Indian Journal of Science and Technology, Vol 9(24), DOI: 10.17485/ijst/2016/v9i24/96106, June 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Will the Certification System for Information Security Management Help to Improve Organizations' Information Security Performance? The Case of K-ISMS

Hee-Kyung Kong[1], Jeong-hun Woo[2], Tae-Sung Kim[2*] and Hyuk Im[2]

[1]Department of Electrical and Computer Engineering, Chungbuk National University, 1 Chungdae-ro, Seowon-gu, Cheongju, Chungbuk - 28644, South Korea; konghk1@naver.com
[2]Department of Information Security Management, Chungbuk National University, 1 Chungdae-ro, Seowon-gu, Cheongju, Chungbuk - 28644, South Korea; wjhfamily@hanmail.net, kimts@chungbuk.ac.kr, Imhyuk5054@gmail.com

Abstract

Background/Objectives: Recognizing the importance of systematic security management in organizations, the government of South Korea introduced the Information Security Management System (ISMS) certification. **Methods/ Statistical Analysis**: In this study, based on prior studies dealing with the goal and evaluation items of ISMS certification, we developed a model to measure the performance of ISMS certification, using the SERVQUAL models, which are service evaluation models. Also, we carried out a survey of organizations that have acquired the certification in order to prove the model's validity and suggest ways to develop ISMS certification. **Findings:** In the present study, we found that investment and concern in security can influence organisational security performance based on prior research, and developed survey items for performance measurement by acquisition of ISMS certification. We conducted surveys of organisations that required ISMS certification and tried to find some factors recognisable as a performance of ISMS certification. The result of the experiment was that factors influencing security performance are responsiveness and specialty. **Application/ Improvements:** Future research is increased ISMS certified company in accordance with the satisfaction and effectiveness of the ISMS certified company improved through systematic empirical and hope enhance the overall security level.

Keywords: Information Security Management System, ISMS Certification, Information Security Performance, Service Quality, SERVQUAL

1. Introduction

Recently, security incidents in many organizations such as public institutions, telecommunications companies, banks and broadcasting stations have happened far too often notwithstanding the many efforts of governments and businesses[1]. The government of South Korea, for example, has forced key telecommunications business providers in Seoul and other cities, along with information and communication service providers, that have traffic rates of an average of 100 million a day for three months and sales of more than 100 billion US dollars in the previous year, to acquire ISMS certification under the second clause of Article 24 of the Act on Promotion of Information and Communications Network, and has a plan to extend the application of the law. Furthermore, the government is encouraging organizations that are free from the law, to acquire ISMS certification, giving extra points for corporate evaluation, public project bids and a discount on tax. Also, they are trying to strengthen

*Author for correspondence

the information security level of businesses, designating the Korea Association for ICT Promotion (KAIT) as the certification evaluation agency (previously, Korea Security and Security Agency KISA) and the sole certification agency of ISMS, preparing for the increase in companies that want to get the certification and thereby addressing the current problem of ISMS. According to the statistics of the Ministry of Science, ICT and Future Planning (MSIP) submitted at the request of the National Assembly in March 2014, only two of the twenty-four financial companies that account for most of the personal information processing have acquired ISMS certification. Moreover, just 129 of all 163 organizations under the law have acquired ISMS certification, which is a compliance rate of 76.7%. Clearly, the diffusion rate of ISMS is disappointingly low. In January 2014, security incidents occurred within two financial companies that had previously acquired ISMS[2]. Due to these incidents, there is a big controversy over the effectiveness of ISMS certification, and many professionals look upon the matter with a jaundiced eye. In their view, ISMS certification is just a security management system of red tape because organizations get ISMS unwillingly by legal requirement rather than voluntarily. Eventually, even if an organization gets the certification, they are not satisfied with security performance. It is a big problem to solve.

We developed the model to measure ISMS performance based on the SERVQUAL models in order to improve the problems with ISMS and to attract voluntary participation from many organizations. The SERVQUAL models have been used to measure service quality in many fields and help service providers find the improvement point[3]. In the present study, we regarded ISMS certification as one aspect of a service and performance of ISMS as an aspect of quality. By using this model, we measured the security performance of the organizations and tried to understand if ISMS actually works, and to find positive or negative factors of ISMS so as to suggest the way to address the problems ISMS has through a survey of the organizations that want to get ISMS, using our model. The government is able to expect improvement in the satisfaction of organizations, which have a plan to introduce ISMS, while the security level across society will be improved by the introduction of the ISMS certification in many organizations. Finally, service providers bolster customers' trust in security and decrease the social cost generated by security incidents.

