The Effects of Managing Confidential Information on IT Security Investment Decision: An Empirical Analysis

Woohyun Shim

Michigan State University, shimwoo@msu.edu

ABSTRACT

Stronger reliance on information technologies is increasing firms' vulnerability to information security breaches. The design of optimal information security investment strategies is complicated by the limited understanding of different security vulnerabilities. This paper provides a conceptual and empirical analysis of the characteristics of information security investment in the presence of different vulnerability levels. By distinguishing confidential and non-confidential information, the paper discusses how information security investment might be affected by different information types as vulnerability increases. The empirical research uses data from 4,378 organizations that participated in surveys conducted by the Korean Internet & Security Agency in 2007 and 2008. Our findings confirm that the decisions of organizations concerning information security investment depend not only on security vulnerability but also on the type of information to be protected: firms managing highly confidential information increase their level of security investments as vulnerability increases, whereas firms with less confidential information at first increase, but then subsequently decrease the investment as vulnerability rises.

Keywords: H.4.2 [Information Systems Applications]: Types of Systems—decision support
Index Terms: information security strategies, security investment, confidential information

1. Introduction

Increased connectivity utilizing Internet-based technologies has changed the way organizations communicate, as well as the way they protect their information. The protection of information systems has become as critical as the protection of other assets [1]. Firms have increased their expenditure on information security and have adopted a range of solutions to protect information systems [2]. Although the technical security solutions have been employed and have continuously improved, various types of security breaches have also continued to increase [3]. The 2008 CSI Computer Crime and Security Survey [4] found for example that most of the responding organizations either had a security policy (68 percent) or were developing a formal information security policy (18 percent); 31 percent of the organizations spent more than 5 percent of their overall information technology (IT) budget on information security. Nonetheless, the survey indicated that 43 percent of respondents had experienced security breaches and 27 percent of those suffered more than 5 incidents [4]. Moreover, the survey reported that the average loss suffered by organizations from security incidents was around $300,000 per organization [4]. Thus, even though organizations have committed considerable funds to IT security investments, the investments do not seem to be effective in preventing many information security breaches [1]. This inadequacy of the investments renders organizations exposed to cyber threats.

The primary intention of this study is to shed light on the relationship between an organization's security vulnerability and its IT security investment. The paper builds on and expands the analyses presented in [1] and [5]. Gordon & Loeb in reference [1] demonstrated that optimal information security investment is affected by information security vulnerability and the associated loss from such vulnerability. The authors proposed two broad types of security breach probability functions, referred to as 'Class I' and 'Class II'. Class I can be represented by breach probability functions that are linear in vulnerability. The expected loss due to security breaches is also linear in vulnerability. For the functions belonging to this class, the expected benefit of information security (EBIS) (i.e., the decrease in the firm's expected loss resulting from the increased security investment) increases as vulnerability rises. Firms with security probability functions belonging to Class I can, therefore, be better off increasing the amount of security investments as the vulnerability of information sets rises. Class II security breach probability functions are convex in vulnerability; that is, EBIS first increases and then decreases as vulnerability rises. A salient feature of the functions in this class is that protecting information sets becomes exceedingly expensive as vulnerability becomes very high. Reference [1] concluded that, for a firm with Class II security breach probability functions when a security environment is very vulnerable, its security investment may not be justified if the benefit of increased security investment (i.e., the reduction in expected loss from the increased security) is very small: the firm may not better off investing its resources on highly vulnerable information sets.

Campbell et al. in reference [5], adopting a different vantage point, argued that security breaches of confidential information, such as user's account information or credit card data, generate a highly significant negative impact on the value of affected firms, whereas security breaches which are not related to confidentiality do not result in the reduction of the value of affected firms. The authors concluded that the leakage of non-confidential information which generates only a small expected loss can be viewed as an acceptable operation cost. In contrast, confidential information leakage should be avoided in order to prevent a high increase in expected loss, which results in a highly negative impact on stock market valuations.

Building on the implications from both [1] and [5], this study conceptually and empirically explores the relationship between security vulnerability level and information security investment in cases where firms manage different types of information (i.e., confidential vs. non-confidential information). Specifically, this study partitions the sample based on whether or not a firm

collects confidential information from its customers. It is hypothesized that firms collecting customer information fall into Class I whereas firms not collecting the information belong to Class II. The study then tests the relationship between vulnerability and information security investment for the partitioned data.

To test the theoretical conclusions, data extracted from the 2007 and 2008 Korean Information Security Surveys conducted by the Korean Information Security Agency (KISA) is used. Korean data is used for two reasons: first, Korea is a country with a world-class information communication technology (ICT) infrastructure.[1] The country also boasts a large and fast growing information security market.[2] Second, the data is a rare sample of all the business in a country. Approached with caution, the results here may suggest, more broadly, findings that can be generalized to other countries.

The results of the data analysis corroborate the conceptual propositions: firms collecting confidential customer information (i.e., Class I) always raise their level of security investment as vulnerability increases, whereas firms without confidential customer information (i.e., Class II) initially increase but then decrease the investment level as vulnerability becomes very high.

The remainder of this article is organized as follows. In the next section, the research literature is reviewed. Section 3 provides background knowledge of measuring vulnerability levels and develops the hypotheses for the empirical study. Section 4 describes the data. The study's results, implications and limitations are discussed in sections 5 and 6.

2. The economics of information security investment

Given increased utilization of the Internet, interest in information security and cyber threats has generated a growing body of research that addresses technical aspects [e.g., 9, 10, 11]. A significant portion of the studies in the fields of computer science and telecommunications has focused primarily on technical aspects, ranging from simple anti-virus software to complex mathematical cryptographic technologies, for protecting information systems and reducing information security breaches. In addition, research using behavioral approaches for preventing information security incidents has attracted many scholars [e.g., 12, 13-17]. Contributors to this research have concentrated mainly on exploring the effect and design of non-technology-based security measures, such as security staff, security policies and security awareness training programs. Moreover, this line of research has also examined technical solutions to lower the risk of information security breaches.

