J Intell Manuf (2012) 23:941–953
DOI 10.1007/s10845-010-0402-7

An analysis on effects of information security investments: a BSC perspective

Hee-Kyung Kong · Tae-Sung Kim · Jungduk Kim

Received: 22 October 2009 / Accepted: 5 April 2010 / Published online: 28 April 2010

Abstract With the growing importance of information security due to the arrival of information society and the spread of the internet, information security is emerging as a tool to guarantee competitive advantage and is at the same time an indispensable requirement for stable business execution for companies and organizations. Additionally, the value of tangible and intangible assets that need to be protected as components of corporate assets are on the rise, where the importance of efficient and effective information asset management and information security investment is increasing for the organizations and companies managing them. However, despite an increase in the information security investment of an organization, there is a lack of systematic methodology pertaining to performance appraisals, which makes decision-making activities and determining means of improvement difficult. The existing financially focused information security investment is inadequate for systematic analyses and understanding due to the opportunity cost type characteristics of information security investment and the difficulty involved in presenting future strategic direction. This paper, considering the characteristics of the effects of information security investment, analyzes from a balanced score card perspective information security investment strategies and performance relationships. In short, critical success factors and key performance indicators are initially obtained from previous research related to information security investment, and the data collected through surveys at related companies and organizations are empirically analyzed utilizing the structural equation model.

Keywords Information security investments · Balanced score card (BSC) · Empirical analysis · Structural equation model (SEM) · Critical success factors (CSF) · Key performance indicators (KPI)

H.-K. Kong
Future Society Research Team, Technology Strategy Research Division, Electronics and Telecommunications Research Institute, 138 Gajeongno, Yuseong-gu, Daejeon 305-700, South Korea
e-mail: konghk@etri.re.kr

T.-S. Kim (✉)
Department of Management Information Systems, Chungbuk National University, 12 Gaeshin-dong, Heungduk-gu, Cheongju, Chungbuk 361-763, South Korea
e-mail: kimts@chungbuk.ac.kr

J. Kim
Department of Information Systems, Chung-Ang University, 72-1 Nae-ri, Daeduk-myon, Ansung, Kyunggi 456-756, South Korea
e-mail: jdkimsac@cau.ac.kr

Introduction

Over the last few decades, information and communication technologies (ICT) have been the leading factors in organizational changes and innovations, and they have been impacting on industrial value chains (Mun et al. 2009). As the value criteria of companies are changing from that of being centered on tangible assets to intangible assets, the value of information that needs to be protected as a corporate asset is rising higher, and the importance of efficient and effective information asset management and information security investment of the organizations and companies managing them is drawing attention. Moreover, in order to cope with diverse risks in a ubiquitous information environment, there is greater demand at present to widen the scope of information security investment and activities. In addition, with the rise in incidents related to information security, local and overseas legal requirements are also increasing, which makes information security management an essential area for corporations. As such, despite the widespread recognition of the importance

of information security, implementations of effective information security systems are often delayed due to a shortage of adequate investment. Furthermore, the lack of a systematic methodology for information security performance quantification makes it difficult for information security investment decision making and improvements in information security to transpire.

The reason for the absence of adequate investment in information security is the lack of objective validity concerning information security as presented to decision makers. Justifying the effect of information security investment when it originates from vague threat tactics is challenging (Kim and Park 2003). This results in recognizing information security investment as a cost of operating organizations. The absence of systematized analytic methods for information security investment makes it difficult to make objective predictions or investment decisions. The performance of information security investment is difficult to assess solely based on financial performance measures such as the prevention of loss from information security incidents, as in the case of performance related to informatization investment. Hence, considering its inherent characteristics, various limitations have arisen when attempting to reflect information security investments in financial terms only. Normally, the information security investment strategy of a company utilizes strategic methodologies such as promotion of their corporate image through the introduction of an information security system and the role of insurance upon the occurrence of security incidents by considering uncertain occurrences. As such, the majority of information security investment strategies are being set up without specific examinations of the causal relationship between justification and strategy. Therefore, this study attempts to analyze the relationship between investment strategies and performance from a BSC perspective considering the characteristics of the information security investment.

First, financially focused business performance goals are set. Next, in order to achieve these goals, goals for increased customer satisfaction are set from a customer perspective. In terms of achieving these, goals for strengthening the internal work process control and asset risk management are then set, being centered on the internal business process. Lastly, the technological and human infrastructure of an information security system is set as the goal as a preceding factor of internal process improvement goals centered on growth and learning. In this manner, the BSC model implemented in a top-down approach assumes that the goal of each perspective is connected by a causal relationship (Kaplan and Norton 1996). For instance, it is assumed that the technological and human infrastructure of an information security system reduces the asset risk of companies and organizations and continuously maintains work while enhancing customer satisfaction by improving internal process perspective goal measurements. The enhanced customer satisfaction is connected to financial goal achievement by either improving or reconsidering the corporate image or by reducing the level of customer dissatisfaction. Nevertheless, an information security investment strategy in which the aforementioned assumption of a causal relationship is not supported empirically could be a highly uncertain challenge for companies and organizations.

In achieving the objective of this study, an enterprise information security investment strategy is set up from a BSC perspective focusing on previous research. By identifying the relationship between information security investment strategy and performance utilizing the structural equation model from this strategy, its validity will be tested. Besides, as a scientific tool for the investment strategy's validity review and a performance measurement of the existing information security investment strategy, BSC shall be offered to companies and organizations that have organized and executed the strategy. Hence, this paper intends to develop a model to analyze the relationship between quantitative and qualitative effects (financial and non-financial indicators) for information security investment.