2. Literature Review

2.1 Information Security

As a benefit of the advances in technology, many enterprises and public institutions can utilize IT technology easily, and they are collecting, processing, storing and retrieving massive amounts of information. But because of physical, managerial and technical vulnerabilities in security, concerns for information leakage and damage are increasing rapidly. All commercial enterprises and public institutions need to pay attention to security, even though security activity is enforced on only a small portion of organizations by law.

The term "information" can be defined as "useful fact and knowledge needed to certain purposes in distinction to data". Information has seven attributes: effectiveness, efficiency, confidentiality, availability, integrity, compliance and reliability. Of these attributes, confidentiality, availability and integrity are the main components of information security and the purpose of information security is to achieve these attributes. Many people argue that the paradigm of information security started after the emergence of technical security. Many organizations had difficulty in conducting information security activities even though they had technical countermeasures to protect information, as there was no department taking complete charge of information security. Thus, the second generation of information security (managerial security) involved the beginnings of creating a department that would take complete charge of security. Unfortunately, at this time, only partial and sporadic countermeasures were initiated against external hacking attacks. Then, the third generation of information security started. Subsequently, organizations were able to respond systematically against threats and manage the level of information security. Lastly, the current, fourth-generation information security is related to compulsory security activity. In the past, organizations were asked to perform security activity voluntarily. But due to this voluntariness, investment in security was inadequate and security incidents occurred continuously. The government enacted the relevant law and forced the organizations to conduct security activity for the improvement of security across society. At present, the information security systems of South Korea are in a transitional stage from the third to the fourth generation

because just part of the organizations are required to provide information security activity under the law.

2.2 Information Security Management System (ISMS)

An ISMS is a system for managing and operating an information security system using a risk-based approach and administering all sorts of security measures to achieve the confidentiality, integrity and availability of information assets through a cycle of five stages: construction, operation, monitoring, examination and improvement. An ISMS asks for connection with the information security and business policy, designation of a Chief Information and Security Officer (CISO), establishment of an enterprise information security policy, and decision making on personal management and budget. While many companies took fragmentary measures, one-off security management and partial security activity against threats before ISMS was developed, now through an ISMS they can execute a systematic response, continuous security management and enterprise-level, balanced security. Now, in connection with information security governance and compliance, they provide their customers with trust and improved stability of communications networks.

The International Organization for Standardization (ISO) and International Electro-technical Commission (IEC) formed a Joint Technical Committee together and developed BS 7799. In 2005, they announced ISO/IEC 27001 and ISO/IEC 27002, which are the international standard of ISMS. Starting with these enactments of international standards, the ISO/IEC 27000 series was persistently created and amended, and the standardization of information security continues to be ongoing. The government of South Korea developed K-ISMS based on the ISO/IEC 27000 series in order to support the information security activity of organizations and is operating ISMS. The K-ISMS certification agency evaluates objectively and independently whether organizational security activities fit the guideline when the ISMS is being constructed and operated in the organization. K-ISMS was introduced in July 2001 when the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. was amended.

The K-ISMS certification criteria are divided into a total of 137 control items and 396 detailed items. Recently, some documentation items were eliminated to reflect the integration of ISMS items and changes in the security management criteria. An information security management process, which is an essential item of ISMS, consists of 12 control items and 47 detailed items, and information security measures consist of 104 control items and 253 detailed items. The information security management process consists of the critical items required for an examination of certification and specifies the establishment of information security policy and scope, responsibility of management, composition of organization and risk management. For the establishment of an information security policy and scope and responsibility of management, the composition of an organization are includes 2 control items and 4 detailed items respectively, while risk management consists of 3 control items and 11 detailed items. Information security measure implementation consists of 2 control items and 2 detailed items, while post management consists of 3 control items and 6 detailed items. A total of 5 stages and 12 control items with 28 detailed items are specified in the ISMS. The establishment of an information security policy and scope, the responsibility of management, composition of the organization, risk management, implementation of information security, and post management have a circulating structure that is persistently managed by the ISMS. An information security measure consists of 13 categories and 92 control items. Control items unrelated to certification can be excluded at the discretion of the organization. If items are excluded as described above, the organization must state the reason. By doing this, ISMS specifies a provisory clause to avoid the exclusion of certain control items either intentionally or inadvertently. Through this provisory clause, ISMS tries to avoid the arbitrary exclusion of certain items by the certified organization.