Research focusing on the economic issues of information security has been a more recent phenomenon. Since the early 2000s, several early contributors in the field of information security have recognized that not only technical and behavioral aspects but also economic issues need to be taken into account [e.g., 1, 18, 19, 20]. A large part of research in this area combines findings in public economics (i.e., the presence of positive and negative externalities) and principal-agent theory (i.e., moral hazard and adverse selection caused by misaligned incentives) with research on technical defenses with the goal of developing effective approaches to information security [18, 21-24].

Of the various economic aspects in information security, the most closely related approach to this study is found in studies rooted in cost-benefit analyses of information security investment. Specifically, Gordon and Loeb [1] formulated an economic modeling framework which can help understand when information security expenditures are desirable and how the type of vulnerability affects an organization's investment in information security. A basic assumption of their study was that, while firms cannot influence information security threats, they can control the level of the information security vulnerability and can choose how much they will invest in security to lower the probability of information security breaches. Contrary to the intuition that information security investment might be an increasing function of information security vulnerability, they argued that decisions about information security investment do not depend on vulnerability, but on the reduction in expected loss (therefore, the increase in expected benefit), which is different depending on the form of the security breach probability function: under certain assumptions related to security breach probability functions, organizations may decide to either increase security investment (Class I) or first increase and then decrease security investment (Class II) as their vulnerability of security rises. For Class I, Gordon and Loeb proposed security breach probability functions which have a positive linear relationship with the vulnerability level; that is, the expected benefits of security investment (i.e., the decrease in the expected loss resulting from the increased security) rises as the level of security vulnerability increases [1]. Consequently, they show that, in this class, a firm's optimal information security investment, which maximizes the expected net benefits from an investment in information security, strictly increases but does so at a decreasing rate as the vulnerability level increases (see figure 1). This implies that firms which belong to this class can always be better off by continuously increasing investment in information security as the vulnerability increases: the optimal investment in information security is a (weakly) increasing function of the vulnerability level.

Gordon and Loeb also argue that there is another scenario, involving different functions, which they term Class II. In this class, breach probability functions of information security generate a very low reduction of expected loss for low and very high vulnerability [1]. That is, for low and very high vulnerability levels, an increase in security investment does not greatly reduce expected loss. However, when the vulnerability level is medium to high, an increase in security investment can effectively reduce the expected loss. When vulnerability is either low or very high in this case, the expected benefits of security investment become very small and the investment cannot be justified. Therefore, the optimal information security investment is a initial increasing and then decreasing function of the vulnerability level (see figure 2).

[1] According to the development index published by International Telecommunications Union (ITU), in 2009, it was ranked the 2nd following Sweden [6]. .

[2] The report published by the World Bank indicated that the number of secure Internet servers per one million people in Korea was ranked 14th in 2009 [7]. KISA reported that, in 2009, the Korean information security market increased 9.2 percent from the previous year [8].

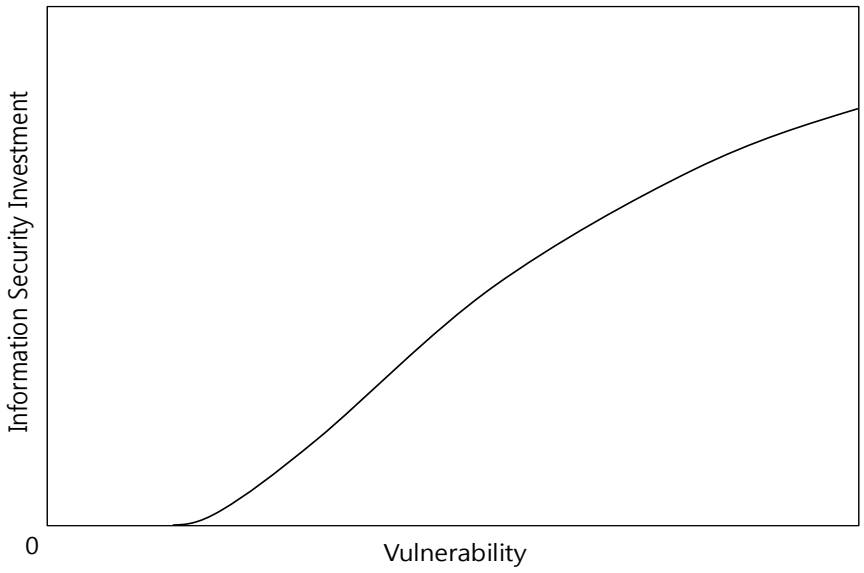

Fig 1. Optimal information security investments for Class I (Adapted from [1])

Subsequently, several other researchers in this field tried to empirically measure the economic costs of information incidents by using, for example, event studies. References [5], [25] and [26] found that different types of security breaches have different economic impacts: security breaches that are not related to confidentiality do not cause a significant negative stock market reaction, whereas such breaches that do result in violations of confidentiality generate a significant negative stock market valuation. Most of the prior studies using the cost-benefit approach, however, provide relatively little information on the characteristics of information security investment.[3] While these studies have generated intuitions about the cost of security breaches, they have generally not provided information related to the actions taken by firms, which face different security environments, with respect to information security. This study expands these prior studies by conducting an empirical analysis of Gordon and Loeb's framework [1].

