A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance

Cheol-Soon Park[†] **and** **Sang-Soo Jang**[††] **and** **Yong-Tae Park**[†††]

KCC(Korea Communications Commision), Korea

KISA(Korea Internet & Security Agency), Korea

Seoul National University(SNU), KOREA

Summary
While the rapid spread of Internet usage enables many tasks that can be performed in only offline environments to be performed in cyber space as well, new security threats such as hacking and viruses have also increased. For that reason, enterprises and organizations recently require comprehensive and systematic information security management system (ISMS) instead of sporadic security management. Consequently, the Information Security Management System (ISMS) certification system has been in effect in Korea since July 2001. As of December 2009, 76 enterprises have been certified, and more than 100 ISO27001 certifications have been issued. As such, since the introduction of the ISMS certification system in Korea, the demand for the certification has been steadily increasing, and it is now recognized as an integral means of strengthening the competitiveness in an enterprise. However, the qualitative aspects of certification regarding the benefit of ISMS have been continuously questioned by actual customers. In order to clarify the situation and remove such doubts, this study will substantiate the fact that development and certification of ISMS positively affect the business performance of enterprises so that they will recognize the effect of obtaining ISMS certification and eventually prevent security accidents and improve their business performance by developing ISMS.
.

Key words:
Information Security; Information Security Management System(ISMS), ISMS Certification, Business Performance

1. Introduction

Development of information and communication technology and the spread of the Internet are not only remarkably changing individual lifestyles and business conduct but also explosively creating new businesses. However, adverse changes and effects such as hacking, viruses and personal information leaking are also rapidly increasing.

Therefore, it has become a key task for governments, enterprises and individuals depending on the Internet to effectively cope with such problems. Particularly, enterprises corresponding to a backbone of a modern society recognize the information security management as one of business management factors. Furthermore, in the security management, external independent evaluation or certification is gradually emphasized. For these reasons, the information security management system (ISMS) certification system has been in effect in Korea since July 2001. As of December 2009, 76 enterprises have been certified, and more than 100 ISO27001 certifications have been issued. Since the ISMS certification system was introduced in Korea, the demand for the certification has been steadily increasing, and it is recognized as an important means of enterprise competitiveness.

Although ISMS certification system is used as a means to protect business information assets and to improve the competitiveness of enterprises, its qualitative aspects of certification regarding the effectiveness of ISMS are questioned by actual customers.

In particular, even though the ISMS was meant for enterprises to use as an opportunity for innovation in their operations and to improve customer satisfaction and public trust by increasing service quality; unfortunately, oftentimes enterprises tend to focus only on attaining the certification, losing the original intent of the certification.

That may be the reason why the number of ISMS certified enterprises is not increasing exceedingly, as the enterprises can not recognize the need to strengthen their competitiveness through the certification. Therefore, it is time to induce enterprises to use ISMS certification as a means to survive rather than to aim at only obtaining the certification. In other words, enterprises need to develop the information security system linked to their businesses in order to establish a basis for information security activities and to enable sustained growth.

Studies to secure the effectiveness of domestic ISMS certification systems and continued efforts for information security are important issues for strengthening the competitiveness of an enterprise. Therefore, this study will substantiate the fact that development and certification of ISMS positively affects the business performance of enterprises so that they will recognize the effect of attaining ISMS certification and eventually prevent

Manuscript received March 5, 2010
Manuscript revised March 20, 2010

security accidents and improve their business performance by developing ISMS.

2. Theoretical Background

2.1 ISMS Certification

ISMS includes a series processes for systematically establishing, documenting and continuous managing procedures to improve the safety and reliability of the assets of an enterprise, and for realizing information confidentiality, integrity and availability which are the goals of information security, and includes the continuous enhancement of information security.

The ISMS certification is a system in which a third party certification agency objectively and independently assesses whether ISMS conforms to a certain certification criteria and to certifying that it meets those standards. In Korea, Article 47 Certification of Information Security Management System in the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. provides the legal basis. It stipulates that the Korea Internet & Security Agency under the Korea Communications Commission will certify the system by evaluating whether the comprehensive management system, including the technical and physical security measures, satisfy the certification criteria.

2.2 ISMS in ISO/IEC

ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) formed a Joint Technical Committee and announced ISO/IEC27001 (Information security management systems - Requirement) and ISO/IEC27002 (Code of practice for information security management) as the international standard for ISMS in 2005.

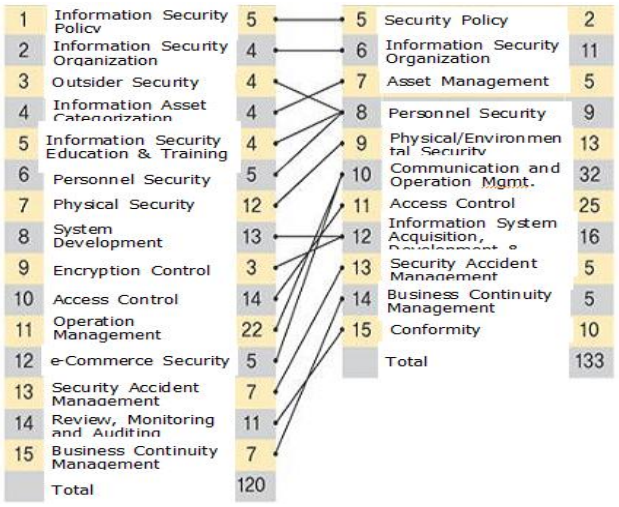
This standard was upgraded from BS (British Standard) 7799 which consists of reference cases in BS7799 Part 1 and certification criteria in BS7799 Part 2. BS7799 Part 1 first became the international standard as ISO/IEC17799 while BS7799 Part 2 became the international standard later. After a revision, the international standards were changed into ISO/IEC27001 which is currently used as the certification criteria and ISO/IEC27002 which is a set of reference cases in 2005.