2.3 Service Quality Evaluation Model

SERVQUAL is one of the methods used to conceptualize and measure service quality. This model is formed from the words "Service" and "Quality" and was developed by Parasuraman et al. in order to measure service quality because they recognized the importance of the quantification of service quality[4,5]. The early version of SERVQUAL consists of 10 dimensions and 97 subordinate items made based on the interviews of focus groups and company managers. Afterwards, inappropriate items were eliminated and integrated through reliability and factorial analysis. SERVQUAL was turned into the 5 dimensions

of tangibles, reliability, responsiveness, assurance, sympathy and 22 items. Tangibles indicate external elements such as physical facility, equipment and appearance of the employee. Reliability is the ability to provide timely, accurate service to the customers. Responsiveness is the willingness to help customers by providing a prompt response time to user requests and fast service and empathy is an interest in and a concern for customers. Assurance is the ability to give customers credit, confidence, knowledge and courtesy.

SERVQUAL is composed of a total of 44 items including respectively 22 items of expected quality and perceived quality. Respondents are required to answer 22 items each, once before and once after a service. These questions are presented as 7-point Likert scale questions ranging from 1 = strongly negative to 7 = strongly positive. Service expectations of customers are measured by such items as word of mouth, past experiences and personal needs formed before service and perceived service quality is measured by experience and the thoughts customers have right after service. SERVQUAL can be calculated by the difference between expectations of service and perceived service in the form of an Equation 1:

Service Quality = Perceived Service Quality – Expected Service Quality (1)

The higher the value of service quality, the more people perceive service quality to be higher than expected. Eventually, customers are satisfied with the service. As the value of Equation (1) represents the total size of service quality, we can assume that the higher the value, the higher the service quality.

2.4 Prior Study Related to Service Quality

SERVQUAL is utilized in many fields, such as education, travel, medical science, information systems and public service. Dagger et al. evaluated service quality, dividing it into technical quality, environmental quality and administrative service quality in the realm of health care[6]. They did not use the original SERVQUAL and introduced the modified model by investigating prior studies related to the service sector. In their study, sub-factors such as facility, time, support, relation and interaction are similar to the overall meanings of items used in SERVQUAL. Lee and Yom measured service quality by using SERVQUAL in the nursing service fields[7]. They used 5 items suggested in SERVQUAL without revision, and changed 22 sub-items to make it more appropriate to the nursing fields. Ahn et al. studied the effects of system quality, information quality and service quality of web portals on enjoyment, usability and satisfaction and they utilized the scales of SERVQUAL to develop the measurement instrument[8].

In addition, Cristobal et al. and Grigoroudis et al. used the scales of SERVQAUL to measure the service quality of web portals[9,10]. Tan and Pawitra evaluated the service quality by using a scale of SERVQUAL in the travel industry[11]. They developed a mathematical expression to evaluate the service quality by combining SERVQUAL with Kano's model in order to classify methods to meet customer's needs and proved the validity of the expression through a survey of Indonesian and Singaporean tourists. Lin carried out an empirical study on the service quality of supermarkets with fuzzy analysis and suggested a transformed SERVQUAL[12]. The model made a proposal to use four dimensions, such as physical appearance (e.g. facilities), reliability, interaction between clerks and customers, convenience and price policy and twenty-two sub-items. Jiang et al. conducted studies empirically on the service quality of information systems, and used four dimensions (reliability, responsiveness, assurance, empathy), and perceived the fact that correlation between service quality and tangibles is low[13]. Van Dyke et al. studied the service quality of information systems by introducing the SERVQUAL model and insisted that the measure of performance is more effective than of service quality, which is calculated by the difference between expected and experienced quality[14]. Yoon and Suh utilised SERVQUAL to evaluate the quality of IT consulting services[15]. In their study, tangibles were eliminated, and dimensions including reliability, responsiveness, assurance and empathy were used. They added process and education dimensions playing a main role in the IT consulting fields, and organised a total of six dimensions and thirty-six sub-items based on previous studies.

3. Proposed Model and Hypothesis

In this study, we suggest five dimensions such as tangibles, reliability, responsiveness and specialty, continuity based on the dimensions presented in SERVQUAL and the purposes and requirements of ISMS. In addition, by referring to prior studies that deal with critical factors related to the outcomes generated by aggressive security

investments and activity, our model generated a total of 23 sub-items including 4 for reliability, 4 for responsiveness, 6 for tangibles, 4 for specialty, 5 for continuity and 3 for performance by acquisition of ISMS. We formulated 5 hypotheses on the relation between perceived performance of ISMS and each dimension. Figure 1 shows the research model.

H1: Reliability will positively influence performance resulting from the acquisition of ISMS certification. Reliability dimension means the level of confidence in security obtained from the persons concerned with and around the organisation by acquisition of ISMS.

H2: Responsiveness will positively influence performance resulting from the acquisition of ISMS certification. Responsiveness dimension indicates an improved level of ability to respond to changes in the external environment and incidents by acquisition of ISMS certification.