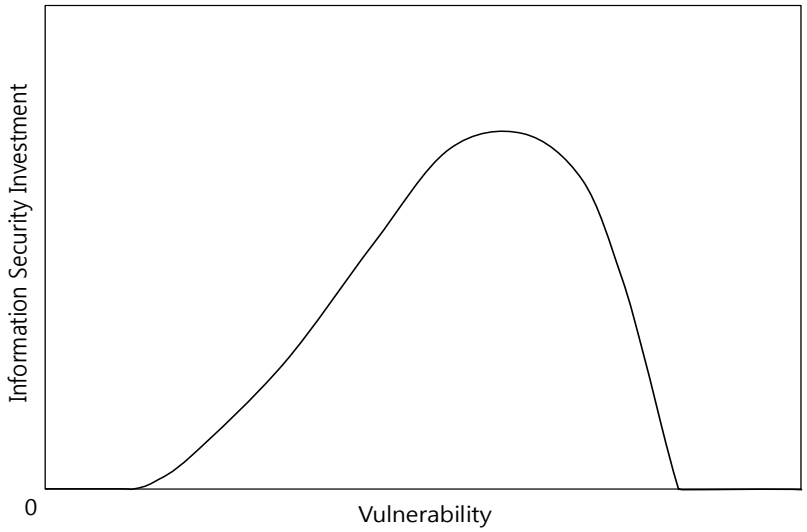

Fig 2. Optimal information security investments for Class II (Adapted from [1])

[3] A notable exception is paper by Tanaka et al. [27]. The authors empirically identified that security investments of e-local governments in Japan can be categorized into Class II. However, they did not address when firms' security investment can belong to Class I.

3. Measuring vulnerability levels and hypotheses

3.1. Measuring vulnerability levels

Firms experience different levels of information security vulnerability for various reasons: some firms suffer vulnerabilities because of unethical or poorly trained employees whereas others may experience vulnerabilities due to outdated security measures. Tanaka et al. [27] that with the increased use of information communication technology (ICT), a firm sharing information and managing it concurrently with other firms is likely to face very high potential risks since its vulnerability is dependent not only on its own countermeasures but also on those of the other firms. They further proposed that security vulnerability depends on a firm's network connection type, which affects the scope and scale of information sharing.

Following the approach proposed by Tanaka et al. [27], this study assumes that a firm's vulnerability level depends on network connection types: closed LAN (e.g., intranet), regional network (e.g., virtual private network (VPN) for employees), and inter-organizational network (e.g., VPNs with employees and other organizations) (see figure 3). We assume that the vulnerability level of a firm using a closed LAN is low since the firm's network is closed and no information is shared with other entities. Firms with this type of network, therefore, usually have strong control over potential vulnerabilities and do not need to overly worry about intrusions from outside attackers through a network. Firms that rely on regional networks have a medium to high exposure to vulnerabilities since they share information only with authorized users through dedicated networks. Since their information sharing is limited within some operational boundaries, these firms can partially control the information security vulnerability. Lastly, the vulnerability level of firms connected through inter-organizational networks can be considered very high. This is because, as Camp and Wolfram [19] indicated, an organization's network connected to other firms' networks can be accessible via the dedicated connections among them. Therefore the vulnerability of firms with inter-organizational networks cannot be controlled by a few networked organizations, but requires all networked firms' concurrent efforts.

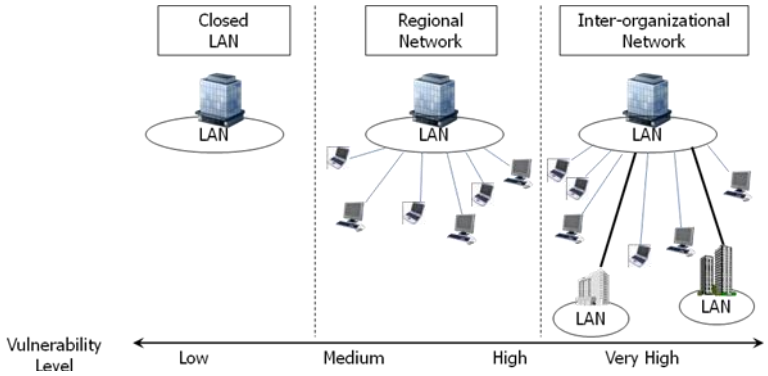

Fig 3. Network types and corresponding vulnerability levels (Adapted from [27])

It should be noted, however, that there are downsides of using the association of network types with vulnerability levels. First, the classification can only take external threats into account and cannot take account of internal threats that are caused by former or current employees. Second, even if we do not specifically comment on connectivity via the Internet, we implicitly assume that all organizations have an Internet connection, and that cyber perpetrators can presumably intrude into an organization via this connection. That is, even firms that predominantly use closed LANs can have Internet connections which might increase their vulnerability level. In spite of these weaknesses network types are still the plausible proxy for vulnerability levels, since they can at least measure the size and number of dedicated and trusted connections, which is the main source of security vulnerability.

Table 1. Relationship between vulnerability levels of different network types and information security investment (Modified from [27])

Network type	Vulnerability level	Cost effectiveness	Information security investment
Closed LAN	Low	Non-cost-effective	No investment
Regional Network	Medium – High	Cost-effective	Potential investment
Inter-organizational Network	Very high	Cost-effective / Non-cost-effective	Potential investment / No investment

Table 1 illustrates the relationship between vulnerability levels of different network types and information security investment. When firms' network types are closed LANs, the level of the information security vulnerability is low. In such cases, as Gordon and Loeb [1] noted, information security investment is not cost-effective and the firms will not invest in information security since the cost of security is higher than the expected loss from an information security breach. When firms use regional networks, the vulnerability level is medium to high. Since investment in information security in this case is cost-effective, firms are likely to make an investment in information security. When firms employ inter-organizational networks, there are two possible cases as mentioned earlier. In the first case the security breach probability functions are linear in terms of vulnerability. In this case, the optimal investment in security increases at a decreasing rate as the vulnerability of the information security becomes very large

(see figure 1). Therefore, information security investment is cost-effective and even firms with very highly vulnerable information systems still have incentives to invest in information security. In the second case the security breach probability functions are not linear and exhibit the characteristic that the costs of the protection of very vulnerable information systems are very high and exceed the benefit of such protection (see figure 2). In this case, information security investment is not cost-effective and hence firms will not invest in information security.