Theoretical background

Previous research related to information security investment

Investment accompanies predictions of the effect of the investment and its objective assessment. The information security field is not an exception, as analysis of the effect of an investment and its objective assessment is required. As the importance of human behavior in the information security field often exceeds that of any technological aspect through the passage of time, economic approaches such as adequate investment levels for information security, information sharing for information security, and the establishment of incentive systems to solve information security issues are freshly gaining the spotlight. As to the need for socioeconomic study for information security, Soo Hoo (2000) analyzed the need for studying information security issues in the insurance industry and companies, suggesting the need for discussions of an efficient investment size as well as related analyses. Not only social scientists such as Gordon et al. (2002), Gal-Or and Ghose (2004) or Shin (2004) but also those who are considered to be traditional information security technology experts such as Anderson (2001) have emphasized the need for socioeconomic investigations of information security as opposed to studies of flaws in mathematical codes for information security issues; they have suggested the need for discussion pertaining to the efficient investment size and its effect, among other issues. Gordon and Loeb (2002) utilized the net present value (NPV) model to analyze effects of information security investment, and

through game theory, Cavusoglu et al. (2002) determined the optimal investment in security controls. Carnegie Mellon University and the University of Idaho presented a method to produce a return on security investment (ROSI) using diverse variables of information security investment (Kim and Park 2003). However, these studies were limited in terms of actual applications due to the convenience issues pertaining to data collection, quantification of information security usefulness and the absence of concrete calculation methods associated with the cost of information security. To overcome these limitations, Kim and Park (2003) as well as Lee and Lee (2007) presented an improved ROSI method based on the total cost of ownership (TCO). Al-Humaigani and Dunn (2003), Tsiakis and Stephanides (2005), Hausken (2006), and Davis (2005) also defined economic assessments of information security investment with ROSI and other methods; they approached the correlation between the investment cost and effect of information security with mathematical modeling. Blatchford (1995), Lee (2003), and Cavusoglu et al. (2002, 2004a) categorized various factors that need to be considered during information security investment. Bodin et al. (2005) and Scott (1998) also suggested investment criteria for information security and mentioned that as information security investment in general has the characteristic of a long-term guarantee while reducing long-term risk, in many instances it does not provide a quantitative investment effect in the short term. Blakely (2001), Witty et al. (2001), Harris (2001), Roper (1999), and Sun (2005) also categorized the cost factors of information security investment. Hong (2003) quantified the level of information security management and analyzed how efforts towards information security affect organizations. Nam (2006) analyzed the effects of information security investment through how the security incidents of a company affect its stock prices. Gwon and Kim (2007) utilized changes in a company's market value while quantitatively measuring information security investment what is known as the event study methodology, a type of social scientific methodology.

Considerations for analysis on information security investment

Assessing and analyzing an investment should systematically quantify the activities and assets of an organization, enable strategic planning, and multi-dimensionally assess even the long-term and intangible effects of an organization. In particular, the following facts must be considered when analyzing information security investment (Nam 2006). The first of these involves the time constraint characteristic of the measuring of the information security investment effect: information security investment should not be restricted to the preservation of current asset value but should be considered in terms of preserving future value. Second is the intangible aspect of the effect of information security investment: as information security has numerous intangible elements in terms of costs and benefits, they are difficult to identify. Even when they are, transformation into monetary value is difficult. The third fact is the multi-faceted aspect of the effect of information security investment: this implies that information security investment is difficult to measure as it contains both qualitative and quantitative aspects. Fourth is the ambiguity of effect of information security investment: the scope of performance measurement for information security investment is extensive and difficult to assess in connection with goals already set within the organization. Therefore, an analytic system should be developed to test the validity of information security investment through the structure of feedback if possible within the business activities of organizations and companies.

BSC overview and causal relationship with CSF and KPI

BSC is a strategic enterprise management that was created by Kaplan and Norton (1992). It is a core constituent of strategic enterprise management along with Value-Based Management (VBM) and Activity-Based Costing/management (ABC) (Kaplan and Norton 1992). BSC is defined as a technique for strategic performance and valuation that quantifies a company's past performance and assesses present and future corporate value by reflecting together financial and non-financial performance indicators of companies and organizations (Kaplan and Norton 2001). BSC can also be defined as a management tool for strategic execution through financial and non-financial performance quantification, a communication tool within an organization, and a management tool for intangible assets (Kaplan and Norton 1992). The existing financial performance indicator-based performance appraisal is unsuitable for present day companies with a growing proportion of intangible assets, and there are limitations in valuation solely of tangible assets. Intangible assets that are expressed as innovation and change that create sufficient value for the knowledge of the staff, customer relationships and organization are recognized as a core capability that leads the company (Kaplan and Norton 1992).

As a tool that can assess these intangible assets of companies, BSC materializes corporate strategy and vision and shares Key Performance Indicators (KPI) that can measure Critical Success Factors (CSF) to carry out these strategies and visions successfully while maximizing the execution of the strategy (Kaplan and Norton 1996). Heskett et al., in a comprehensive study of profit chains, looked for success factors in service organizations such as Progressive Insurance, Southwest Airlines, MCI and Taco Bell. They argued that tangible performance indicators (e.g., higher return on invested capital) are produced from intangible performance indicators (e.g., staff morale or customer satisfaction) (Kaplan and

Norton 1996). Performance measurement is the selection and use of quantitative and qualitative measures of capacities, processes and outcomes to develop information about critical aspects of activities, including their effect on the achievement of goals. One important purpose of performance measurement is to assess whether progress is being made towards the desired goals and whether activities are performed efficiently. Performance measurement can also serve to identify problems that may require additional efforts or attention. In order to measure performance activities, some quantifiable variables must be defined. These are called *criteria*, sometimes are referred as KPIs, and are defined as standards, rules, or tests on which a judgment or decision can be based on. An indicator is a combination of metrics that provide insights into processes, capacities and outcomes; and metrics are measurement standards that are used to scale and provide meaningful interpretation of quantities measured for each criterion (e.g. an indicator) (Romero et al. 2008).

Research model and setting of hypothesis

Research model design

This study intends to perform simultaneously a literature review focusing on preceding studies along with an empirical study directed at related companies. First, general concepts of analysis of information security investment focusing on a literature review related to specific definitions of investment strategies for information security are considered as the subject of this study. This study has its purpose in presenting methods of setting investment strategies for the information security of companies to cope with changing business environments actively as well as in testing the validity of those strategies. Therefore, investment strategies for information security as the subject of this study include those of companies currently practicing it as the scope of the study.