H3: Tangibles will influence performance resulting from the acquisition of ISMS certification. The tangibles dimension indicates an improved level of security organisation competency and the establishment of a security strategy and goal by the acquisition of ISMS certification.

H4: Specialty will positively influence performance resulting from the acquisition of ISMS certification. In this study, we changed over from the assurance dimension, which evaluates ways and means to gain customers' trust in the original SERVQUAL, to the specialty dimension. Specialty dimensions can be defined as the level of enactment of the law and policy and organisational competency to protect information assets from external threat. Sub-items associated with specialty dimensions consist of policy, management systems and security level.

H5: Continuity will positively influence the performance resulting from the acquisition of ISMS certification.

Although a continuity dimension doesn't appear in the SERVQUAL model, we added one because security asks not for one-time management but for continuous concern and investment. A continuity dimension has a relevance to whether or not employees perform a job not through one-time reinforcement of security competency but through company training and company culture formation with continuous interest in security by acquisition of ISMS certification.

Finally, security performance is the concept of overall performance of security by acquisition of ISMS certification, and it can be measured by whether the security goal, efficiency of security investment and security competency

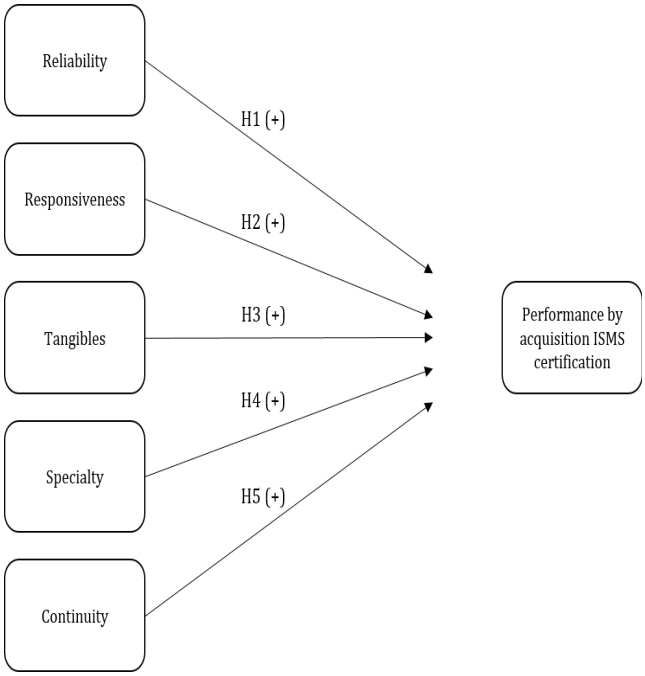

Figure 1. The research model.

are improved. Table 1 summarizes the preceding studies on SERVQUAL for information security.

4. Research Methods

In this study, SmartPLS v3.1.6 of the PLS program is used for analysis of reliability and validity. PLS doesn't ask for the strict observance of a minimum sampling number and normal distribution, and carries out assessment of structural models and measurement models at the same time. We selected 252 organizations (264 services) specifying the e-mail address of the person in charge of information security on the website of an organization acquired and holding ISMS certification, and conducted a survey of them from 1 September 2014 to 21 November 2014 by e-mail. We collected a total of 26 questionnaires for a return rate of about 10%. Of these, 25 copies, excluding one copy of unreliable response, were used to analyze the results. The responding organizations are classified based on whether or not they are listed on the KOSDAQ stock market and securities market, the number of employees and industry sector. Five organizations are listed on the market, while the other 20 organizations are not (public institutions are classified with unlisted organizations). ISMS certification coverage is divided into all and partial enterprise departments. Eight organizations acquired