3.2. Two hypotheses

This subsection describes the hypotheses informing the empirical research design. Based on the discussion in the previous section, it is reasonable to assume that organizations face an increasing potential vulnerability problem as their networks become strongly correlated with other firms' networks [27]. On the other hand, organizations have to consider the cost effectiveness of an information security investment when they make such investment decisions [27]. However, as noted earlier, when organizations are faced with very high vulnerability, there can be two possibilities based on the forms of the security breach probability functions. That is, organizations can either make a decision to invest or decide not to make an investment. We hypothesize that firms which have to manage strictly confidential information[4] belong to Class I since the leakage of such information cause greater losses than the leakage of other types of information [5]. These firms will not decrease the level of investment in information security despite the increase in the level of vulnerability. Therefore, we hypothesize:

H1: Firms that manage a large amount of strictly confidential information increase the level of investment in information security with a decreasing rate as the level of the security vulnerability increases.

On the other hand, we assume that firms with little or no confidential information fall into Class II. That is, when the vulnerability is very high, firms in this class would reduce the level of information security investment since it might not be cost effective to protect such non-confidential information. As a result:

H2: Firms that manage little or no confidential information first increase and then decrease the level of investment in information security as the level of the security vulnerability increases.

4. Data

The data for this study was extracted from the 2007 and 2008 Korean Information Security Surveys, conducted by the Korea Internet & Security Agency [28, 29]. The survey covered 10 industries using a random sample of businesses with more than five employees that participated in the Korean Census on Basic Characteristics of Establishments [30]. The 2007 survey was conducted using personal interviews while the 2008 survey combined internet-based and personal interview techniques for data collection. Survey respondents were the information security (IS) or finance directors of the participating organizations. The main goal of these surveys was to gather detailed information on current information security practices in Korean businesses. Over this two-year period, the surveys collected data on 5,336 organizations (2,508 in 2007 and 2,828 in 2008). For purposes of empirical analysis, we pooled the data from both years. This is equivalent to assuming that the factors influencing the dependent variable did not change during these two years, which seems defensible. Table 2 lists the variables used.

Table 2. Dependent and independent variables

Variables	Measures	Description
Dependent variables	• Information security investment rate	• The relative portion of a firm's IT budget which is dedicated to the firm's activities related to information security • Seven categories: 1(0%), 2(less than 1%), 3(1~ less than 3%), 4(3~ less than 5%), 5(5~ less than 7%), 6(7~ less than 10%), and 7(10% or more)
Independent variables	• Vulnerability level	• Firms with a closed LAN, a regional network, or an inter-organizational network are categorized as having low, medium-high, or very high vulnerability, respectively. • Each category is coded as a 0-1 dummy variable and low vulnerability level is used as a default category.
	• Firm size	• Proxied by the number of employees • Five categories; 1(5~9 employees), 2(10~49 employees), 3, 50~249 employees), 4(250~299 employees), and 5(300 employees or more)
	• Industry type	• 10 industries • Each category is coded as a 0-1 dummy variable and 'Other service industry' is used as a default category.

[4] This study uses narrowly defined confidential information; that is, confidential information is limited to the information which is critical to a firm's survival. For some information that could, more broadly, be considered confidential, the cost of security can be far higher than the expected value of damage from the leakage of the information. For example, information related to a firm's new product portfolio or related to selling a particular business unit may become nearly public information and too expensive to be secured when security vulnerability is very high [1]. A firm's rational activity in this case is not to invest in security. This study does not regard this type of information as confidential.

We use customer private information as a proxy for confidential information. The data was divided according to whether or not a firm collects private information from customers through its website: firms collecting private information from customers through their websites are categorized into one group, for the purpose of testing H1, and firms not collecting the private information are categorized into the other group, for the purpose of testing H2.[5] This categorization reflects the assumption that firms collecting private information online will have to ensure a higher level of confidentiality than firms that do not collect private information online. According to references [5] and [25], the leakage of private information caused by unauthorized access to users' account information or credit card data generates great reputation loss and negative market valuation to a firm. In addition, recent cases show that leakage of customer information causes huge financial damage to a firm.[6] Therefore, we hypothesize that firms which manage confidential information collected from customers will not reduce the level of information security investment in spite of high security vulnerability (i.e., they fall within Class I). In contrast, firms that do not collect confidential information online will reduce investment in information security at high vulnerability levels since their benefits under these conditions are very low (i.e., they are in Class II). Table 3 shows how information types are here classified according to whether or not firms collect private information. Since data was collected from firms with websites, the number of observations was reduced to 4,378.

Table 3. Information types and classes of firms

Private information	Information type	Cost effectiveness when very high vulnerability	Class
Collect	High confidentiality	Cost-effective	Class I
Not collect	Low confidentiality	Non-cost-effective	Class II

The share of the total information technology budget dedicated to the firm's activities related to information security is used as a dependent variable (hereinafter referred to as 'information security investment rate') [31].[7] Despite the potential limitation,[8] this variable is widely used to measure the level of information security investment [e.g., 4, 31, 32, 33-36]. The KISA surveys document information security investment rate using seven categories: 0%, 0~1%, 1~3%, 3~5%, 5~7%, 7~10% and over 10%. We assign 1 through 7 to each category, respectively. Figure 4 shows the frequency with which organizations invest in information security. Only 10.2 percent of organizations had invested more than 5 percent of their total information technology budgets in information security.