To have an information security management system internationally certified, the internal system must be established in accordance with the execution guidelines (ISO27002) of Part 1 and must be evaluated in accordance with Part 2 (ISO27001) based on the execution record during a certain period.

2.3 Comparison of ISMS

In order to certify the information security management system in domestic and foreign countries, an information security management system optimized to the environment of certifying agencies in each country must be developed and operated such that certification evaluation criteria of each country are satisfied. The certification evaluation criteria mentioned above consist of security control items, and each security control item defines the detailed security factors required for executing the security task.

When comparing the detailed security requirements for control items consisting of certification standards in domestic and foreign countries, the control items can be matched as shown in <Figure 1 - 1>. Although the control items are categorized into 11 or 15 subjects and detailed items are defined, the security requirements consisting of each control item are almost similar.



<Figure 1-1> Mapping of Korea's ISMS and ISO 27001 Control Items.

In Korea, the ISMS is designed to be suitable for the domestic environment, including all international standards (ISO27001). The ISMS includes 5 management processes (14 steps), documentation and 15 domains. It is designed to emphasize 4 areas (3. outsider security, 5. information security education and training, 9. encryption control, and 12. e - commerce security) added to 11 items of ISO27001.

While the number of control items does not necessarily raise or lower the security level, Korea's ISMS consists of 442 detailed checklist items, more than that of ISO27001. The security level could be systemically improved by

selecting the control items needed for the information security management system of each enterprise and then by establishing and executing the management system of each security requirement.

In Korea, both ISMS and ISO27001 certifications are accepted. ISO27001 certification is issued by certifying agencies such as BSI Korea (http://asia.bsi - global.com/Korea/index.xalter) and DNV (http:// www.dnv.co.kr) while ISMS certification is issued by KISA (Korea Internet & Security Agency, http:// www.kisa.or.kr). An organization requesting the certification agrees on certification scope and schedule with the certifying agency and signs a contract.

After the certification is obtained, it can be maintained only when the post evaluation having a short period of time is carried out every six months for ISO27001 and every year for Korean ISMS. The post evaluation is conducted to inspect the maintenance of continuous information security management system. The short post evaluation is conducted in the same way as that of the initial evaluation just like the same as the initial evaluation. The certification can be withdrawn if a serious problem is found during the post evaluation. The certification is valid for 3 years. Reevaluation is needed after the expiration. It is also needed when a major change to the certification scope occurs.

2.4 Purpose and Expected Benefits of ISMS

The major motivation or benefits of enterprises attaining ISMS certification can be summarized as follows:

First, the potential loss from the possible threat of the current information system operation can be quantitatively predicted and followed up. Administrators and users can understand the risk level and reduce the risk possibility. Second, the stability, effectiveness, efficiency and reliability of the organization's assets can be improved. Third, visual presentation of risk level through risk analysis and evaluation can inspire the security awareness of the administrators and users. Fourth, it supports decision making to establish the security measures with consideration to priority and cost/effectiveness aspects of the high risk areas. Fifth, certification by the government means that the enterprise is properly managing information security thus improving public trust and competitiveness. Sixth, the enterprise can notify the users or trade partners that it is complying with the legislation, procedure or guidelines to improve their corporate image. Seventh, it can substantially support the corporate goal.

However, despite the clear benefits as mentioned above, such benefits may not be clearly visible to the enterprises obtaining the certification. Therefore, it is not easy to rationalize the information security management system certification by using conventional cost/effectiveness analyses and it is also difficult to analyze and manage the tangible and intangible measurement factors that can be additionally attained.

2.5 Preceding Studies of Benefits of Information Security

As of now, the studies of the effects of ISMS certification on an enterprise′s performance are inadequate. However, there are numerous and various studies of information security performance measurement which are prerequisites of ISMS performance measurement, which is as follows.

Gi Hyang Hong (2003) showed that, although both information security control and activity affect the performance of information security, the activities have more direct effect than controls. He also showed that information security control can regulate the effect of the activities on the performance or indirectly affect the performance through the activities, thus verifying the effects of the control on the performance. Furthermore, the study confirmed that the information security control, activity and performance factors form a certain pattern to create internal cohesion between one another and that the information security status of an organization can be categorized by high and low level type.

Il Soon Shin (2005) surveyed the economic efficiency studies of information security in Korea, and classified and analyzed the international studies by damage estimation from cyber attack, study of economic efficiency of privacy, and study of information security cost/investment value according to their subjects. The paper also clarified the need for economic analysis and an approach towards information security and presented the basis for enacting the appropriate information security policy suitable for the national and enterprise wide level as well as practical measures to ensure information security.

