# Types of Information Vulnerability and IT Security Investment: An Empirical Analysis of Businesses in Korea

W. SHIM*
Michigan State University, MI, USA

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 the information types as vulnerability increases. The empirical research uses data from 4,378 organizations that participated in surveys conducted by the Korea 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 first increase then decrease the investment as vulnerability rises.

Keywords: Security investment, Vulnerability, Customer information, Confidentiality

## 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 (Gordon & Loeb, 2002). Firms have increased their expenditure on information security and have adopted a range of solutions to protect information systems (Zhao, Xue, & Whinston, 2009). Although technical security solutions have continuously improved and employed, various types of security breaches have also continued to increase (Majuca, Yurcik, & Kesan, 2006). The 2008 CSI Computer Crime and Security Survey (Richardson, 2008) 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 (Richardson, 2008). Moreover, the survey reported that the average loss of organizations from security incidents was around $300,000 per organization (Richardson, 2008). 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 (Gordon & Loeb, 2002). This inadequacy of the investments renders organizations exposed to cyber threats.

The primary intention of this study is to make conceptual and empirical contributions 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 Gordon and Loeb (2002) and Campbell et al. (2003). Gordon and Loeb (2002) demonstrated that optimal information security investment is affected by the information

*Author's addresses: W. Shim, Department of Telecommunication, Information Studies & Media, College of Communication Arts & Science, East Lansing, Michigan, USA. Tel: 1-517-974-4250. Fax: 1-517-355-1292. E-mail: shimwoo@msu.edu

security vulnerability and the associated loss from the vulnerability. The authors proposed that 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 resulted by the increased security investment) increases as vulnerability rises. Firms with security probability functions belonging to Class I therefore can be better off concentrating the security investments on highly vulnerable information sets. Class II security breach probability functions are convex in vulnerability, that is, EBIS first increases and then decreases as vulnerability rises. The functions in this class have the property that protecting information sets becomes exceedingly expensive as vulnerability becomes very high. Gordon and Loeb (2002) concluded that, when a security environment is very vulnerable, a firm's 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. Campbell et al. (2003), 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 to prevent the high increase in expected loss which results in a highly negative impact on stock market valuations.

Taking the implications from Gordon & Lobe (2002) and Campbell et al. (2003) together, 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 because is used for two reasons: first, Korea is a country with 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. With caution, the results 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 the confidential

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

[2] The report published by World Bank indicated that the number of secure Internet servers per one million people in Korea was ranked 14th in 2009 (World Bank, 2010). KISA reported that, in 2009, Korean information security market was increased a 9.2 percent from the previous year (Ahn, 2010).

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 detailed 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., Cohen, 1995; Denning & Denning, 1997; Mukherjee, Heberlein, & Levitt, 1994). 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., Hsiao, Kerr, & Madnick, 1979; Parker, 1981, 1983; Straub Jr, 1990; Straub Jr. & Nance, 1990; Straub Jr. & Welke, 1998). 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, the 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., R. Anderson, 2001; Camp & Wolfram, 2000; L Gordon & Loeb, 2002; Varian, 2000). 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 to develop effective approaches to information security (R. Anderson, 2001; Camp, 2005; Gordon & Loeb, 2006a, 2006b).

Of the various economic aspects in information security, the most closely related approach to this study are studies rooted in cost-benefit analyses of information security investment. Specifically, Gordon and Loeb (2002) started to develop 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 firms can control the level of the information security vulnerability,[3] and can choose how much they will invest in security to lower the probability of information security breach. Contrary to the intuition that information security investment might be an increasing function of the information security vulnerability, they argued that decisions on 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 make either increasing security investment (Class I) or first increasing and then decreasing security investment (Class II)

[3] However, the authors assume that firms cannot influence information security threats (L Gordon & Loeb, 2002).

as their vulnerability of security rises. For Class I, Gordon and Loeb (2002) 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) raises as the level of security vulnerability increases. 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 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.

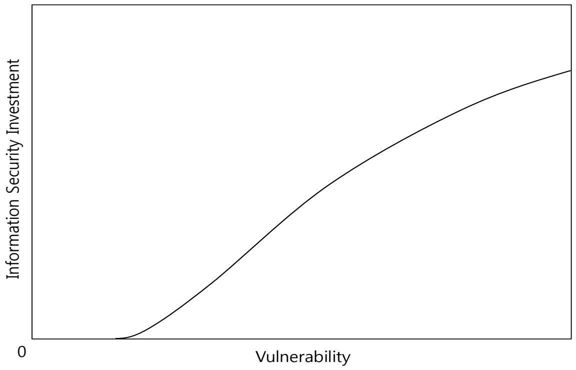

Fig 1. Optimal information security investments for Class I (Adapted from Gordon and Loeb (2002))

Gordon and Loeb (2002) also argue that there is another scenario, called 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. 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. In this class, when vulnerability is either low or very high, the expected benefits of security investment become very small and the investment cannot be justified. Therefore, the optimal information security investment is a first increasing and then decreasing function of the vulnerability level (see figure 2).