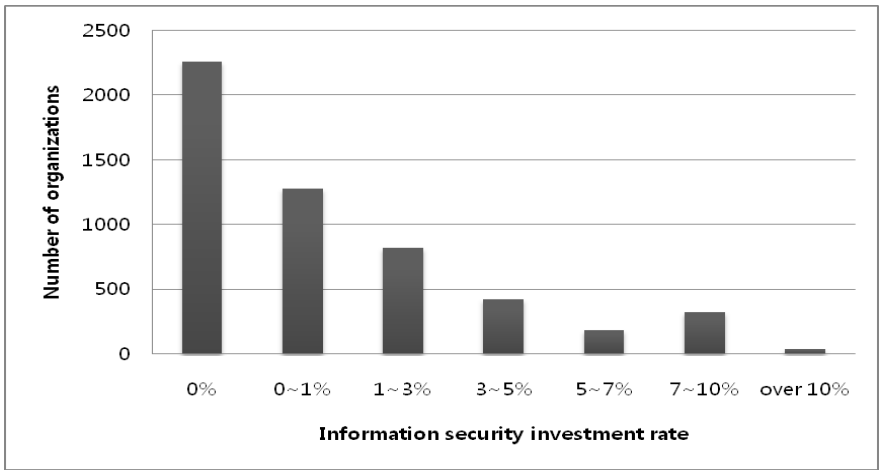

Fig 4. Number of organizations investing in information security by information security investment rate

As discussed above, an organization's network type is used as a proxy for its vulnerability level. The KISA surveys differentiate three network types: closed LAN, regional network, and inter-organizational network (see figure 5). Organizations

[5] While there might be some firms which collect private information offline, it is assumed here that these firms also collect private information online.

[6] For example, TJX Companies, Inc announced that the cost of a data breach, in which hackers stole 45 million customer credit and debit card information, was estimated at $256 million.

[7] One might argue that it is not clear whether a firm spending a low share of its high IT budget on security is in a better situation than a firm spending a high share of its low IT budget on security. However, since firms' IT budgets are different based on their dependency on IT, it can at least be inferred that firms spending a high share of their IT budget on security make a stronger effort to secure their information system than do firms spending a low share of their IT budget on security.

[8] According to Richardson [4], not all the funds in the security budget come from an IT budget – e.g., some funds can come from the audit department or other departments.

using their closed LANs have their own intranet, but are not connected with outside organizations via dedicated connections.[9] We assign these organizations to the group of low information security vulnerability. Organizations which use regional networks are connected outside their own organizations through dedicated networks, but their connections are restricted to selected employees. We classify such organizations within the group with medium to high levels of information security vulnerability. Organizations employing inter-organizational networks are connected not only with employees outside the organizations but also directly with other business partners via dedicated and trusted connections. We treat them as belonging to the group with a very high information security vulnerability level. Each category is coded as a 0-1 dummy variable and the low vulnerability level is used as a default category.

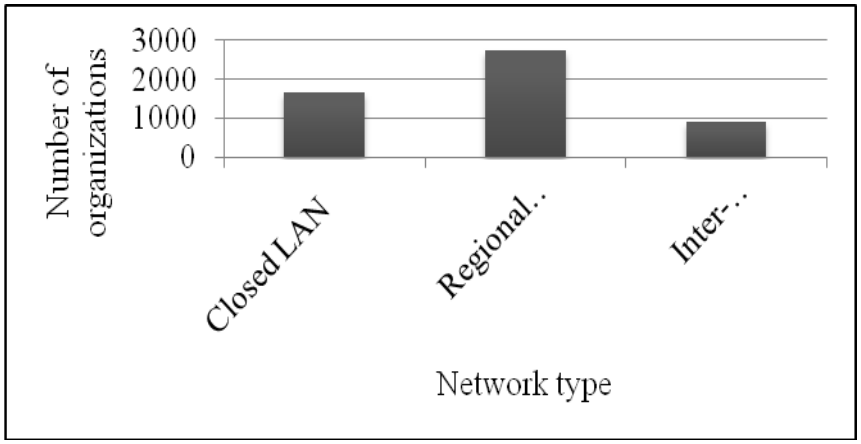

Fig 5. Number of organizations by network types

In addition, we included several control variables that may also influence information security investment. First, we take the effect of organization size into account since it can affect the level of information security investment (see also [27]). For example, a lack of IT resources in small organizations may be associated with under-investment in information security regardless of their vulnerability levels. In contrast, large organizations with sufficient IT resources may be able to invest high amounts in information security even if their vulnerability level is low. Firm size is measured by the number of employees. The KISA surveys classify firms into five categories: 5~9 employees, 10~49 employees, 50~249 employees, 250~299 employees and over 300 employees. We assign 1 through 5 to each category, respectively (see figure 6).

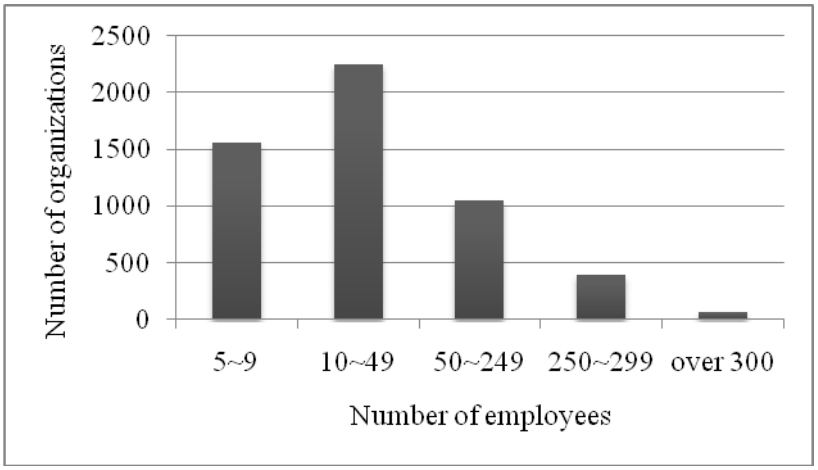

Fig 6. Number of organizations by number of employees

Second, we control for industry type in the regression analysis since industry-specific differences may influence the level of vulnerability and, consequently, in turn, information security investment. For instance, firms in the banking industry are attacked more often and customers of this industry are usually very sensitive to security breaches. Therefore, other things being equal, one would expect financial service providers to invest more in information security than firms in other industries. The surveys group firms in 10 different industries: (1) agriculture, forestry, and fisheries, (2) manufacturing, (3) construction, (4) wholesaling, (5) retailing, (6) restaurant and lodging, (7) logistics and telecommunications, (8) financial and insurance, (9) real estate, renting and business activities, and (10) other services. We create nine dummy variables indicating the industry type of the organization using 'other services' as the default category.