Through preceding studies of analyses of information security, CSF and KPI as they pertain to information security investment are obtained and taken as the theoretical basis to be considered when setting up investment strategies for information security. When linking the CSF and KPI of information security investment obtained from preceding studies to four perspectives (growth and learning, internal process, customer, and financial), enterprise-wide investment strategies for information security are set up. These strategies are presented as the research model and hypothesis of this study based on a BSC causal link diagram. In an empirical analysis, data are collected through surveys of Korean companies currently investing in information security, and the compatibility assessment and hypothesis of the research model are tested utilizing the structural equation model analytic method with the collected data. For the empirical analysis, a survey prepared with a five-point Likert scale is used so that the characteristics of each variable are reflected. Amos 7.0 is used to analyze the research model. Based on the results of this empirical analysis, BSC is utilized to present the setting of investment strategies for information security and investment strategy policy by stages.

In this study, CSF signifies the 'investment strategies for the information security of a company' that enable the company to achieve its intended goals through information security investment. Additionally, KPI refers to a company's 'detailed investment strategies for information security' in a manner more specific than CSF, where KPIs that need to be managed for the company to increase their current business performance and future value have been made objective through quantitative figures. This study obtained and formed performance indicators from BSC perspectives through a literature review. The four most widely used perspectives in BSC studies were applied to each indicator; while CSF and KPI were structured focusing on literature related to BSC, analyses of information security investment and performance appraisal related literature were also done.

Growth and learning perspective measures how well companies and organizations can prepare against changes in information security technology. These measures serve as the performance motive of the other three perspectives. The importance of fostering human resources with information security knowledge and technology is stressed in the majority of studies; going a step further, the importance of an incentive system is mentioned more than the technological issues of information security. Therefore, through the information security policy set up, technology introduction, security certification and related infrastructure or information security training, emphasis is placed on the user's capability or corporate and organizational culture that attempts to apply basic technology or new technology.

The internal process perspective deals with the efficiency and efficacy of providing information system products and services through information security investment. Here, in terms of strengthening internal process control, efficiency aspects such as the strengthening of the internal process control of general staff and information security staff are addressed. In addition, cost reduction aspects of information assets such as reductions of defect time due to incidents and problems with information systems, reductions of security incidents, reductions in work deficiency, or reductions in information system vulnerability reduced through information asset security, as well as asset risk management aspects such as information asset security and information system quality maintenance are dealt with. That is, the internal process perspective measures the process efficiency of the information system, information asset management and security. Through information security investment, information systems and information assets should be

protected as much as possible and made to work continuously. To do this, the internal process should be optimally managed and operation performances continuously assessed while enhancing efficiency. Therefore, performance indicators related to these issues should not only be measured and managed regularly but also should be compared with industry standards and averaged when assessing productivity.

Customer perspective is the user perspective of those using the provided information security system. It includes the internal/external users of the company as customers. Its indicator uses the level of user satisfaction and attempts to measure the increased use of information systems or reductions of the number of customer complaints through information security investment, for example, with customer satisfaction indicators. Customer perspective indicators include a reduction of customer complaints, market share, winning new customers and maintaining existing customers, corporate image improvement, and increased use of information systems.

Financial perspective is the appraisal of the monetary value of information security investment that mostly cites indicators from existing economic analyses of information security investment. Their corresponding indicators are reductions of direct loss, reductions in compensation for information security incidents, reductions in information security maintenance costs, stock quotes and financial values. While economic approaches of information security are based on quantified data, there are many real-life issues for security incidents related to information security and defect-related information to be measured and managed enterprise-wide. Information security issues include security incidents and defects that are not reported nor managed normally, as security incidents negatively affect the stock price and image of the company and can be used detrimentally by competitors. Nevertheless, within the company, enterprise-wide information security incidents and defects need to be reported systematically and managed in an economic approach of information security investment. According to Nam (2006) and Gwon and Kim (2007) information security incident's influence on the stock price is appraised by being categorized into security incidents and defects, and their results compared. Moreover, the effect of information security investment, rather than itself being a direct performance measure of company business as an information system, plays the indirect role of assisting the attainment of the organization's goal, thus including non-quantitative indicators considered as organizational unit effects such as a supporting system for strategies of companies and organizations as well as structural changes in companies and organizations. Therefore, this study includes stock quotes and financial values as performance indicators from the financial perspective.

The CSF of each perspective and the KPI within it presented in Table 1 are recognized in terms of their validity through a Delphi method directed at expert groups currently in charge of information security related practices. The Delphi method was carried out from 23 January to 15 February 2008 with the participation of an expert group that included senior persons in charge and practicing staff with decision-making authority at companies investing in information security as well as researchers at laboratories and academics in the information security management sector.

Hypotheses

As shown in Fig. 1, these hypotheses assume a causal link between the CSFs of each perspective. Based on this, they are structured as a direct/indirect effect of each stage, as shown below. In the hypothesis of each stage, detailed sub-hypotheses are again set up.

Hypothesis 1 Success factors of growth and learning perspective shall positively affect those of the internal process perspective.

H1a: The building of the technological/human infrastructure of the information security system shall positively affect the strengthening of internal process controls.

H1b: The building of the technological/human infrastructure of the information security system shall positively affect asset risk management.

Hypothesis 2 Success factors of growth and learning perspectives shall positively affect those of the customer perspective.

H2a: The building of the technological/human infrastructure of the information security system shall positively affect customer satisfaction.

Hypothesis 3 Success factors of the growth and learning perspective shall positively affect those of the financial perspective.

H3a: The building of the technological/human infrastructure of the information security system shall positively affect business performance.