Table 1. Measurement instrument

Dimensions	Items	Related research
Reliability	Trust in internal information security management systems increased.	Hone and Eloff[16]
	Employees' trust in internal managerial, technical, physical security regulations increased.	Saint [17]
	Global business opportunity is expanded by the acquisition of ISMS certification.	Helokunnas and Kuusisto[18]
	Communication channels with customers and feedback structure are improved.	Humphreys[19]
Responsiveness	We take an immediate measure in advance by expecting security incidents.	Gerber et al.[20]
	We can respond quickly when security incidents occur.	
	We can respond to changes in security technology quickly and flexibly.	
	Security incidents such as information leakage decreased.	Gordon and Loeb[21]
Tangibles	Liability and authority for task and organisation management related to information security.	Posthumus and Solms[22]
	Documentation and management of document are aggressively achieved.	Hone and Eloff[16]
	Methods to comply with security regulation by regularisation of security works are clear.	Hone and Eloff[16]
	We have enterprise work processes (such as a methodology) appropriate to security activity.	Solms[23]
	A cooperative system for security works between departments is constructed and established.	Werlinger et al.[24]
	We can construct information security policies and a management system properly.	Hone and Eloff[16]
Specialty	Employees' awareness about security and formation of security culture at the office are improved.	Vroom and Solms[25]
	Employees have special knowledge about managerial, technical and physical protective action of certification examination criteria and rules and legal framework.	Saint[17]
	Works such as risk analysis and evaluation are conducted properly.	Blakley et al.[26] Karabacak and Sogukpinar[27]
	The ability to manage cooperative firms is improved.	Khalfan[28]
Continuity	Management's concern and awareness are increased.	Gonzalez[29] , D'Arcy et al.[30]
	Employees are participating voluntarily in information security education and training,	
	Top management's active participation and investment in information security education and security are increased.	
	Effective implementation of information security policy and feedback activity of related laws and rules are conducted.	Humphreys[19]
	Continuous information security activity is conducted through internal audit.	
Security performance	The security level (confidentiality, availability, integrity) of the enterprise is improved.	Helokunnas and Kuusisto[18]
	Efficiency of investment in security is increased.	Purser[31]
	Organisational security competency is improved.	Baskerville and Siponen[32]

ISMS certification for all enterprise departments, while 17 organizations got the certification for partial enterprise departments. The number of employees is divided into "less than 50", "less than 100", "less than 300", "less than 500" and "more than 500". Lastly, the number of information and communication service providers is the highest in the industry sector, followed by public organizations, education, financial company, wholesale and retail business, manufacturer, culture, logistics and collection agencies.

Table 2. Descriptive statistics for the measurement items

Dimensions	Items	Mean	Variance
Reliability	Trust in internal information security management systems increased.	4.79	1.32
	Employees' trust in internal managerial, technical and physical security regulations increased.	5.00	1.65
	Global business opportunity is expanded by the acquisition of ISMS certification.	3.63	2.25
	Communication channel with customers and feedback structure are improved.	4.63	1.90
	Subtotal	4.51	
Responsiveness	We take an immediate measure in advance by expecting security incidents.	4.50	1.91
	We can respond quickly when security incidents occur.	4.54	2.17
	We can respond to changes in security technology quickly and flexibly.	4.25	2.54
	Security incidents such as information leakage decreased.	4.79	2.00
	Subtotal	4.52	
Tangibles	Liability and authority for task and organisation management related to information security.	5.21	1.39
	Documentation and management of documents are aggressively achieved.	4.75	1.85
	Methods to comply with security regulation by regularisation of security works are clear.	5.25	1.41
	We have enterprise work process (such as a methodology) appropriate to security activity.	4.79	2.00
	A cooperative system for security works between departments is constructed and established.	4.83	2.06
	We can properly construct information security policies and management system.	5.21	0.96
	Subtotal	5.01	
Specialty	Employees' awareness about security and formation of security culture at the office is improved.	5.00	2.17
	Employees have special knowledge about managerial, technical and physical protective action of certification examination criterion and rules and legal framework.	4.79	2.09
	Works such as risk analysis and evaluation are conducted properly.	4.96	1.43
	The ability to manage a cooperative firm is improved.	4.17	1.62
	Subtotal	4.73	
Continuity	Management's concern and awareness are increased.	5.29	1.43
	Employees are participating voluntarily in information security education and training,	4.83	1.80
	Top management's active participation and investment in information security education and security are increased.	4.92	2.17
	Effective implementation of information security policy and feedback activity of related laws and rules are conducted.	4.75	1.59
	Continuous information security activity is conducted through internal audit.	5.08	1.73
	Subtotal	5.57	
Security performance	The security level (confidentiality, availability, integrity) of the enterprise is improved.	5.17	2.23
	Efficiency of investment in security is increased.	4.38	1.07
	Organisational security competency is improved.	4.83	2.58
	Subtotal	4.79	

Table 3. Internal consistency analysis

	AVE	Composite Reliability	Cronbach's alpha
Reliability	0.697	0.902	0.859
Responsiveness	0.886	0.969	0.956
Tangibles	0.718	0.938	0.923
Specialty	0.614	0.864	0.789
Continuity	0.751	0.938	0.917
Security performance	0.800	0.923	0.875