[9] As mentioned above, even firms using closed LANs might have Internet connections.

5. Findings

The information security investment rate is the dependent variable in the regression analyses. However, the predominance of zeros and the discrete characteristic of the dependent variable suggest that ordinary least squares regression is inappropriate. According to [37] and [38], if the dependent variable shows these characteristics, the coefficient estimates of ordinary least squares regression are asymptotically biased and inconsistent.

Given these characteristics of the dependent variable, Poisson or negative binomial models can be applied. Because of the limitation of the Poisson model caused by the assumption of equivalence between the mean and variance of the dependent variable, however, we use the negative binomial regression model which makes a model for our analysis more desirable. Therefore, we employ the negative binomial regression model with a maximum likelihood estimation developed by Hausman, Hall and Griliches [39]. This model can be specified as:

$$P\left(\frac{k_i}{\varepsilon}\right) = e^{-\mu_i \exp(\varepsilon)} \mu_i^{k_i} \Big/ k_i!$$

where k_i is firm *i*'s information security investment rate and $\mu_i = e^{(B'X_i+\varepsilon)}$ when X_i is the vector of independent variables for firm *i*'s case. Also, $P(k_i/\varepsilon)$ indicates the probability that firm *i* will make information security investment in *k*th category; μ_i is the mean of k_i or the average of information security investment rate; $\exp(\varepsilon)$ is assumed to have a gamma distribution with a mean of 1.0 and a variance of α^2. The estimated model has the form $k_i = B'X_i + \varepsilon$. Estimates of the parameters are the effects of the independent variables on the expected information security investment rate.

To investigate the effect of vulnerability on information security investment, we estimated the equation for the likelihood of information security investment using multivariate regression analysis. Table 4 presents the results from the negative binomial regression analysis. Models 1 and 3 are the baseline models, which include control variables only, for firms collecting private information through their websites and those firms who do not collect such information through their websites. Model 2 tests the relationship between the information security investment rate and the vulnerability levels when firms collect private information from customers. Model 4 tests the same relationship with Model 2, but under circumstances when firms do not collect customers' private information.[10]

Several interesting conclusions can be drawn from the results in Table 4. For Model 2 which includes firms collecting private information, the positive coefficients of the dummy variables for vulnerability levels indicate that a firm's likelihood of investment in information security is positively influenced by the firm's level of security vulnerability. The magnitudes and signs of the coefficients can be interpreted as the average proportional change in the dependent variable, which is the information security investment rate, resulting from a one-unit change in the independent variable. It should be noted that the results of the calculations should be interpreted carefully because the dependent variable is used as a seven-category variable. The coefficient of the variable for medium to high vulnerability indicates a 0.135 percent increase in the dependent variable compared to low vulnerability, which is the reference group. Similarly, the coefficient of 0.231 for the variable for very high vulnerability is interpreted to mean that a change of vulnerability from a low level to a very high level is associated with a 0.231 percent increase in the dependent variable. Therefore, other things being equal, firms with medium-high vulnerability are likely to invest more in information security than firms with low vulnerability, and firms with very high vulnerability are likely to make the highest security investment. The findings also evidence that the coefficient of 0.231 for the very high vulnerability variable is smaller than the coefficient of 0.135 for the medium to high vulnerability variable multiplied by two, which is 0.27. This implies that security investment increases with a decreasing rate. Therefore, this result supports H1: firms managing confidential information are likely to increase information security investment, but do so at a decreasing rate as the firms' vulnerability level increases.

For Model 4, which includes firms not collecting private information, the results suggest the presence of propensities similar to those shown in the previous analysis: the coefficient of the variable for medium to high vulnerability indicates 0.179 percent increase in the dependent variable compared to the low vulnerability variable whereas the coefficient of 0.169 for the very high vulnerability variable shows 0.169 percent increase in the dependent variable compared to the low vulnerability variable. This implies that, although firms with very high vulnerability are likely to invest more in information security than firms with low security vulnerability, the firms are likely to invest less in information security than firms with medium to high vulnerability. Therefore, this result supports H2 as presented in the previous section. In sum, we found evidence that, when firms' vulnerability level is between low to high, they increase the investment as the vulnerability level increases. However, when the vulnerability becomes very high, our findings show that only firms maintaining confidential information are likely to increase information security investment.

With respect to control variables, the results indicate that a firm's probability of information security investment is significantly affected by firm size: in all models, the size variable has positive and statistically significant coefficients. The industry type variables indicate that a firm's probability of information security investment is affected by certain types of industries, but only the financial and insurance industry shows positive signs and statistical significance in all models. This implies that firms in this industry have an incentive to invest more in information security regardless of the collection of private information.

To examine the goodness of fit of the models, we conducted chi-squared tests for the models by comparing the difference between log likelihood values of the current models and the null models (i.e., the intercept-only models). All values yielded $p<0.001$ and hence the models were statistically significant. We also identified that likelihood-ratio G^2 tests show that the introduction of vulnerability levels in Models 2 and 4 significantly improved the fit of the models.

[10] Pearson correlations of the independent variables did not show any significant correlations.