KISA (2006) measured the social and economic loss from Internet attack to estimate the actual cost from the loss and recovery. The study identified the variables of loss costs and recovery costs and presented the appropriate countermeasures when the same accident occurs. Direct costs of attack may include the loss cost and recovery loss while the indirect costs include the degradation of production efficiency, data loss/recovery costs, and liabilities.

Kim Jeong-deok/Park Jeong-eun (2003) and Seon Han-gil (2005) verified the effectiveness of estimating the benefit of information security investment in terms of TCO (Total Cost of Ownership) such as the reduction of information security accidents, reduction of business opportunity loss, reduction of asset loss, reduction of damage from competition, reduction of image degradation and time to recover from the accident.

KISA (2006) measured national information security level in three indices of information security base (T), information security environment (E) and adverse effect of informatization (N). The information security base index measures the system and data protection while the information security environment index measures the professional manpower ratio and information security budget ratio and adverse effect index of informatization measures combating hacking, viruses and personal information violation ratio.

Ekenberg et al (1995), in order to measure the effectiveness of risk analysis activity, measured the benefits of the economic, technical, environmental, social and psychological aspects of corporations, customers, vendors, contractors and other stakeholders by using the probability scale. They presented that it is possible to define the benefits of information security from the aspect of various stakeholders. Parker (1997) showed that information security promotes the use of information technology, maintains the competitive advantage, improves public image, and protects the enterprise′s assets. He presented the promotion of information technology usage and improved effectiveness of asset protection as the goal of information security of the enterprise.

As a study of manpower related to benefits of internal organization in benefits of information security, Frank (1991) et al observed the effect of custom, PC knowledge, expertise of PC usage and official policy on manpower security. The study showed that the custom and PC knowledge improves the manpower security while the official policies affect manpower security when there is no custom. Therefore, information security policy and the goal of information security control like custom contribute to preventing information security accidents by personnel.

As a study of information security affecting the benefits of an external organization in benefits of information security, Sinangin (2002) showed that personnel training and information security accident policy can prevent the additional damage and public image degradation from accidents. He defined the goal of information security activities as not only the prevention of loss but also management of information security image to the public.

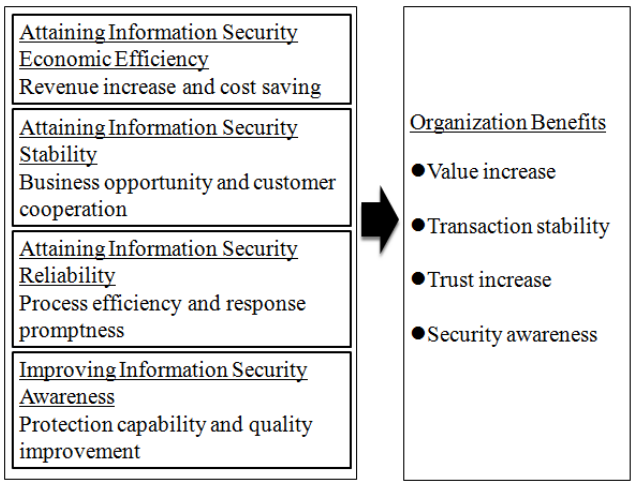
3. Study Model, Assumptions and Study Method

3.1 Study Model

This study intends to show the effects both of securing economics, stability, reliability and of recognizing the information security on enterprise performance to verify that ISMS certification does affect the enterprise performance.

Recently, many companies are continuously investing in ISMS as a means to improve the information security management process so as to protect the enterprise′s information assets and strengthen their competitiveness. Particularly, recognizing that product oriented technical response has its limitations in efficiently coping with attacks such as the 7.7 DDos attacks which are becoming more intellectualized, interest in developing information security management systems are increasing. Considering the social responsibility of enterprises according to class action suits against accidents of personal information leakage, the issue of information security is accepted as a matter of survival for the enterprise. ISMS certification can significantly affect enterprise performance, and it is particularly important to the IT service providers who are heavily dependent upon the Internet. However, acquiring ISMS certification per se does not ensure a continuous competitive advantage for an enterprise, and even the companies attaining the same certification show different effects after certification.

Therefore, this study intends to select the appropriate variables by using the findings of the preceding information security performance measurement studies and theoretical consideration, and then illustrate how ISMS certification affects an enterprise′s performance after obtaining the certification as shown in <Figure 3-1>. As factors affecting the organization′s performance, 8 independent variables (measured indices) and 4 dependent variables (organization performance indices) were categorized into similar index groups. <Figure 3-1> shows the categorized study model.



<Figure 3-1> Study Model

3.2 Assumptions

To study the relations among the variables such as the information security economic efficiency, stability, reliability and awareness, etc.. presented in the study model, the following assumptions were made in 8 steps:

①Assumption 1: The sales increase will affect value increase.

② Assumption 2: Cost savings will affect value increase.

③ Assumption 3: Business opportunity will affect transaction stability.

④Assumption 4: Customer cooperation will affect transaction stability.

⑤ Assumption 5: Process efficiency will affect trust increase.

⑥ Assumption 6: Response quikness will affect trust increase.

⑦ Assumption 7: Protection capability will affect security awareness increase.

