumption that ‘Reputation’ is regarded as a significant information security investment decision factor, ‘SETA program’ showed the highest priority with 0.293 weight. Next was ‘Information security policy (0.239)’, ‘Monitoring/Auditing (0.206)’, ‘Information security products (0.170)’, ‘Cyber insurance (0.092)’. Through this, information security education, training and awareness program for employees was also found to be considered by enterprises as an information security investment decision countermeasure to provide against corporate image loss such as corporate reputation damage.

Fifth, under the assumption that ‘Regulatory’ is regarded as a significant information security investment decision factor, ‘Information security policy’ showed the highest priority with 0.323 weight. Next as ‘Monitoring/Auditing (0.246)’, ‘SETA program (0.183)’, ‘Information security products (0.158)’, ‘Cyber insurance (0.090)’. As an information security countermeasure to respond to regulations such as information security–related laws and policies, formalized information security policies and regular information security policies were found to be considered first.

Table 6. Research analysis results

Information security investment decision factors	Weight	Rank	Information security countermeasures	Weight	Rank
Productivity	0.124	4	Information security policy	0.230	2
			SETA program	0.269	1
			Information security products	0.217	4
			Monitoring / Auditing	0.219	3
			Cyber insurance	0.065	5
Profitability	0.115	6	Information security policy	0.175	4
			SETA program	0.198	3
			Information security products	0.300	1
			Monitoring / Auditing	0.235	2
			Cyber insurance	0.092	5
Input Costs	0.110	7	Information security policy	0.199	3
			SETA program	0.182	4
			Information security products	0.282	1
			Monitoring / Auditing	0.232	2
			Cyber insurance	0.105	5
Reputation	0.121	5	Information security policy	0.239	2
			SETA program	0.293	1
			Information security products	0.170	4
			Monitoring / Auditing	0.206	3
			Cyber insurance	0.092	5
Regulatory	0.229	1	Information security policy	0.323	1
			SETA program	0.183	3
			Information security products	0.158	4
			Monitoring / Auditing	0.246	2
			Cyber insurance	0.090	5
Customer satisfaction index	0.134	3	Information security policy	0.189	4
			SETA program	0.230	2
			Information security products	0.245	1
			Monitoring / Auditing	0.213	3
			Cyber insurance	0.123	5
Competitive advantage	0.167	2	Information security policy	0.150	4
			SETA program	0.227	3
			Information security products	0.273	1
			Monitoring / Auditing	0.257	2
			Cyber insurance	0.093	5

Sixth, under the assumption that ‘Customer satisfaction index’ is regarded as a significant information security investment decision factor, ‘Information security products’ showed the highest priority with 0.245 weight. Next was ‘SETA program (0.230)’, ‘Monitoring/Auditing (0.213)’, ‘Information security policy (0.189)’, ‘Cyber insurance (0.123)’. When enterprises choose information security countermeasure with an expectation to elevate customer satisfaction and loyalty, they are deemed to consider information security product primarily.

Seventh, under the assumption that ‘Competitive advantage’ is regarded as a significant information security investment decision factor, ‘Information security products’ showed the highest priority with 0.273 weight. Next was ‘Monitoring/Auditing (0.257)’, ‘SETA program (0.227)’, ‘Information security policy (0.150)’, ‘Cyber insurance (0.093)’. This order of priority demonstrates that enterprises are deemed to consider information security products primarily when selecting a countermeasure to information security investment with an expectation to improve own competitive advantage over other rivals. The following Table 6 shows the analysis results.

V. Conclusion and Implications

Based on this research analysis on information security investment decision and their countermeasures, the following implications are presented.

First, when information security investment decision factors were divided into quantitative investment decision factors, qualitative investment decision factors and strategic investment decision factors according to features, they showed similar weights in general with the qualitative investment decision factors presenting higher significance relatively. This implies that if we are to explore ways to encourage corporate information security investment to an optimal level, qualitative analysis will be necessary on the effects of information security investment such as prevention against possible corporate image loss in addition to financial numbers to view such effects.

Secondly, regulatory represented a relatively higher weight in the information security investment decision factors. Regulatory is defined as those from information security related laws and policies. Based in this research, it is deemed that enterprises importantly regard regulatory compliance according to information security related laws and regulations and possibility of additional expenses in making information security investment. Therefore, to help enterprise invest in information security to an optimum level, a first thing would be to implement laws and policies considering enterprises situations.

Third, if this research analysis is utilized in selecting countermeasure way to information security investment, more practically applicable information would be offered. When companies make a decision on information protection investment, this research analysis is expected to help them review countermeasures priority appropriate for their investment purposes or criteria and reach an effective countermeasure selection.

Forth, this research viewed cyber insurance as an ex post countermeasure to information security investment. However, the awareness on the importance of cyber insurance as an information security countermeasure was found to be relatively lower. Most OECD member countries are pursuing integrated personal information protection policies both in the public and private sectors and related insurance products are being expanded. Many of the surveyed companies herein were mid and small-sized enterprises but they are in industries with high risk of information security accidents. In this sense, it should be noted that diverse investment countermeasures such as cyber insurance need to be more actively utilized.

VI. Limitations and Future Research

This research may be limited in the follow aspects.
AHP model in this research may face criticism for its methodology whether the information security investment decision factors and information security countermeasures include all kinds of factors and countermeasures and whether its implementation was done in a valid and appropriate manner.

Therefore, continued investigation will be necessary on what kind of information security investment factors and information security countermeasures should be factored in additionally in an empirical analysis.

Also, in analyzing information security investment decision factors and information security countermeasures selections, surveyed companies will need to be grouped into industry-specific areas to further compare and analyze the outcomes according to common enterprise situation and purpose of decision making.