Through the building of the technological/human infrastructure, the success factors of the growth and learning perspective become the motive in enhancing the internal process improvement. In this study, internal process improvement is classified into the strengthening of internal process control and asset risk management in terms of information security investment. Theoretically, the success factors of the growth and learning perspective can be expected to affect the internal process perspective positively. The growth and learning perspective forms the basis of growth and learning through continuous information security training and investment and corresponds to the primary performance motive in attaining the mission of information security. This performance motive directly affects the improvement of internal improvement,

Table 1 CSF and KPI of BSC perspective for the information investment strategy

Perspectives	CSF (constructs)	KPI (variables)	Supporting literature
Growth and learning	Information security's technological/human infrastructure	Information security policy setting and review Information security technology introduction Security certification acquisition Infrastructure-building related information security technology Core professionals for information security Training of human resources with information security knowledge and technology	Blatchford (1995), Lee (2003), Hong (2003), Kim and Lee (2005), Sun (2005), Nam (2006)
Internal process	Strengthening of internal process control	Strengthening of the internal process control of the general staff Strengthening of the internal process control of the information security staff	Blatchford (1995), Scott (1998, 2002), Harris (2001), Hong (2003), Cavusoglu et al. (2004a,b), Sun (2005)
	Asset risk management	Reduction of information asset management costs Reduction of defect time and work deficiency due to security incidents Reduction of hacking Reduction in information system vulnerability	Blatchford (1995), NIST (1996), Scott (1998, 2002), Harris (2001), Cavusoglu et al. (2004a,b), Hong (2003), Tanaka et al. (2005), Sun (2005)
Customer	Customer satisfaction	Reduction of customer complaints Market share Winning new customers Maintaining existing customers Corporate image improvement degree Increased use through information system	Scott (1998, 2002), Hong (2003), Cavusoglu et al. (2004a,b), Nam (2006), Kim and Lee (2005), Sun (2005), Gwon and Kim (2007)
Financial	Business performance	Reduction of direct loss due to information security incidents Reduction of compensation for information security incidents Reduction in information security maintenance costs Stock quotes and financial values	Blatchford (1995), NIST (1996), Kim and Park (2003), Blakely (2001), Gordon and Loeb (2002), Al-Humaigani and Dunn (2003), Campbell et al. (2003), Cavusoglu et al. (2004a,b), Kumar (2004), Davis (2005), Tsiakis and Stephanides (2005), Kim and Lee (2005), Bodin et al. (2005), Nam (2006), Gwon and Kim (2007), Lee and Lee (2007)

and this type of influence can be expected to directly/indirectly affect the customer and financial perspectives. Therefore, information security related workforce management and training, management of expert knowledge, and related factors will serve as the basic infrastructure and capability in efficiently managing actual work.

Hypothesis 4 Success factors of the internal process perspective shall positively affect those of the customer perspective.

H4a: Strengthening of the internal process control through information security investment shall positively affect customer satisfaction.

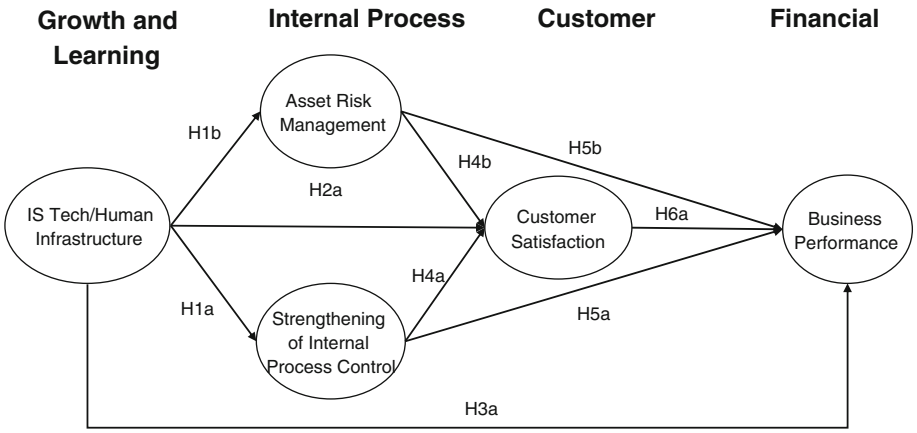

Fig. 1 The research model

H4b: Asset risk management through information security investment shall positively affect customer satisfaction.

Hypothesis 5 Success factors of the internal process perspective shall positively affect those of the financial perspective.

H5a: Strengthening of the internal process control through information security investment shall positively affect business performance.

H5b: Asset risk management through information security investment shall positively affect business performance.

The internal process perspective affects the performance of the customer perspective, and the degree of improvement in the internal process is measured by the strengthening of the internal process control and asset risk management levels. The success factors of the internal process perspective presented in this study are classified into the strengthening of the internal process control through information security investment and the risk management of information assets. These success factors of the internal process perspective serve the purpose of protecting work continuity from the risk management of the existing information system and information assets as well as related defects through information security investment. This success factor affects the customer perspective directly and affects the financial perspective indirectly through the customer perspective. Furthermore, it may directly affect the financial perspective through a perspective other than the customer perspective. This implies that internal process improvement can be defined as a performance motive that can affect increases in both customer satisfaction and business performance.

Hypothesis 6 Success factors from a customer perspective shall positively affect those of a financial perspective.

H6a: Increased customer satisfaction through information security investment shall positively affect business performance.

Empirical analysis and testing and results

Data collection

The survey for the empirical analysis selected the following related companies which were seen as considering information security important in business environment as the assumed sample: financial industry including banks and securities, home shopping companies, internet portals and system integration firms, internet service providers, online game companies, e-learning companies, medical service firms, national and public research institutes and public institutions. The survey was carried out at these companies and organizations because the goal of the study lies in testing the validity of strategies through clarification of the causal links between the BSC perspective investment strategy and performance considering the characteristics of information security investment. Hence, it was directed at companies already investing in information security and performing appraisals of the performance of this investment.