⑧ Assumption 8: Quality improvement will affect security awareness increase.

3.3 Measurement Method

As the concepts used in the model and assumptions consist of various abstract concepts, they are measured through surveys shown in <Table 3-1> so as to verify the study assumptions.

<Table 3-1> ISMS Benefit Measurement Method

Concept	Variable	No. of Measured Items	Measurement
Attaining information security economic efficiency	Sales increase	2	Likert 7 Point Scale
	Cost savings		
Attaining information security stability	Business opportunity	2	
	Customer cooperation		
Attaining information security reliability	Process efficiency	2	
	Response quickness		
Improving information security awareness	Protection capability	2	
	Quality improvement		

To analyze the benefits of ISMS certification before and after the induction of the ISMS certification, the staff in charge of certification at 76 enterprises which have obtained ISMS certification were surveyed for 8 days between November 25, 2009 and December 3 2009. <Table 3-2> shows the business types of the surveyed enterprises.

<Table 3-2> Business Types of Surveyed ISMS Certified Enterprises

Business	No. of Enterprises	Survey Response	Survey Response Rate (%)
Information Security Company	20	6	17
ISP/IDC	18	1	3
School (Remote School)	17	16	47
Banking/ Insurance	6	1	3
Medical/ Air Transport	4	3	9
Internet Shopping Mall/ Portal	3	3	9
Others	8	4	12
Total	76	34	100

<Table 3-3> shows the size of ISMS certified enterprises in terms of number of employees. 50% were small-to-medium sized companies while 41% were large companies.

<Table 3-3> Company Sizes of ISMS Certified Companies in Terms of No. of Employees

Type		Occurrence	Rate(%)
No. of Employees	Small-to-medium sized companies	38	50
	Large companies	31	41
	Others (No information on no. of employees)	7	9

※No. of ISMS certified enterprises in Korea: 76 (as of November 2009)

※Small-to-Medium Sized Company: A company with less than 300 full-time employees or fewer (Enforcement Decree of the Framework Act on Small and Medium Enterprises)

<Table 3-4> shows the size of ISMS certified enterprises in terms of sales. Small companies with sales less than KRW 10 billion were 16% of the total.

<Table 3-4> Sales of ISMS Certified Enterprises

Type		Occurrence	Rate (%)
2008 Sales	Less than KRW 5 Billion	8	11
	KRW 5 Billion ~ 10 Billion	4	5
	KRW 10 Billion ~ 15 Billion	2	3
	KRW 15 Billion ~ 20 Billion	2	3
	KRW 20 Billion ~ 25 Billion	1	1
	KRW 25 Billion or More	33	43
	Others (sales of remote school, etc.)	26	34

※No. of ISMS certified enterprises in Korea: 76 (as of November 2009)

<Table 3-5> shows certification maintenance period of ISMS certified enterprises. 24% had the certification for less than 1 year while 50% had it for 3 years or longer.

<Table 3-5> Certification maintenance Period of ISMS Certified Enterprises

Type		Occurrence	Rate (%)
Certification Maintenance Period	Less than 1 Year	18	24
	1 ~ 3 Years	20	26
	3 ~ 6 Years	37	49
	7 Years or Longer	1	1

※No. of ISMS certified enterprises in Korea: 76 (as of November 2009)

<Table 3-6> shows the qualitative average of the effectiveness before and after the acquisition of the ISMS certification through the survey in accordance with the variables. It shows a 68% increase of protection capability from the information security awareness improvement, a 53% increase of process efficiency from attaining information security reliability and a 43% increase of quality improvement from information security awareness.

<Table 3-6> Benefits of ISMS Certification

Variable	Independent Variable (Measured Factors)	Benefit
Attaining information security economic efficiency	Revenue increase	14% Increase
	Cost savings	30% Decrease
Attaining information security stability	Business opportunity	25% Increase
	Customer cooperation	39% Increase
Attaining information security reliability	Process efficiency	53% Increase
	Response quickness	37% Increase
Improving information security awareness	Protection capability	68% Increase
	Quality improvement	43% Increase

4. Verification and Interpretation of Results

4.1 Analysis Model

To study the effects of information security factors and benefits of ISMS certification by using the results in <Table 3-6>, 8 independent variables and 4 dependent variables are categorized into similar index groups and regression analysis was performed to estimate the economic benefits. <Table 4-1> shows the categorization and assumptions for regression.

<Table 4-1> Assumptions for Regression Analysis

Variable	Independent Variable (Measured Factors)	Dependent Variables	Assumption
Attaining information security economic efficiency	Sales increase	Value increase	Attaining the information security economic efficiency (sales increase and cost savings) will affect increasing the value.
	Cost savings		
Attaining information security stability	Business opportunity	Transaction stability	Attaining information security stability (business opportunity and customer cooperation) will affect increasing transaction stability.
	Customer cooperation		
Attaining information security reliability	Process efficiency	Trust increase	Attaining information security reliability (process efficiency and response quickness) will affect increasing the trust increase.
	Response quickness		
Improving information security awareness	Protection capability	Protection awareness	Improving information security awareness (protection capability and quality improvement) will affect increasing the protection awareness.
	Quality improvement		