Table 4. Confirmatory factor analysis

	Reliability	Responsiveness	Tangibles	Specialty	Continuity	Security performance
A1	0.837					
A2	0.874					
A3	0.815					
A4	0.812					
B1		0.967				
B2		0.979				
B3		0.948				
B4		0.868				
C1			0.840			
C2			0.799			
C3			0.943			
C4			0.886			
C5			0.794			
C6			0.812			
D1				0.765		
D2				0.817		
D3				0.739		
D4				0.810		
E1					0.889	
E2					0.835	
E3					0.940	
E4					0.837	
E5					0.826	
F1						0.886
F2						0.871
F3						0.925

5. Results

5.1 Descriptive Statistics

Statistical analysis results of the organizations that responded to the survey by item are presented in Table 2. Response score ranges from 1 (strongly negative) to 7 (strongly positive). Improvement of security performance by the acquisition of ISMS certification scores 4.79. Continuity (5.57) received the highest performance score by dimension, followed by tangibles (5.01), specialty (4.73), responsiveness (4.52) and reliability (4.51).

5.2 Reliability and Validity Analysis

The PLS analysis requires testing the internal consistency, convergent validity and discriminant validity of question

Table 5. Discriminant validity analysis

	Reliability	Responsiveness	Tangibles	Specialty	Continuity	Security Performance
Reliability	(0.835)					
Responsiveness	0.491	(0.941)				
Tangibles	0.873	0.575	(0.847)			
Specialty	0.694	0.665	0.778	(0.783)		
Continuity	0.908	0.612	0.966	0.775	(0.866)	
Security performance	0.493	0.825	0.556	0.856	0.598	(0.894)

※ Numerical value inside ( ) is the square root of AVE.

Table 6. Hypothesis testing

Hypothesis		Path coefficient	t-value	Results
H1	Reliability → Security performance	-0.085	0.547	Not supported
H2	Responsiveness → Security performance	0.465	2.915	Supported
H3	Tangibles → Security performance	-0.574	1.805	Not supported
H4	Specialty → Security performance	0.802	3.647	Supported
H5	Continuity → Security performance	0.323	1.105	Not supported

※ Correlation is significant at the 0.05 level (t-value > 1.96).

items and constructs. To test the internal consistency, reliability, responsiveness, tangibles, specialty, continuity and security performance were analyzed in terms of Fornell and Larcker's composite reliability and internal consistency[33]. Table 3 shows the analysis results. The composite reliability proved to be higher than 0.7, the reference standard suggested by Nunnally and Thompson et al. Cronbach's alpha, widely in use for testing reliability, proved to be 0.7 and higher, indicating the internal consistency was good[34-36].

The convergent validity was tested with AVE and factor loadings of constructs. As in Tables 3 and 4, the AVE proved to be higher than 0.5, the reference standard suggested by Fornell and Larcker and Chin. All factor loadings of constructs proved to be higher than 0.7, the reference standard suggested by Fornell and Larcker[32,35]. As in Table 5, the discriminant validity was tested based on whether the square root of every AVE marked on the diagonal axis of correlation coefficients was bigger than the coefficients of the other constructs. As a result, the smallest square root of AVE (0.783) was not bigger than the largest coefficient (0.966), indicating failure to verify the discriminant validity. Nevertheless, the constructs and question items used here were found to be fit for the structural model analysis as their internal consistency and convergent validity met all the reference requirements excluding discriminant validity.

5.3 Structural Model Analysis

In the PLS analysis, the explanatory power of the path model is expressed as the explained variance, $R2$[37]. The PLS analysis of R^2 showed reliability, responsiveness, tangibles and specialty, and continuity explained 90.3% of security performance, which exceeded Falk and Miller's power (10%)[38]. Next, in Goodness-of-Fit (GoF) testing, the impact of GoF was 0.820, which was higher than Wetzels et al. reference standard, indicating a very high goodness of fit for the model[39]. With the PLS analysis, path coefficients and their significance were tested. For this, the full sample was used to find out the path coefficients of the structural model. The bootstrapping provided in PLS was used to calculate the t-value for the path coefficient. Table 6 summarises the analysis results. The results of the analysis are as follows in the order of

hypotheses. In short, 3 out of 5 hypotheses set up in the present study except the hypothesis 1, 3 and 5 were found to be significant and adopted.

6. Results

In the present study, we found that investment and concern in security can influence organisational security performance based on prior research, and developed survey items for performance measurement by acquisition of ISMS certification. We conducted surveys of organisations that required ISMS certification and tried to find some factors recognisable as a performance of ISMS certification. The result of the experiment was that factors influencing security performance are responsiveness and specialty. Two factors have a positive correlation with security performance, and it turned out that organisations perceive the improvement of security performance level when the ability of responding to security accidents and changes in the external environment is improved and professional competency in security is strengthened.