The sample selected to obtain the responses containing expertise and accuracy related to the performance of information security investment is described below. First, as organizations objectively thought to be already investing in existing information security, companies possessing and running provisional organizations concerning information security incidents, companies having been awarded the information security grand prize hosted by the Ministry of Information and Communication since 2002, companies having acquired information security related certifications of ISO 27001 and ISMS, and member firms of information security practice conference were included. In addition, to conform to the study's objective of performance research in the area of information security investment, it was directed at the staff and executives of information security departments who may participate in the decision-making process as it is related to information security investment, and who analyze

and assess that performance, rather than those in charge of information security technical support or technology-related areas. The survey's methodology utilized personal interviews, e-mail, posts, web surveys and similar mediums. Based on the list of companies and organizations undergoing measurements and appraisals related to the performance of their information security investments, 600 companies and organizations were selected. After a validity review and pilot test with the first stage of the survey from 23 January to 15 February 2008, 7 learning and growth perspective items, 10 internal process perspective items, 6 customer perspective items, 4 financial perspective items, and 8 items were selected for an analysis of the responding companies and respondents for the second stage main survey, which continued for 5 weeks, from 18 February to 24 March 2008. Excluding personal interviews, all other surveys went through the process of explaining the aim of the survey and requesting cooperation through direct phone calls with corresponding companies in an effort to raise the recovery rate and quality of responses. As a result, a total of 133 of 600 distributed surveys were recovered for a recovery rate of approximately 22.1%.

Reliability and validity

Structural equation modeling was conducted using AMOS to test the causal model (Kline 2000). This study, for a confirmatory test of the theoretical measurement model, performed a confirmatory factor analysis directed at all variables including critical success factors and performance indicators of each perspective. Confirmatory factor analysis is a technique that tests hypothesized factor structures through actual data after setting the relationships between the variables under a theoretical background (Kline 2000).

Considering the results of the confirmatory factor analysis of the entire measurement model, it can be said that the standard load volume between the measured items and each constituent concept are all statistically significant (t value > 2), as shown in Table 2. Hence, they show the convergent validity of the measured items (Bagozzi and Yi 1991).

In this study, the confidence level was analyzed through the internal consistency confidence measurement of Cronbach's α analysis. According to Chaiy (1995), the most widely used factor in the testing of the confidence level of a survey is Cronbach's α value, a calculated factor of an internal consistency method, where as a method of raising the confidence level of a measurement tool by determining various items with which to measure the same concept, it was found to be capable of improving the confidence level by excluding items of decreasing confidence among several items (Bae 2007). In the course of this determination of items hampering the confidence level, each measurement variable item of F3 (Y10), F4 (Y15) and F5 (Y20) were removed. Considering the characteristics of this study, confidence analysis was performed with the criteria of the Cronbach's α value of 0.8. Regarding the measured results of Cronbach's α for each factor extracted from a factor analysis, all factors were found to be within the 0.863–0.911 range. As a result, each item of this study can also be said to have the confidence level of each factor tested.

As shown above, all factor accumulations have statistically significant p values through a confirmatory factor analysis. Therefore, the convergence validity and single dimensionality between of each constituent concept are obtained (Anderson and Gerbing 1988), and the confidence level of each constituent concept that measures the internal consistency of the item as surpassing 0.8, an acceptable level in all factors, is considered to satisfy the confidence level (Devaraj et al. 2002). Additionally, regarding the average variance as another measurement of confidence level, this should exceed 0.5, the size of the variance where the item can describe the theoretical variable, to satisfy the confidence level (Bagozzi 1988). In this study, the average variance values of all factors surpassed the acceptable level, thus satisfying the confidence level.

According to Fornell and Larcker (1981), if the square root of each factor's average variance extracted (AVE) is larger than the correlation coefficient between the corresponding factor and other factors, discriminant validity of the corresponding model is regarded to exist.

Therefore, to increase the discrimination between constituent concepts, F1 (X4) and F1 (X5), which were shown to have a high level of correlation between constituent concepts, were removed. As a result of observing the correlation between the five theoretical variables included in the research model to test the discriminant validity between the constituent concepts, 1.0 was not included in the 95% confidence level of the correlation coefficient Anderson and Gerbing (1988), as shown in Table 3. More strictly, the AVE surpasses the square value (Φ^2) of the correlation coefficients between the concepts; thus, it can be said that discriminant validity of constituent concepts does exist (Fornell and Larcker, 1981).

Model fitness

The model is fit when the χ^2 value is smaller, and the p value for χ^2 should be identical to or larger than 0.05 and the Q value (χ^2/df) should be smaller or identical to 2 to be fit as well. Additionally, the optimal structuring of items per factor were assessed through fitness indicators that included the root mean-square residual (RMR $\leq$ 0.05), the root mean-square error of approximation (RMSEA $<$ 0.05 $\sim$ 0.08), the normed fit index (NFI $\geq$ 0.9), the comparative fit index (CFI $\geq$ 0.9), the Turker–Lewis index (TLI $\geq$ 0.9), the goodness-of-fit index (GFI $\geq$ 0.9), and the adjusted goodness-of-fit index (AGFI $\geq$ 0.9).

Table 2 Results of confirmatory factor analysis

Constructs	Variables	Factor loading	t value (C.R.)	S.E.	C.R.	AVE	Cronbach's α
F1	X1	0.863	–	0.34	0.902	0.652	0.897
	X2	0.858	12.981	0.32			
	X3	0.786	10.717	0.425			
	X6	0.617	7.653	0.128			
	X7	0.802	11.057	0.456			
F2	Y1	0.899	–	0.186	0.896	0.811	0.889
	Y2	0.89	13.035	0.186			
F3	Y3	0.756	–	0.199	0.940	0.695	0.865
	Y4	0.715	8.043	0.166			
	Y5	0.756	8.387	0.147			
	Y6	0.76	8.603	0.133			
	Y7	0.794	9.05	0.181			
	Y8	0.519	5.708	0.456			
	Y9	0.603	6.652	0.255			
F4	Y11	0.632	–	0.495	0.934	0.741	0.911
	Y12	0.885	8.286	0.148			
	Y13	0.917	8.42	0.112			
	Y14	0.821	7.829	0.29			
	Y16	0.883	8.29	0.169			
F5	Y17	0.913	–	0.177	0.865	0.685	0.863
	Y18	0.927	16.387	0.146			
	Y19	0.664	8.859	0.657			