4.2 Awareness Method

With regard to the information security factors affecting the organization performance, in order to test the assumptions of regression analysis, regression equation was designed as follows. Here, the regression analysis verifies how much the information security factors were affected in comparison with the time before the induction of the ISMS certification system:

① value increase = constant + sales increase + cost savings

② transaction stability = constant + cost savings + customer cooperation

③ trust increase = constant + process efficiency + response quickness

④ security awareness = constant + protection capability + quality improvement

The results of each and for each equation are shown in detail in the regression analysis result table. Here, dependent variables like value increase, transaction stability, trust increase and security awareness are the performance indices used to identify the degree of improvement as compared with the time before ISMS certification is induced. They reflect the result as it is obtained by applying the 7 point scale. Additionally, the independent variables like sales increase, cost savings, customer cooperation, process efficiency, response quickness, protection capability and quality improvement are the measuring indices needed to identify the degree of improvement as compared with the time before ISMS certification is induced. They also reflect the result as it is obtained by applying the 7 point scale. Since the same scale was applied to both dependent variables and independent variables, they are reflected as they are without having to normalize to a 100 point scale.

4.3 Analysis Result

The regression analysis was performed to verify the effects on organization performance using the valid samples of 34 enterprises identified by the survey of ISMS certified agencies. <Table 4-2> shows the result of regression analysis of the model design. As for the result of dependent variable value increases, the sales increase is 0.0005, significant in a 95% confidence interval while cost savings is 0.0565 in a 90% confidence interval. Furthermore, when the sales increase and the cost savings are changed by as much as a unit, the beta value indicates that the value increases are increased by 0.78183 and 0.22258, respectively.

The value of P of the regression model is 0.0001 and shows the very significant result. R^2 was 52.68%. Although multi-co-linearity can be also determined by correlation analysis, it can also be evaluated using the VIF value. Since VIF was 1.27965, there was no multi-co-linearity.

<Table 4-2> Assumptions 1 and 2: Value Increase Regression Analysis Result

Variable	Constant	Sales Increase	Cost Savings	Regression Model
Freedom	1	1	1	2
Beta	28.06739	078183	022258	
Standard Error	4.67939	0.20196	0.11219	
T Value	6	3.87	1.98	
F Value				16.7
R2				0.5268
P Value	0.0001	0.0005	0.0565	0.0001
VIF	0	1.27965	1.27965	

<Table 4-3> shows the results of transaction stability regression analysis. Since the P values of business opportunity and customer cooperation are 0.0521 and 0.0346, respectively, business opportunity and customer cooperation affect transaction stability. In particular, When business opportunity and customer cooperation are increase by as much as a unit, the transaction stabilities are increased by 0.33361 and 0.38153, respectively. The regression model also showed a very significant result. It had R^2 of 39.18%, and there was no multi-co-linearity.

<Table 4-3> Assumptions 3 and 4: Result of Transaction Stability Regression Analysis

Variable	Constant	Business Opportunity	Customer Cooperation	Regression Model
Freedom	1	1	1	2
Beta	9.64706	0.33361	0.38153	
Standard Error	4.67939	0.20196	0.11219	
T Value	1.1	2.02	2.21	
F Value				9.66
R2				0.3918
P Value	0.2801	0.0521	0.0346	0.0006
VIF	0	1.40241	1.40241	

Table <4-4> shows the results of trust increase regression analysis. Although the process efficiency shows significant results, response quickness does not. When process efficiency is increased by as much as a unit, the increase was increased by 0.36907. The regression model was significant as the value of P was 0.0012. It has R^2 of 36%, and there was no multi-co-linearity.

<Table 4-4> Assumptions 5 and 6: Result of Trust Increase Regression Analysis

Variable	Constant	Process Efficiency	Response Quickness	Regression Model
Freedom	1	1	1	2
Beta	31.7719	0.36907	0.20704	
Standard Error	7.96772	0.18093	0.15536	
T Value	3.99	2.04	1.33	
F Value				8.44
R2				0.36
P Value	0.0004	0.0503	0.1927	0.0012
VIF	0	1.777171	1.777171	

<Table 4-5> shows the results of security awareness regression analysis. Although the protection capability shows significant results, quality improvement does not. However, the assumption is accepted because the regression model shows significant results. When protection capability is increased by as much as a unit, the security awareness is increased by 0.89569. It had R^2 of 78.41%, and there was no multi-co-linearity.

<Table 4-5> Assumptions 7 and 8: Result of Security Awareness Regression Analysis

Variable	Constant	Protection Capability	Quality Improvement	Regression Model
Freedom	1	1	1	2
Beta	4.1402	0.89569	0.1256	
Standard Error	6.72883	0.11288	0.11183	
T Value	0.62	7.93	1.12	
F Value				54.47
R2				0.7841
P Value	0.543	0.0001	0.2703	0.0001
VIF	0	1.40241	1.40241	

With the regression analysis, we have practically verified how much each of factors of ISMS certification system affecting the organization performance affects the improvement of organization performance after the certification.

Furthermore, the improvement of whole tasks after the certification was classified into 8 effect groups and analyzed. As a result, <Table 4-6> shows that 6 groups of value increase, information security economic efficiency, trust increase, information security stability, information security reliability and information security awareness had higher effects

In other words, the assumptions of the study model were verified to be acceptable. Therefore, we can conclude that attaining information security economic efficiency, attaining information security stability, attaining information security reliability and increasing information security awareness have all contributed to increase economic effect.