Table 4. Negative binomial regression results for information security investment rate[a]

Variable	Collecting private information		Not collecting private information	
	Model 1	Model 2	Model 3	Model 4
Intercept	0.739*** (0.053)	0.622*** (0.066)	0.315*** (0.042)	0.255*** (0.044)
Medium to high vulnerability		0.135** (0.053)		0.179*** (0.031)
Very high vulnerability		0.231*** (0.057)		0.169*** (0.041)
Firm size	0.111*** (0.016)	0.098*** (0.016)	0.175*** (0.013)	0.154*** (0.014)
Agriculture, forestry & fisheries	0.223*** (0.082)	0.202** (0.081)	0.080 (0.082)	0.059 (0.081)
Manufacturing	0.016 (0.063)	0.024 (0.063)	0.167*** (0.042)	0.141*** (0.042)
Construction	-0.095 (0.099)	-0.074 (0.098)	0.035 (0.053)	0.029 (0.053)
Wholesaling	-0.050 (0.068)	-0.036 (0.068)	0.177*** (0.049)	0.152*** (0.049)
Retailing	-0.105* (0.059)	-0.114* (0.059)	0.038 (0.056)	0.018 (0.056)
Restaurant & lodging	0.007 (0.074)	0.026 (0.074)	-0.084 (0.066)	-0.090 (0.066)
Logistics & telecommunications	-0.014 (0.066)	-0.019 (0.066)	0.158*** (0.055)	0.127** (0.055)
Financial & insurance	0.092** (0.047)	0.084* (0.047)	0.223*** (0.057)	0.163*** (0.058)
Real estate, renting & business services	0.001 (0.059)	-0.001 (0.059)	0.189*** (0.047)	0.172*** (0.047)
N	1600	1600	2778	2778
χ^2	64.44***	87.69***	218.04***	253.18***
log-likelihood	138.15	147.28	-1196.84	-1178.58

[a] Standard errors are in parentheses.
* p<.0.1
** p<.05
*** p<.01

6. Implications and limitations

Given the broader use of ICTs by organizations, the protection of information assets has become as critical to organization as is the protection of traditional tangible assets [1]. Therefore, many researchers have addressed the issue of information security. While a variety of theoretical work exists, which studies information security from technical, behavioral and economic viewpoints, relatively little empirical research has been conducted, particularly from an economic perspective. This study helps fill this gap in the literature by conducting an empirical analysis, based on the economic model for information security investment strategies presented by Gordon and Loeb [1]. The economic model they formulated, which considered the relationship between the vulnerability level and information security investment at a conceptual level, recognized that while some expenditures on information security is beneficial to firms, not all security investments are always worthwhile. Therefore, in order to determine the amount to invest in information security, firms would compare the expected benefits of the investment with cost of the investment. Gordon and Loeb [1] suggested two broad types of security breach probability functions: for firms with the first class of security breach probability functions, the increases in the amount of investment in information security reduce the expected loss from an information security breach. The optimal investment in information security of such firms is always (weakly) increasing as the level of vulnerability increases. For firms with the second class of security breach probability functions, they are not always better off investing their resources on high vulnerability information assets. A key feature of this class of security breach probability functions is that the cost of protecting highly vulnerable information sets becomes extremely

expensive as the vulnerability of the information set becomes very large. The optimal investment in information security first increases and then decreases in the vulnerability. Based on reference [1], the analysis undertaken in this article investigates, in particular, how the vulnerability level, and the expected loss associated with the different information types (i.e., confidential and non-confidential), affect the level of investment in information security.

This article verified that the decision a firm makes regarding information security investments depends on the vulnerability level of particular information types. The analysis conducted in this article found that, for firms collecting highly confidential information such as user's personal information, the amount to invest in information security is a (weakly) increasing function of the vulnerability level (i.e., Class I). For these firms, since a breach of such information can result in a catastrophic negative impact on the value of the firms, they try to avoid the large expected loss associated with a breach of highly confidential information regardless of the vulnerability level. On the other hand, for firms not collecting confidential information, the amount spent on information security first increases and then decreases with the vulnerability level (i.e., Class II). For these firms, the leakage of such information generates only a small expected loss. Therefore, when the information is so vulnerable to keep it to a very high level of security, more spending on information security is not worth the cost (i.e., marginal costs exceed marginal benefits), and thereby the firms may protect the information only at a moderate level.

Our findings for firms differing actions corresponding to these two different classes shed new light on the issue of the level of investment in information security. The empirical results illustrated above suggest that the concave relationship between the vulnerability level and the information security investment for firms with confidential information holds in our sample of firms. That is, for firms in this group, this study identified that information security investment increases with a decreasing rate, as the vulnerability becomes high. In contrast, it was found that firms with little or no confidential information do not always increase the amount to invest in information security; for firms in this group, the information security investment initially rises, but ultimately decreases as the vulnerability becomes very high. This means that information security investment for firms of this group is not cost-effective when the vulnerability level is very high. A meaningful effort of managers in the firms with very high vulnerability might translate into an investment in information security only at a moderate level [1].

Despite the interesting findings, the analysis conducted here has some limitations. One limitation is inherent to the data. The data used in this study was mostly based on categorized variables, rather than qualitative values. In addition, the data was available for only two single points in time. Therefore, it was not possible to systematically explore dynamic aspects of information security investment. This study also did not consider the interdependencies of information security decisions among firms that are connected to each other [e.g., 24, 40].

One also has to keep in mind that the empirical data for the paper reflect the situation in one particular national context. Whereas the findings in our sample can be generalized for the South Korean economy in general, one cannot assume generalizability to other nations without additional triangulation. Thus, the findings and lessons may be more applicable to nations with comparable economic structure and legal and regulatory institutions. This will likely include other OECD member countries but the transferability to nations in the developing world maybe more limited. Consequently, it would be highly desirable to have a more standardized and more detailed information basis available across nations.