References

[1] A. Herzog, N. Shahmehri, C. Duma, "An Ontology of Information Security", *International Journal of Information Security and Privacy*, Vol.1, No.4, 2007, pp.1-23.

[2] Akshai Aggarwal, Vishnu Kanhere, Shankar Kanhere, Nilesh Bajoria, Budgeting for Information Security and ROI Approach, *Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers*, Tenerife, Spain, December 16-18, 2005, pp75-80.

[3] C. S. Huang, Y. J. Lin, "An Evaluation Model for Determining Insurance Policy Using AHP and Fuzzy Logic: Case Studies of Life and Annuity Insurances", *Proceedings of the 8th WSEAS International Conference on Fuzzy Systems*, Vancouver, British Columbia, Canada, June 19-21, 2007, pp.126-131.

[4] D. B. Parker, "The Strategic Values of Information Security in Business", *Computer & Security*, Vol. 16, No. 7, 1997, pp. 572-582.

[5] D. H. Kim, T. Lee, P. H. In, "Effective Security Safeguard Selection Process for Return on Security Investment", *IEEE Asia-Pacific Services Computing Conference*, 2008, pp. 668-673.

[6] J. Blight, "Customer Privacy versus Customer Service", *Information Security Technical Report*, Vol. 21, No. 1, 1997, pp. 43-46.

[7] J. D`Arcy, A. Hovav, D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Miuse: A Deterrence Approach", *Information Systems Research*, Vol. 20, No. 1, 2008, pp. 1-20.

[8] J.N. Sheen, “Fuzzy Economic Decision-models for Information Security Investment”, *Proceedings of the 9th WSEAS Int. Conference on Instrumentation, Measurement, Circuits and Systems*, 2010, pp.141-147.

[9] K. I. Chang, S. M. Kang, "The Empirical Study on the Individual Determinant having a Key Impact on IT Investment and Adoption", *Entrue Journal of Information Technology*, Vol. 2, No. 1, 2003, pp. 99-106..

[10] K. Muralidar, R. Santhannam, "Using the Analytic Hierarchy Process for Information System Project Selection", *Information & Management*, Vol. 18, No. 1, 1990, pp. 87-95.

[11] L. A. Gordon, M. P. Loeb, "The economics of information security investment", *ACM Transactions on Information and System Security*, Vol. 5, No. 2, 2002, pp. 438-457.

[12] L. Demetz, D. Bachlechner, "To Invest or not to Invest?", WEIS(Workshop on the Economics of Information Security), 2012.

[13] L. E. Sanchez, A. S. Parra, "Managing Security and its Maturity in Small and Medium-sized Enterprises", *Journal of Universal Computer Science*, Vol. 15, No. 15, 2009, pp. 3038-3058.

[14] L. K. Ram, S. J. Park, Chandrasekar Subramanian, "Understanding the Value of Countermeasure Portfolios in Information Systems Security", *Journal of Management Information Systems*, Vol. 25, No. 2, 2008, pp. 241-279.

[15] M. C. Y. Tam, V. M. R. Tummala, "An Application of the AHP in Vendor Selection of a Telecommunications System", *Omega*, Vol. 29, No. 2, 2001, pp. 171-182.

[16] Q. J. Yeh, A. J. T. Chang, "Threats and Countermeasures for Information System Security-A cross-Industry Study", *Information & Management*, Vol. 44, No. 5, 2007, pp.480-491.

[17] R. Böhme, "Cyber-Insurance Revisited", *WEIS (Workshop on the Economics of Information Security)*, 2005.

[18] R. Richardson, 2008 CSI Computer Crime & Security Survey, Computer Security Institute, 1, 2009.

[19] S. A. Butler, "Security Attribute Evaluation Method: A Cost-Benefit Approach", *Proceedings of the 24th International Conference on Software Engineering*, 2002, pp.232-240.

[20] S. H. Nam, "An Empirical Study on the Impact of Security Events to the Stock Price in the Analysis Method of Enterprise Security Investment Effect", Korea University, Doctoral Dissertation, December, 2006.

[21] S. Keller, A. Powell, A. Horstmann, C. Predmore, M. Crawford, "Information Security Threats and Practices in Small Businesses", *Information Systems Management*, Vol. 22, No. 2, 2005, pp. 7-19.

[22] T. L. Saaty, *The Analytic Hierarchy Process*, McGraw-Hill, 1980.

[23] V. Dimopoulos, S. Furnell, M. Jennex, I. Kritharas, "Approaches to IT security in Small and Medium Enterprises", *Proceedings of the 2nd Australian Information Security Management Conference*, 2004, pp. 73-82.

[24] W. Liu, H. Tanaka, K. Matsuura, "Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms", *Information and Media Technologies*, Vol.3, No.2, 2008, pp. 464-478.

[25] W. S. Lee, S. S. Jang, "A Study on Information Security Management System Model for Small and Medium Enterprises", *In: Proceedings of the 8th WSEAS International Conference on E-Activities and Information Security and Privacy. World Scientific and Engineering Academy and Society (WSEAS)*, 2009. p. 84-87.

[26] W. Sonnenreich, J. Albanese, B. Stout, "Return on Security Investment (ROSI) - A Practical Quantitative Model", *Journal of Research and Practice in Information Technology*, Vol.38, No. 1, 2006, pp. 55-66.

[27] W.S. Baer, A. Parkinson, "Cyberinsurance in IT Security Management", *Security & Privacy, IEEE*, Vol. 5, No. 3, 2007, pp. 50-56.

Cheol Hwan Jang is a master`s course in the Department of Information Security Management at Chngbuk National University. He received his bachelor degrees in Law from Chngbuk National University. His research interests include software development, information security management and security consulting

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.