Table 3 Correlation coefficients matrix between constructs

	SQRT (AVE)	Information security's technological/human infrastructure	Strengthening of internal process control	Asset risk management	Customer satisfaction	Business performance
Information security's technological/human infrastructure	0.807	1				
Strengthening of internal process control	0.901	0.760	1			
Asset risk management	0.901	0.216	0.174	1		
Customer satisfaction	0.861	0.472	0.591	0.123	1	
Business performance	0.828	0.688	0.743	0.222	0.651	1

All correlation coefficients are significant at 0.01 level (both sides)

Hair et al. (2006) suggested that fitness can be considered with RMSEA and RMR values below 0.08 when the sample size is below 250, the number of observed variables is between 12 and 30, and the CFI is >0.95 (Bae 2007). Additionally, Yu et al. (2005) assessed the fitness of the model considering recommended criteria such as the goodness-of-fit index (GFI $\geq$ 0.8) and the adjusted goodness-of-fit index (AGFI $\geq$ 0.8). As a result of checking the fitness of the entire confirmed model through these procedures, $\chi^2 = 298$, $df = 199$, $p = 0.00$, $Q\ (\chi^2/df) = 1.499$, RMR = 0.049, RMSEA = 0.061, NFI = 0.86, CFI = 0.94, TLI = 0.94, GFI = 0.82, and AGFI = 0.78 were determined, thus showing overall positive fitness.

In this study, the model's fitness and related parameters were estimated via structural equation model analysis. When measuring the fitness indicators of the optimal research model analyzed in this study, they were found to be $\chi^2 = 216$, $df = 192$, $p = 0.112$, $Q\ (\chi^2/df) = 1.125$, RMR = 0.44, RMSEA = 0.030, NFI = 0.90, CFI = 0.98, TLI = 0.98, GFI = 0.87, and AGFI = 0.83, which are acceptable as overall fitness assessment indicators. Therefore, the suggested model appears to be fit and does not appear to pose a prob-

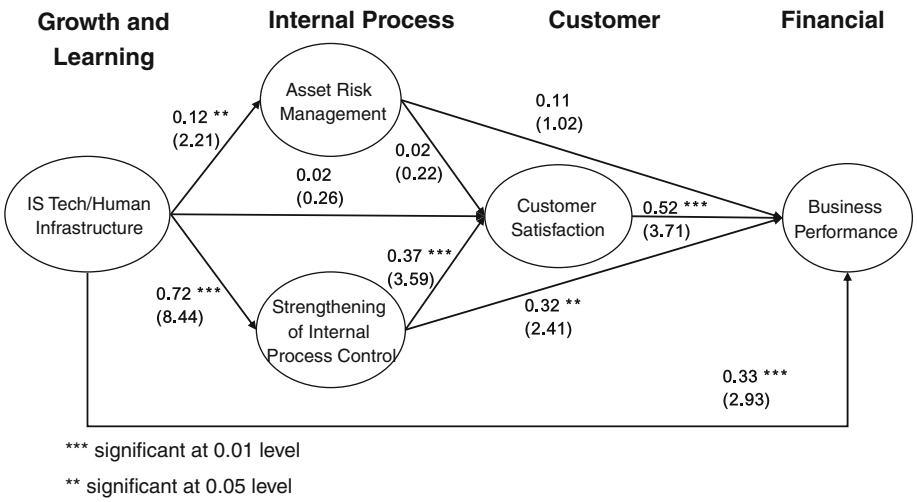

Fig. 2 Results of analysis on the research model

lem when estimating the relationship between these study variables. Figure 2 shows the path diagram shown as a result of the analysis using the AMOS values of the research model.

Hypothesis testing

The path model results are shown in Table 4. In the cases of hypotheses 1a and 1b, the building of a technological/human infrastructure for information security in growth and learning perspective is shown to affect asset risk management of internal process perspective and strengthening of internal process control significantly. For hypothesis 1, the building of a technological/human infrastructure from a growth and learning perspective is shown to affect the strengthening of internal process control as a success factor for internal process improvement more compared to asset risk management from an internal process perspective. Additionally, the building of a technological/human infrastructure did not significantly affect customer satisfaction directly, thus rejecting hypothesis 2a. In various earlier studies such as Lee (2003), information security investment was defined as to protect the availability, immaculateness, and confidentiality of information assets such as technology, human resources, education, policy and consulting, and was argued to lead to improvements at the corporate information security level. Their results are in good agreement with those of this study, and this is considered to be an area requiring further study of the effect of future performance appraisals on information security investment.

Asset risk management from an internal process perspective also did not significantly affect customer satisfaction directly, thus rejecting hypothesis 4b. Moreover, asset risk management did not significantly affect the business performance of the financial perspective directly. However, strengthening of the internal process control of the internal process perspective did significantly affect customer satisfaction from a customer perspective and business performance from financial perspective, both directly and indirectly, thus affirming hypotheses 4 and 5a. Cavusoglu et al. (2004a,b) argued that the corporate confidence level, among other factors, should be considered during information security investment. They mentioned management's importance in economic terms. This can be considered as coinciding with the present study. For hypotheses 4 and 5, only success factors for the strengthening of internal process control were shown to affect both customer and financial perspectives among internal process perspectives. This attests to the fact that among the success factors from an internal process perspective, the factor for the strengthening of internal process control is a greater performance motive compared to the asset risk management factor. Thirdly, the customer satisfaction from a customer perspective significantly affected business performance from a financial perspective. For hypothesis 6, increased customer satisfaction such as corporate image improvement through information security investment can be seen to affect business performance positively. This may imply that recently companies have recognized that they should improve the level of information security in order to increase business performance. It can be considered that improvements in customer relationships and the corporate image gradually affect business performance. Lastly, the building of a technological/human infrastructure from a growth and learning perspective significantly affected business performance from a financial perspective directly, thus affirming hypothesis 3a. Recently, a majority of local and foreign companies are moving towards raising the level of their information security through the introduction of new technologies and training. This testifies to the fact that the building of a technological/human infrastructure for information security is becoming a crucial factor in the performance management of information security for companies and orga-