<Table 4-6> Summary of Study Model Verification Result

Assumption	Description	Result
1	Sales increase of ISMS certified enterprise will affect its value increase.	Accepted
2	Cost saving of ISMS certified enterprise will affect its value increase.	Accepted
3	Business opportunity of ISMS certified enterprise will affect transaction stability increase.	Accepted
4	Customer cooperation of ISMS certified enterprise will affect transaction stability increase.	Accepted
5	Process efficiency of ISMS certified enterprise will affect trust increase.	Accepted
6	Response quickness of ISMS certified enterprise will affect trust increase.	Rejected
7	Protection capability of ISMS certified enterprise will affect security awareness increase.	Accepted
8	Quality improvement of ISMS certified enterprise will affect security awareness increase.	Rejected

Verification of assumptions indicates that ISMS certification not only improves value increase, transaction stability, trust increase and security awareness but also contributes to increase economic benefits. Such effects of ISMS certification are judged to be greatly affected by policy, legislative and regulatory support or interest based on the following:

In Korea, ISMS certified companies receive various benefits such as added scores in bidding, procurement and credit evaluation by government agencies, credit evaluation agencies, technology guarantee funds and commercial enterprises. When an enterprise is ISMS certified, the enterprise is exempted from the mandatory information security safety assessment and receives a rate of discount in taking out an insurance related to information security. In particular, Such policies support and benefits are judged to positively affect the enterprise′s value increase and trust improvement.

The government is also promoting the information security safety assessment and the ISMS certification system studied in this paper, in order to improve the information security level of the ISP, IDC, shopping malls and other companies, the government made it mandatory for them to adopt a certain level of information security measures since the January 25 Internet attack in 2003 so that citizens can safely use the Internet. Such regulations are judged to have positive affects regarding value increase, transaction stability, trust increase and security awareness.

Therefore, analogizing from the result obtained by verifying the positive effects of each of the assumptions on the performance of ISMS certified enterprises through the regression analysis, it is necessary to let the public know the fact that the sales increase, cost savings, business opportunity, customer cooperation, process efficiency, and protection capability are directly caused by obtaining the economic efficiency of information security, i.e., an important issues of organization performance, let management strategy, information organization strategies and information security strategies of the enterprise consistently driven, activate ISMS certification throughout the enterprise, and thus emphasize the importance all the time.

4.4 Additional Analysis

● Additional Analysis 1

A regression analysis was performed to test how much the information security products and services for developing and certifying ISMS improve business after the certification. A simple regression analysis was performed since the a high correlation between the independent variables generates the multi-co-linearity and makes it difficult to apply the multiple regression analysis. As a result, the analysis result table is too enormous to be represented. Therefore, only the results will be briefly described here.

The improvement was verified with 12 performance indices which were divided into 8 categories. For the regression analysis, 8 categories, which correspond to dependent variables, including the value increase, the value, attaining information security economic efficiency, trust increase, attaining information security stability, transaction stability, attaining information security reliability, information security awareness increase and security awareness. Explanatory variables including 9 information security products and services such as the intrusion control system, intrusion detection system, intrusion prevention system, virtual private network (PVN), Web firewall, DB security solution, document security solution (DRM), access control system (physical security), and controlled security monitoring service. Additionally, the number of regular fulltime information security personnel, the number of fulltime outsourced and contracted personnel, the number of regular part time personnel, and the number of part time outsourced and contracted personnel were used for the analysis.

The results indicated that the intrusion prevention system, intrusion detection system, document security solution, all information security products and services, the number of regular fulltime personnel, the number of fulltime outsourced and contracted personnel, and total number of information security personnel affected the organization performance. Particularly, the document security solution and the number of outsourced and contracted personnel were found to have much effect on value increase.

● Additional Analysis 2

To quantitatively create the results verified through the study model, the economic effects before and after adopting the information security management system were tested on the basis of the financial data and surveys of actual companies.

In order to create the economic benefits of ISMS certification of the actual companies, the small-to-medium sized companies with ISMS certification were first selected as they would clearly show the economic benefits. Korea Computer Forms Co., Ltd. was selected based on the criteria of the companies with less effects from external regeneration factors (economic depression of the certain industry, management problem, etc.), companies with objective financial statements (external auditing companies), and conventional manufacturing companies (excluding the information security service providers). Then 15 companies of similar size in similar industries were extracted. Then the financial performance of Korea Computer Forms for 3 years after ISMS certification (2006~2008) was compared with that of the 15 companies. Since the volume of financial data is too large, only the results will be briefly described here.

The effects of ISMS certification on company performance were measured in terms of 3 major indices; improvement in efficiency of formalized business processes, increase of global business opportunities, and reduction of damage costs from intrusion accidents. <Table 4-7> shows the summary of the results. It shows that a total of KRW 228 million in economic benefits were realized annually for each certification.