Subsequently, several other researchers in this field tried to empirically measure the economic costs of information incidents, for example, by using event studies. Cambell et al. (2003), Acquisti et al. (2006) and Muntermann & Roßnagel (2009) 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 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.[4] While the studies have generated intuitions about the cost of security breaches, they have generally not provided information related to activities of firms, which face different security environments, on information security. This study expands these prior studies by conducting an empirical analysis of Gordon and Loeb's (2002) framework.

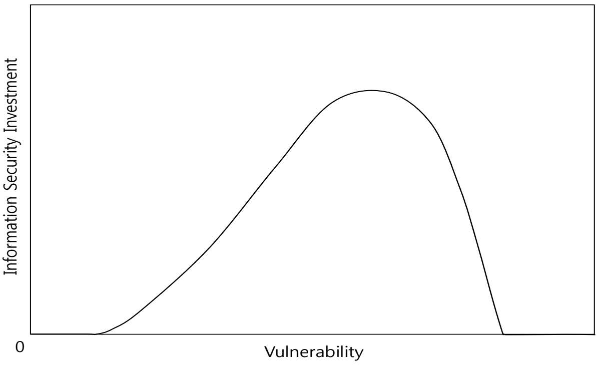

Fig 2. Optimal information security investments for Class II (Adapted from Gordon and Loeb (2002))

## 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 suffer due to outdated security measures. Tanaka et al. (2005) argued 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 the vulnerability is dependent not only on countermeasures of the firm but also on those of the others. 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. (2005), 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 worry much 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, 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

[4] A notable exception is paper by Tanaka et al. (2005). The authors empirically identified that security investments of e-local governments in Japan can be categorized into Class II. However, they did not present when firms' security investment can belong to Class I.

is because, as Camp and Wolfram (2000) 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.[5]

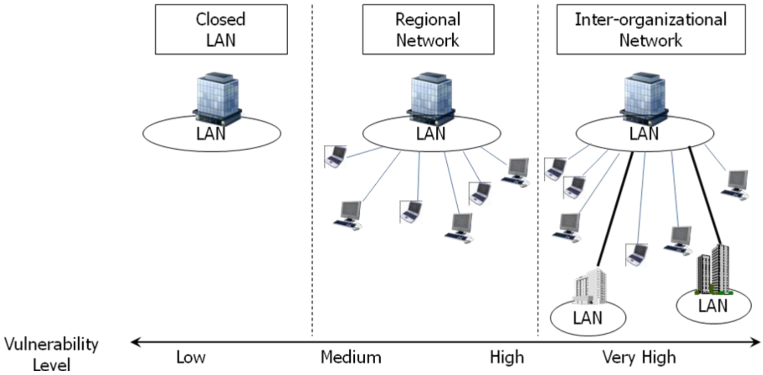

Fig 3. Network types and corresponding vulnerability levels (Adapted from Tanaka et al. (2005))

Table I illustrates the relation 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 this case, as Gordon and Loeb (2002) 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 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 the 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 show 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.

[5] However, there are downsides of the association of network types with vulnerability levels. First, the classification can only take external threats into account, while this 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 the 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 the 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 I. Relation between vulnerability levels of different network types and information security investment (Modified from Tanaka et al. (2005))

| **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<br>/ Non cost effective | Potential investment<br>/ No investment |

### *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 increasing potential vulnerability problem as their networks become strongly correlated with other firms' networks (Tanaka, et al., 2005). On the other hand, organizations have to consider the cost effectiveness of the information security investment when they make the investment decisions (Tanaka, et al., 2005). However, as we mentioned earlier, when organizations face very high vulnerability, there can be two possibilities based on the forms of the security breach probability functions. That is, organizations can make either investment or no investment. We hypothesize that firms which have to manage 'strictly' confidential information[6] belong to Class I since the leakage of such information cause greater losses than the leakage of other types of information (Campbell, et al., 2003). They 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 only little 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 (2007, 2008). The

[6] 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 confidential information, 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 (Gordon & Loeb, 2002). 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.

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 (Statistics Korea, 2006). 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. Main goal of these surveys was to gather detailed information on current information security practices in Korean businesses. Over the period of two years, 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 do not change during the two years, which seems defensible. Table II lists the variables used.