Table 4 Path model results

	Path	Estimate	*t* Values	Assessment ($p \leq 0.05$)
H1a	Information security's tech/human infrastructure → Strengthening of internal process control	0.72	8.44***	Supported
H1b	Information security's tech/human infrastructure → Asset risk management	0.12	2.21**	Supported
H2a	Information security's tech/human infrastructure → Customer satisfaction	0.02	0.26*	Not supported
H3a	Information security's tech/human infrastructure → Business performance	0.33	2.93***	Supported
H4a	Strengthening of internal process control → Customer satisfaction	0.37	3.59***	Supported
H4b	Asset risk management → Customer satisfaction	0.02	0.22*	Not supported
H5a	Strengthening of internal process control → Business performance	0.32	2.41**	Supported
H5b	Asset risk management → Business performance	0.11	1.02*	Not supported
H6a	Customer satisfaction → Business performance	0.512	3.71***	Supported

* Significat at 0.1 level
** Significant at 0.05 level
*** Significant 0.01 level

nizations. Furthermore, a study by Scott (1998) mentioned that as information security investment in general is a type of long-term guarantee, it is difficult to suggest a quantitative investment effect in the short term. Moreover, if a shortage of information security control exists, the likely loss factors are reduced productivity, diminishing profits, falling corporate image, and financial loss (Scott 2002). It was mentioned that information security investment directly leads to business performance and at the same time raises the level of the company's enterprise-wide information security improvement, through which in the long term results in an improvement of the company's internal efficiency and increased external customer satisfaction as its performance. These results can be analyzed to coincide with results of the present study.

Discussion and conclusion

Summary and implication of the study

This study sought to present BSC as an analytic tool for enterprise-wide strategies of information security in response to the changing corporate business environment. The BSC perspective of investment strategies of information security were set up considering the characteristics of information security investment, and the validity of the BSC perspective investment strategies for information security were tested by finding a causal link between the investment strategies and performance as these factors relate to information security while utilizing the structural equation model. To this end, the causal link of the BSC perspective was initially formulated into a model, and the relationships between each perspective were assumed in several types of hypotheses. The caual links were subsequently analyzed empirically using the Path Model of Amos. The established investment strategies for information security were obtained with a strategic diagram of BSC causal links that was set as the research model. With 5 CSF factors as theoretical variables and 27 KPI factors as measurement variables, the relationships between the variables were then analyzed. In addition, 9 research hypotheses were presented centering on the path of the BSC research model.

The significance of the findings is shown below. This study can be practically applied in relation to investment strategies for information security, and BSC can be presented as an analytic tool and framework when setting up and execution investment strategies for information security. To this end, the validity of BSC perspective investment strategies for information security, specifically the causal links and influence on the investment performance of information security, were tested through an empirical analysis. Based on results obtained here, the following points are the implications of this study. First, the BSC perspective investment strategies for information security have causal links between them and positively affect the improvement of a company's investment performance due to the level of information security. Second, companies having already set up and executed investment strategies for information security may consider BSC utili-

zation as a tool for a validity assessment of existing strategies and as a performance measurement of their information security system.

In conclusion, in summarizing the present study results, in an effort to raise the level of information security of companies and organizations, the asset risk management and work process control above all should be strengthened through the building of a technological/human infrastructure from a learning and growth perspective. The success of this type of internal process improvement affects the next step of customer satisfaction from a customer perspective. Moreover, once customer satisfaction increases along with the building of a technological/human infrastructure, it can be concluded that business performance from a financial perspective will be enhanced.

Limitations and future research suggestion

This study, despite its intentions, can be said to be of an investigative nature for future serious empirical analysis. Investment strategies for information security were set up based on preceding studies, and the validity of investment strategies were measured directed at subjects with somewhat limited understanding on investment strategies for information security. Although the results of this study are a product of a survey directed at companies who either already have invested or is in the process of investing in information security, companies in actual practice, rather than accurately identifying or analyzing the investment performance for information security, are more interested in temporary improvement of information security level such as external and internal corporate image or review of certifications. Also, as the strategies were set up based on preceding studies when setting up BSC perspective studies, it's possible that realistic strategies were not adequately presented, and as the survey questionnaire were structured so that measured variables are obtained and factors are measured relying on preceding studies, companies selected specimen may not have received adequately realistic questionnaires.

In future studies, more realistic and detailed strategies should be presented through interview and case studies with persons in charge of performance appraisal for information security, investment strategy experts. In selecting indicators, a more realistic tools should be developed that can analyze realistic corporate activities, and through this investment performance of information security should be more precisely measured, and based on this studies on diverse causal links would be possible. In addition, the model can be extended to include more detailed investment items in the perspective of BSC. Furthermore, variables' measurement target should be narrowed into more specific and professional groups such as Chief Security Officers (CSOs) and security consultants. Also, as the issue of information security is largely affected by cyber environment, future studies should consider environment factors of information security investment such as social and governmental regulations, legal actions, IT governance and IT compliance aspects as well.

References

Al-Humaigani, M., & Dunn, D. B. (2003). A model of return on investment for information systems security. *Circuits and Systems, 1*, 483–485.

Anderson, R. (2001). Why information security is hard-an economic perspective. *Computer Security Application Conference* (pp. 358-365).

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: a review and recommended two-step approach. *Psychological Bulletin, 103*, 411–423.

Bae, B. R. (2007). *Principles and practice of structural equation modeling using Amos 7*. South Korea: Cheongram (in Korean).