<Table 4-7> The economic effects of ISMS certification on company performance

Index	Major Cause	Benefit	Total
Improvement of Efficiency of Formalized Business Process	Reduction of annual business process time	KRW 42 million	KRW 228 million
Increase of Global Business Opportunities	Increase of added value (productivity) of each employee	KRW 20 million	
Reduction of Damage from Intrusion Accident	Reduction of R&D loss cost	KRW 164 million	

Furthermore, the analysis indicated that ISMS certification resulted in expansion of information security products and services as well as the information security employment markets. As shown in <Table 4-8>, each certification resulted in an annual sales increase of KRW 215 million and the additional employment of 2.47 persons annually.

<Table 4-8> Economic Effects on the Information Security Industry

Effect	Category	Benefit	Total
Sales Increase of Information Security Industry	①Certification fee (KISA)	about KRW 7.3 million	about KRW 215.3 million
	②Information security consulting	about KRW 30 million	
	③Information security products and services costs	about KRW 178 million	
Employment Generation	④Information security consultant	0.36 M/Y	2.47 M/Y (Employment creation of 2.47 persons annually)
	⑤Information security evaluator	0.11 M/Y	
	⑥Information security staff	2 M.Y	

To summarize the economic effects of adopting the information security management system on the information security industry, each certification showed a benefit of KRW 430 million and additional employment of 2.47 persons annually.

5. Conclusion

This study intended to observe how information security certification affects an enterprise′s performance. To that end, the study model and assumptions including variables of attaining information security economic efficiency, attaining stability, attaining reliability and information security awareness were developed and verified. The results can be summarized as follows:

First, attaining information security economic efficiency positively affects value increase. When an enterprise receives ISMS certification, there are positive public relations effects of better corporate image, followed by additional customers, resulting in sales increase. It showed that preventing intrusions would have cost saving effects as damage from potential accidents can be prevented.

Second, attaining information security reliability affects an increase in transaction stability. While ISMS certification directly affects an increase in corporate value, attaining the information security reliability affects transaction stability, thus helping the stability of the information assets of the enterprise.

Third, attaining information security reliability positively affects an increase in trust. Although business process efficiency, a lower level variable, from ISMS certification is shown to affect an increase in trust, it had no effect on response quickness.

Fourth, increasing information security awareness positively affects an increase in security awareness. Having ISMS certification provided motivation for all employees and thus affected strengthening employee capability and awareness of information security. However, it is shown to have no effect on quality improvement.

In conclusion, each organization performance factor affected organization performance after certification was tested using the regression analysis. By grouping the factors in 8 categories and analyzing the improvement after certification, 6 groups increased in value-- attaining information security economic efficiency, increasing reliability, attaining information security stability, attaining information security reliability and increasing information security awareness were found to be highly affected. In other words, the assumptions of the study model were verified to be acceptable. Therefore, attaining information security economic efficiency, attaining information security stability, attaining information security reliability, and increasing information security awareness all contributed to an increase in economic effects. Furthermore, the additional analysis showed that the intrusion prevention system, intrusion detection system, document security solutions, all information security products and services, the number of regular fulltime personnel, the number of outsourced and contracted fulltime personnel, and the total number of information security staff are shown to affect an enterprise′s performance. Particularly, in terms of the information security products and services group and the personnel group, the document security solution was highly effective in the information security products and services group while the number of fulltime personnel was more effective than the number of part time personnel in the personnel group.

As a quantitative result of the additional study model using the financial data and surveys from actual companies, the total economic effects regarding certification of the enterprises and the information security industry was shown to be KRW 443 million and to generate additional employment of 2.47 persons annually.

The results of this study can be referred to for effective information regarding security activities and decision making as to which directions to take to attain the certification of an information security management system and to form foundational measures to improve performance.

As it was difficult to translate the benefits of information security management systems into values, this study analyzed and presented the actual outcomes brought about by ISMS certification in order to actively induce the

voluntary development and certification of information security systems by enterprises and to establish a basis for the overall growth of the information security industry through additional employment and revenue increase.

This study of the effects of information security systems on enterprise performance had some limitations. First, the lack of any preceding studies of information security management systems′ benefits and measurements meant there was no reference model to be used as the standard. Second, the model focused on the economic performance of the enterprise and faced limitations in specifically measuring the enterprise′s unique characteristics.

Therefore, it is envisaged that more studies of benefits and measurements of ISMS certification should be conducted and the various measurement models befitting the particular characteristics of the information security support arena be developed to be used in measuring information security benefits not only for enterprises but for the country as a whole. Furthermore, international guidelines for information security management systems′ benefits and measurements should be created to help in developing and enhancing system models to be used as the international standard.

References

[1] Ekenberg, L., Oberol, S. & Orci, I., *" A cost model for managing information security hazards"*, Computer Security, Vol. 14, pp.707-717, 1995.

[2] Frank, J., Shamir, B., & Briggs, W., *"Security-related behavior of PC users in organizations"*, Information & Management Vol. 21, pp.127-135, 1991.

[3] Giidhue, D. I. & Straub, D. W., *"A Study of Perception of the Adequacy of Security"*, Information & Management Vol. 20, pp.13-27, 1991.

[4] Goh, H. U. and Jeong, Y. B., *"The Effect of ISO 9001:2000 Quality Management System's Requirement on Business Performance"* Journal of Society of Korea and Systems Engineering Vol, 30, No. 3, pp.135-149, September 2007.