ACKNOWLEDGEMENTS

The author would like to thank the Korean Internet & Security Agency (KISA) for providing access to data from the 2007 and 2008 Korean Information Security Surveys.

REFERENCES

[1] L. Gordon and M. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, vol. 5, pp. 438-457, 2002.
[2] X. Zhao, *et al.*, "Managing Interdependent Information Security Risks: An Investigation of Commercial Cyberinsurance and Risk Pooling Arrangement," presented at the Thirtieth International Conference on Information Systems, Phoenix, AR, 2009.
[3] R. P. Majuca, *et al.*, "The evolution of cyberinsurance. In ACM Computing Research Repository (CoRR), Technical Report cs.CR/0601020," 2006.
[4] R. Richardson, "2008 CSI Computer Crime and Security Survey," Computer Security Institute2008.
[5] K. Campbell, *et al.*, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer Security*, vol. 11, pp. 431-448, 2003.
[6] International Telecommunication Union, "Measuring the Information Society: The ICT Development Index," International Telecommunication Union (ITU), Geneva, Switzerland2009.
[7] World Bank, "World Development Indicators 2010," World Bank, Washington, DC2010.
[8] N. Ahn, "Information Security Market Increases 10% to 800 Billion in 2009," in *Maeil Business Newspaper*, ed. Seoul, Korea: Maeil Business Newspaper, 2010.
[9] F. B. Cohen, *Protection and security on the information superhighway*. New York: John Wiley & Sons, Inc, 1995.
[10] D. Denning and P. J. Denning, *Internet besieged: Countering cyberspace scofflaws*. Reading, MA: ACM Press, 1997.
[11] B. Mukherjee, *et al.*, "Network intrusion detection," *IEEE network*, vol. 8, pp. 26-41, 1994.
[12] D. K. Hsiao, *et al.*, *Computer security*. New York: Academic Press, 1979.
[13] D. B. Parker, *Computer security management*. Reston, VA: Reston, 1981.
[14] D. B. Parker, *Fighting computer crime*. New York: Scribner, 1983.
[15] D. Straub Jr, "Effective IS Security," *Information Systems Research*, vol. 1, pp. 255-276, 1990.
[16] D. W. Straub Jr. and W. D. Nance, "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly*, vol. 14, pp. 45-60, 1990.
[17] D. W. Straub Jr. and R. J. Welke, "Coping with systems risk: security planning models for management decision making," *MIS Quarterly*, pp. 441-469, 1998.
[18] R. Anderson, "Why Information Security is Hard - An Economic Perspective," in *17th Annual Conputer Security Applications Conference*,

New Orleans, LA, 2001.
[19] L. J. Camp and C. Wolfram, "Pricing security," in *The CERT Information Survivability Workshop*, Boston, 2000, pp. 31–39.
[20] H. Varian, "Managing Online Security Risks," in *The New York Times*, ed, 2000.
[21] L. J. Camp, "Economics of Information Security," *SSRN eLibrary*, 2006.
[22] L. Gordon and M. Loeb, "Economic aspects of information security: An emerging field of research," *Information Systems Frontiers*, vol. 8, pp. 335-337, 2006.
[23] L. Gordon and M. Loeb, *Managing Cybersecurity Resources: A Cost-Benefit Analysis*. New York: McGraw-Hill, 2006.
[24] L. J. Camp, "The State of Economics of Information Security," *I/S A Journal of Law and Policy in the Information Society*, vol. 2, pp. 189-205, 2005.
[25] A. Acquisti, *et al.*, "Is there a cost to privacy breaches? An event study," 2006.
[26] J. Muntermann and H. Roßnagel, "On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market," *Identity and Privacy in the Internet Age*, pp. 1-14, 2009.
[27] H. Tanaka, *et al.*, "Vulnerability and information security investment: An empirical analysis of e-local government in Japan," *Journal of Accounting and Public Policy*, vol. 24, pp. 37-59, 2005.
[28] Korean Internet & Security Agency, "2007 Korean Information Security Survey," Korean Internet & Security Agency, Seoul, Korea2007.
[29] Korean Internet & Security Agency, "2008 Korean Information Security Survey," Korean Internet & Security Agency, Seoul, Korea2008.
[30] Statistics Korea, "Korean Census on Basic Characteristics of Establishments," Statistics Korea, Daejon, Korea2006.
[31] L. Gordon, *et al.*, "2004 CSI/FBI computer crime and security survey," *COMPUTER SECURITY JOURNAL*, vol. 20, pp. 33-51, 2004.
[32] J. Anderson, "Why We Need a New Definition of Information Security " *Computers & Security*, vol. 22, pp. 308-313, 2003.
[33] L. Gordon, *et al.*, "2005 CSI/FBI computer crime and security survey," Computer Security Institute2005.
[34] L. Gordon, *et al.*, "2006 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY."," *Computer*, vol. 22, 2006.
[35] M. Johnson and E. Goetz, "Embedding information security into the organization," *IEEE Security & Privacy*, pp. 16-24, 2007.
[36] R. Richardson, "2007 CSI computer crime and security survey," Computer Security Institute2007.
[37] W. H. Greene, *Econometric analysis*, 5th ed. Upper Saddle River, NJ: Pearson Education Inc., 2003.
[38] S. Long, *Regression models for categorical and limited dependent variables*. Thousand Oaks, CA: Sage Publications, Inc, 1997.
[39] J. Hausman, *et al.*, "Econometric Models for Count Data with an Application to the Patents-R & D Relationship," *Econometrica*, vol. 52, pp. 909-938, 1984.
[40] H. Kunreuther and G. Heal, "Interdependent security," *Journal of Risk and Uncertainty*, vol. 26, pp. 231-249, 2003.