Bagozzi, R. P., & Yi, Y. (1991). Multitrait-multimethod matrices in consumer research. *Journal of Consumer Research, 17*(4), 426–439.

Bagozzi, R. P. (1988). Performance and satisfaction in and industrial sales force: An examination of their antecedents and simultaneity. *Journal of Marketing, 44*, 65–77.

Blakely, B. (2001). Returns on security investment: An imprecise but necessary calculation. *Secure Business Quarterly, 1*(2), 27.

Blatchford, C. (1995). Information Security Controls Are They Cost-effective. *Computer Audit Journal, 3*, 11–19.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM, 48*, 79–83.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448.

Cavusoglu, H., Mishra, B. K., & Raghunathan, S. (2002). Optimal design of IT security architecture. *Working Paper*. TX: University of Texas at Dallas.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004a). Economics of IT security management: Four improvements to current security practices. *Communications of the Association for Information System, 14*, 65–75.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004b). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87–92.

Chaiy, S. I. (1995). *Social Science Research Methodology*. South Korea: Hakhyunsa (in Korean).

Davis, A. (2005). Return on security investment—proving it's worth it. *Network Security, 2*, 8–10.

Devaraj, S., Fan, M., & Kohli, R. (2002). Antecedent of B2C channel satisfaction and preference: Validating e-Commerce metrics. *Information Systems Research, 13*(3), 316–333.

Fornell, C., & Larcker, D. (1981). Evaluating structural equations models with unobservable variables and measurement error. *Journal of Marketing Research, 18*, 39–50.

Gal-Or, E., & Ghose, A. (2004). The economic incentives for sharing security information. *Working Paper*. Pittsburgh: University of Pittsburgh and Carnegie Mellon University.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457.

Gordon L. A., Loeb, M. P., & Lucyshyn, W. (2002). An economics perspective on the sharing of information related to security breaches. In *Proceedings of Workshop on the Economics of Information Security*.

Gwon, Y. O., & Kim, B. D. (2007). The effect of information security breach and security investment announcement on the market value of Korean firms. *Information Systems Review, 9*(1), 105–120. (in Korean).

Hair, J. F., Jr., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data Analysis 6th ed*. NJ: Prentice-Hall International.

Harris, S. (2001). *CISSP All-in-One Exam Guide*. New York: McGraw-Hill.

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information System Frontiers, 8*(5), 338–349.

Hong, K. H. (2003). *A study on the effect of information security controls and processes on the performance on the performance of information security*. South Korea: Kook-Min University. (in Korean).

Kaplan, R. S., & Norton, D. P. (1996). *The balanced scorecard—translating strategy into action*. Boston: Harvard Business School Press.

Kaplan, R. S., & Norton, D. P. (1992). The balanced scorecard—measures that drive. *Harvard Business Review*, Jan/Fab (pp. 71–79).

Kaplan, R. S., & Norton, D. P. (2001). *The Strategy-focused organization*. Boston: Harvard Business School Press.

Kim, S. K., & Lee, H. J. (2005). Cost-benefit analysis of security investments: methodology and case study. *International Conference on Computational Science and Its Applications, 3482*, 1239–1248.

Kim, J. D., & Park, J. E. (2003) A study on TCO-based return on security investment (ROSI). In *Proceedings of the Korea Digital Policy Conference* (Vol. 1, pp. 251–261) (in Korean).

Kline, R. B. (2000). *Principles and practice of structural equation modeling*. New Jersey: The Guilford Press.

Kumar, K. L. (2004). A framework for assessing the business value of information technology infrastructures. *Journal of Management Information Systems, 21*(2), 11–32.

Lee, V. C. S. (2003). A fuzzy multi-criteria decision model for information system security investment. *Lecture Notes in Computer Science, 2690*, 436–441.

Lee, J. S. & Lee, H. J. (2007). Evaluating information security investment using TCO-based Security ROI. In: *Proceedings of the Korea Information Processing Society Conference* (pp. 1125–1128) (in Korean).

Mun, J. T., Shin, M. S., & Jung, M. Y. (2009). A goal-oriented trust model for virtual organization creation. *Journal of Intelligent Manufacturing*. http://www.springerlink.com/content/03685347x1837440/.

Nam, S. H. (2006). *An empirical study on the impact of security events to the stock price in the analysis method of enterprise security investment effect*. South Korea: Korea University. (in Korean).

NIST (1996) An introduction to computer security. *NIST Special Publication 800-12*.

Romero, D., Galeano, N., & Molina1, A. (2008). Virtual organisation breeding environments value system and its elements. *Journal of Intelligent Manufacturing*. http://www.springerlink.com/content/x2374786057w57j3/.

Roper, C. A. (1999). *Risk management for security professionals*. London: Butterworth-Heinemann.

Scott, D. (1998). *Security Investment Justification and Success Factors*. Stamford: Gartner.

Scott, D. (2002). Best practices and trends in business continuity Planning, U.S. Symposium/ITxpo.

Shin, I. S. (2004). Review the economics means to information security. *Information Security Review, 1*(1), 27–40. (in Korean).

Soo Hoo, K. J. (2000). *How much is enough? A risk-management approach to computer security*. Palo Alto, CA: Stanford University.

Sun, H. G. (2005). A Study on the effect of information security policy and organization on the performance of information security. In *Proceedings of the Korea management information system international conference*, (pp. 1087–1095) (in Korean).

Tanaka, H., Matuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of E-local government in Japan. *Journal of Accounting and Public Policy, 24*, 37–59.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers and Security, 24*(2), 105–108.

Witty, R. J., Girard, J., Graff, J. W., Hallawell, A., Hildreth, B., MacDonald, N., Malik, W. J., Pescatore, J., Reynolds, M., Russell, K., Wheatman, V., Dubiel, J. P., & Weintraub, A. (2001). *The price of information security*. Stamford: Gartner.

Yu, J. E., Ha Choi, M. K., & Rho, J. J. (2005). Extending the TAM for a t-commerce. *Information and Management, 42*, 965–976.