We additionally conducted a survey of 25 organisations that responded to prior surveys to deduce an improvement plan for ISMS certification. A total of 13 organisations responded to our additional survey. An improvement plan of K-ISMS made based on this questionnaire is as follows: In the first place, information security policy, organisation and goal, which are mandatory factors needed to get the certification, have a negative correlation with security performance. An ISMS aims for the systematic construction of information security through the establishment of an information security policy, organisations and goal. However, tangibles related to the systematic construction of information security have a negative relationship with security performance by acquisition of an ISMS certification. It follows from what has been said that the construction of a formal system through acquisition of ISMS certification and made by a consultant in a short time act as an obstacle for security works. Four of 13 organisations introduced ISMS certification on their own, and the rest acquired the certification with the help of a consulting firm. Organisations need to involve employees in real construction of ISMS rather than to get the aid of an external consulting firm, and just to observe the guidelines the government sets in order to overcome the problems of ISMS. Also, the certification agency has to try to contribute to the practical improvement of security levels by applying to a rigid certification criterion reflecting the distinct characteristics of the industry to which organisations belong. In the second place, specific campaign activity on ISMS certification is needed. Only 7 of 13 organisations answered "agree" or "strongly agree" for the question, "Did your organisation get a beneficial effect on security by acquiring ISMS certification?" We may say that the person in charge of security assesses the effects of the acquisition of ISMS certification to be low. If public recognition of ISMS certification through campaign activity were to increase, organisations that have acquired ISMS certification can get the trust of the persons concerned and their customers. In short, there is no need to urge strict regulation. Then, many organisations will make an effort to acquire ISMS certifications, and as a result, these efforts will result in a rise in the security level across society. In the third place, activation of security education is the critical element. Continuous information security education is needed on a continuing basis. Organisations have to provide all employees as well as the persons in charge of security with security education from a special educational institution. Consequentially, organisations can develop the ability to respond to recent information security issues and have a specialty of information security from continuing education. To the question, "What is the most important thing in security?" 8 of 13 organisations answered continuous and systematic security education and training. Its value is greatly higher in comparison with human resources management (2) and IT security management (3). Furthermore, as to the question, "What is the most important thing for additional supplement for information security?" many respondents answered, that reinforcement of information security (6) is more important than security audit and reinforcement of monitoring (4) and construction of software (3). Therefore, we can say there will be security advancement across society and improvement of satisfaction with the acquisition of ISMS certification.

Respondents were sensitive to the survey due to the characteristics of security. It's also not easy to find respondents as our research required the person in charge of security works to participate in the survey. Although a total of 25 copies are far too few, our research met the minimum requirement, exceeding 10% of the whole population. Following the development of precise weighted value of measurement through sufficient empirical data, organisations can measure security performance after the introduction of ISMS certification and prepare ways

to increase the satisfaction level of organisations that are required to get ISMS certification.

7. Acknowledgment

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Korean Government (NRF-2011-0025512). This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2015S1A5A2A01009763).