[5] Hong, G. H., *"Study of Effect of Information Security Control and Activities to Information Security Performance"*, PhD Dissertation, Kukmin University, pp.68-138 2003

[6] Hype Cycle for Regulations and Related Standards, Gartner, 2008.

[7] ISO/IEC27001: Information technology — Security techniques — Information security management systems — Requirements, 2005.

[8] ISO/IEC27002: Information technology — Security techniques — Code of practice for information security management, 2005.

[9] ITGI *"Information Security Governance : Guidance for Boards of Directors and Executive Management"*, 2002.

[10] KCC, Act for Information and Communication Network Usage Promotion, Information Security, etc., 2009.

[11] Kim, I. H., Gu, T. Y. and Choi, G. S., *"An Empirical Study on the Firm Performance of Quality"*, Management System (ISO9001/00)

[12] Kim, J. D. and Park, J. E., *"Study of Return on Investment of TCO Based Information Security (ROSI)"*, Korea Society of Digital Policy Foundation Conference Proceeding, pp.251~261, 2003.

[13] Kim, Y. J., *"Study of Information Security Process Model Development"*, Joongang University, 2000.

[14] KISA, *"Calculation of National Information Security Level Evaluation Index and Study of Drive for Globalization"*, 2006.

[15] KISA, *"Development of Enterprise Information Security Level Evaluation Methodology"*, 2008

[16] KISA, *"Development of Information Security Level Evaluation Items and Methodology"*, 2002.

[17] KISA, *"Study of Enhancement of Information Security Safety Diagnosis System Operation"*, 2009

[18] KISA, *"Study of Information Security Management System Development to Introduce Information Security Governance Concept"*, 2009.

[19] KISA, *"Study of Information Security Governance Standardization for Information and Communication Enterprises"*, 2008.

[20] KISA, *"2007 Information Security Status Survey – Enterprises"*, 2007

[21] KISA, *"2008 Information Security Status Survey – Enterprises"*, 2008

[22] Nah, J. S. and Jeon, S. H., *"Study of Effect of Information System Auditor's Competency on Auditing Performance"*, Informatization Policy, Vol. 14, No. 2, Summer 2007, pp.3~18.

[23] NIST SP 800-100, *"Information Security Handbook for Managers"*, 2007.

[24] Parker, D. B., *"The Strategic Values of Information Security in Business"*, Computer & Security, Vol. 16, pp.572-582, 1997.

[25] Pironti, J. P., *"Developing Metrics for Effective Information Security Governance"*, ISACA, 2007.

[26] Seon, H. G., *"Effect of Koran Enterprises' Information Security Policy and Organization Factors on Information Security"*, Korea Society of Management Information Systems, Spring Conference Proceeding, pp.1087~1095, 2005.

[27] Sethuraman, S., *"Road Map for Information Security: What to Do After BS 7799 Certification*", ISACA, 2006

[28] Shin, I. S., *"Exploratory Study of Economic Significance of Information Security"*, Information Security Review, Vo. 1, No. 1, pp.27~40, 2005.

[29] Shin, S. H., *"Study of Effect of BSC Operation to Public Agency Performance"*, PhD Dissertation, Dankuk University, pp.65~89, 2007

[30] Sinangin, D, *"Computer Forensics Investigations in a Corporate Environment"*, Computer Fraud & Security, Volume 2002, Issue 6, pp.11-14, 1 June 2002.

[31] Sweren, S. H., "*ISO 17799: Then, Now and in the Future"*, ISACA, 2006

[32] Westby J. and Allen J., *"Governing for Enterprise Security (GES) Implementation Guide"*, CMU/SEI 2007.

[33] 2002 Report of the result of ISMS Pilot Project, JIPDEC 2002.

[34] http://www.iso17799software.com/presentation/index.html
[35] http://www.iso.ch/iso/en/ISOOnline.frontpage
[36] http://www.ukas.org
[37] http://www.truseure.co.kr
[38] http://www.bsi-global.com/Information+Security/04_Standards_infosec/index.xhtml
[39] http://athena.fit.qut.edu.au/security/as4444.htm
[40] http://www.kab.or.kr/index_k.html
[41] http://www.isoeasy.org

Cheol-Soon Park is a director of Korea Communications Commission. He graduated from Seoul National University(SNU) with two bachelor's degrees (History, International Relations) and a master's degree(Public Policy). He is also a doctoral candidate in Technology and Management at SNU. Furthermore, he obtained one more bachelor's degree (Media Arts and Science) and two more master's degrees (Technology Management, European Policy) from other universities. His research interests are information security, technology innovation, and communications policy.

Sang-Soo Jang is a Director at KISA(Korea Internet & Security Agency). He received the B.S. degree in Information and Telecommunication Engineering from Korea Aerospace University in 1989. In 2000, he received the M.S. degree in Information Security from Graduate school of International Affairs & Information the Dongguk University. His areas of interest include Computer & Network, Information System, Information Security Management.

Yong-tae Park is a professor in the Department of Industrial Engineering at Seoul National University (SNU) in Korea. He holds a B.S. in Industrial Engineering from SNU and an M.S. and Ph.D. in Operations Management from the University of Wisconsin-Madison. He won the Technology Innovation Management(TIM) Research Award in 2009. His research interests lie in areas of innovation management, industrial knowledge network, information economics and security, etc.