8. References

1. Kim SY, Park ST, Ko MH. Analysis of the competencies of information security consultants: Comparison between required level and retention level. Indian Journal of Science and Technology. 2015 Sept; 8(21):1-8.
2. Kim HA. The percentage of information security companies which got ISMS certification is zero. EDAILY. 2014 3 Mar.
3. Im H, Seo DH, Bark DH, Park ST. An exploratory study on service quality measurement of the fourth generation mobile telecommunication: The case of the Korean market. Indian Journal of Science and Technology. 2015 Sep; 8(21):1-12.
4. Parasuraman A, Zeithaml VA, Berry LL. A conceptual model of service quality and its implications for future research. Journal of Marketing. 1985; 49(4):41–50.
5. Parasuraman A, Zeithaml VA, Berry LL. SERVQUAL: A multiple-item scale for measuring consumer perceptions of service quality. Journal of Retailing. 1988; 64(1):12–40.
6. Dagger TS, Sweeney JC, Johnson LW. A hierarchical model of health service quality scale development and investigation of an integrated model. Journal of Service Research. 2007; 10(2):123-42.
7. Lee MA, Yom YH. A comparative study of patients' and nurses' perceptions of the quality of nursing services, satisfaction and intent to revisit the hospital: A questionnaire survey. Journal of Nursing Studies. 2007; 44(4):545-55.
8. Ahn T, Ryu S, Han I. The impact of web quality and playfulness on user acceptance of online retailing. Information and Management. 2007; 44(3):263-75.
9. Cristobal E, Flavian C, Guinaliu M. Perceived e-Service Quality (PeSQ): Measurement validation and effects on consumer satisfaction and web site loyalty. Managing Service Quality: An International Journal. 2007; 17(3):317-40.
10. Grigoroudis E, Litosa C, Moustakisa VA, Politisa Y, Tsironisa L. The assessment of user-perceived web quality: Application of a satisfaction benchmarking approach. European Journal of Operational Research. 2008; 187(3):1346-57.
11. Tan KC, Pawitra TA. Integrating SERVQUAL and Kano's model into QFD for service excellence development. Managing Service Quality: An International Journal. 2001; 11(6):418-30.
12. Lin H. Fuzzy application in service quality analysis: An empirical study. Expert Systems with Applications. 2010; 37(1):517-26.
13. Jiang JJ, Klein G, Christopher LC. Measuring information system service quality: SERVQUAL from the other Side. MIS Quarterly. 2006; 26(2):145-66.
14. Van Dyke TP, Kappelman KA, Victor R. Measuring information systems service quality: Concerns on the use of the SERVQUAL questionnaire. MIS Quarterly. 1997; 21(2):195-208.
15. Yoon S, Suh H. Ensuring IT consulting SERVQUAL and user satisfaction: A modified measurement tool. Information Systems Frontiers. 2004; 6(4):341-51.
16. Hone K, Eloff JHP. Information security policy - What do international information security standards say? Computers and Security. 2002; 21(5):402-9.
17. Saint R. Information security management best practice based on ISO/IEC 17799. Information Management Journal. 2005 Jul/Aug; 62-6.
18. Helokunnas T, Kuusisto R. Information security culture in a value net. Proceedings of Engineering Management Conference; 2003. p. 190-4.
19. Humphreys E. Information security management standards: Compliance, governance and risk management. Information Security Technical Report. 2008; 13(4):247-55.
20. Gerber M, Solms RV. Information security requirements – interpreting the legal aspects. Computers and Security. 2008; 27(5-6):124-35.
21. Gordon LA, Loeb MP. The economics of information security investment. ACM Transactions on Information and System Security. 2002; 5(4):438-57.
22. Posthumus S, Solms RV. A framework for the governance of information security. Computers and Security. 2004; 23(8):638-46.
23. Solms BV. Information security - A multidimensional discipline. Computers and Security. 2001; 20(6):504-8.
24. Werlinger R, Hawkey K, Beznosov K. An integrated view of human, organizational and technological challenges of IT security management. Information Management and Computer Security. 2009; 17(1):4-19.
25. Vroom C, Solms RV. Towards information security behavioral compliance. Computers and Security. 2004; 23(3):191-8.

26. Blakley B, McDermott E, Geer D. Information security is information risk management. Proceedings of the 2001 Workshop on New Security Paradigms; 2001. p. 97-104.
27. Karabacak B, Sogukpinar I. ISRAM: Information security risk analysis method. Computers and Security. 2005; 24(2):147-59.
28. Khalfan AM. Information security considerations in IS/IT outsourcing projects: A descriptive case study of two sectors. Journal of Information Management. 2004; 24(1):29-42.
29. Gonzalez JJ, Sawicka A. A framework for human factors in information security. Proceedings of the 2002 WSEAS International Conference on Information Security; Rio de Janeiro. p. 2002.
30. D'Arcy J, Hovav A, Galletta D. User awareness of security counter measures and its impact on information systems misuse: A deterrence approach. Information Systems Research. 2009; 20(1):79-98.
31. Purser SA. Improving the ROI of the security management process. Computers and Security. 2004; 23(7):542-6.
32. Baskerville R, Siponen M. An information security meta-policy for emergent organizations. Logistics Information Management. 2002; 15(5-6):337-46.
33. Fornell C, Larcker D. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research. 1981; 18(1):39-50.
34. Nunnally JC. Introduction to Statistics for Psychology and Education. NY: McGraw-Hill; 1975.
35. Thompson R, Barclay DW, Higgins CA. The partial least squares approach to causal modeling: Personal computer adoption and use as an illustration. Technology Studies: Special Issue on Research Methodology. 1995; 2(2):284-324.
36. Chin WW. The Partial Least Squares Approach to Structural Equation Modeling in Modern Business Research Methods. In: Marcoulides GA, editor. Manwah, NJ: Lawrence Erlbaum Associates; 1998. p. 295-336.
37. Chin WW, Gopal A. Adoption intention in GSS: Importance of beliefs. Data Base Advance. 1995; 26(2-3):42-64.
38. Falk RF, Miller NB. A Primer for Soft Modeling. University of Akron Press; 1992.
39. Wetzels M, Odekerken-Schroder G, Van Oppen C. Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. MIS Quarterly. 2009; 33(1):177-95.