Table II. 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 on information security<br>• 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 low, medium-high, or very high vulnerability, respectively.<br>• 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<br>• 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<br>• Each category is coded as a 0-1 dummy variable and 'Other service industry' is used as a default category. |

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 which is to test H1, and firms not collecting the private information are categorized into the other group which is to test H2.[7] This categorization reflects the assumption that firms collecting private information

[7] There might be some firms which collect private information offline. However, it may be reasonable to assume that these firms also collect private information online.

online will have to ascertain higher confidentiality than firms that do not collect private information online. According to Campbell et al. (2003) and Acquisti et al. (2006), 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.[8] 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., be in Class I). In contrast, firms that do not collect confidential information online will reduce investment in information security at high vulnerability levels since its benefits under these conditions are very low (i.e., they are in Class II). Table 3 shows how we classify information types by whether or not firms collect private information. Since we only used firms with websites, the number of observations was reduced to 4,378.

Table III. 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 on information security is used as dependent variable (hereinafter referred to as 'information security investment rate') (Gordon, Loeb, Lucyshyn, & Richardson, 2004).[9] Despite the potential limitation,[10] this variable is widely used to measure the level of information security investment (e.g., J. Anderson, 2003; Gordon, et al., 2004; Gordon, Loeb, Lucyshyn, & Richardson, 2005, 2006; Johnson & Goetz, 2007; Richardson, 2007, 2008). 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 of organizations investing in information security. Only 10.2 percent of organizations had invested more than 5 percent of their total information technology budgets in information security.

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

[9] One might argue that it is not clear whether a firm spending a low share of its high IT budget on security is better 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 IT budget on their security make a stronger effort to secure their information system than firms spending a low share of IT budget on their security.

[10] According to Richardson (Richardson, 2008), not all the funds in the security budget come from IT budget – e.g., some funds can come from audit or other departments.

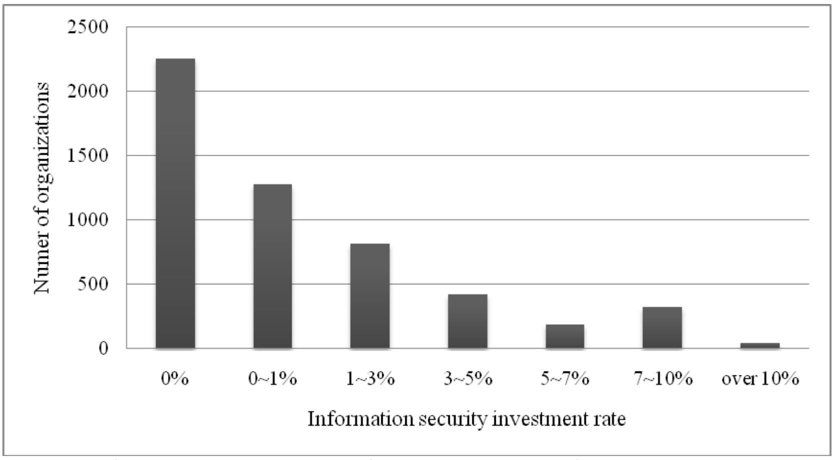

Fig 4. Number of organizations investing in information security by information security investment rate

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 using their closed LANs have their own intranet, but are not connected with outside organizations via dedicated connections.[11] We attribute these organizations to the group of low information security vulnerability. Organizations which use regional networks are connected with outside the organizations through dedicated networks, but their connections are restricted to selected employees. We classify such organizations in 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 the group with very high information security vulnerability level. Each category is coded as a 0-1 dummy variable and low vulnerability level is used as a default category.

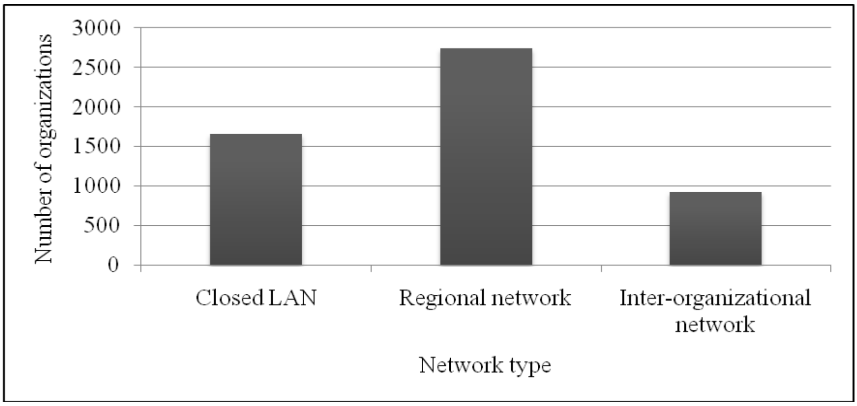

Fig 5. Number of organizations by network types

[11] As mentioned in the footnote 5, even firms using closed LANs might have Internet connections.

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 Tanaka et al., 2005). For example, a lack of IT resources in small organizations may be associated with under-invest 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 and over 300 employees. We assign 1 through 5 to each category, respectively (see figure 6).

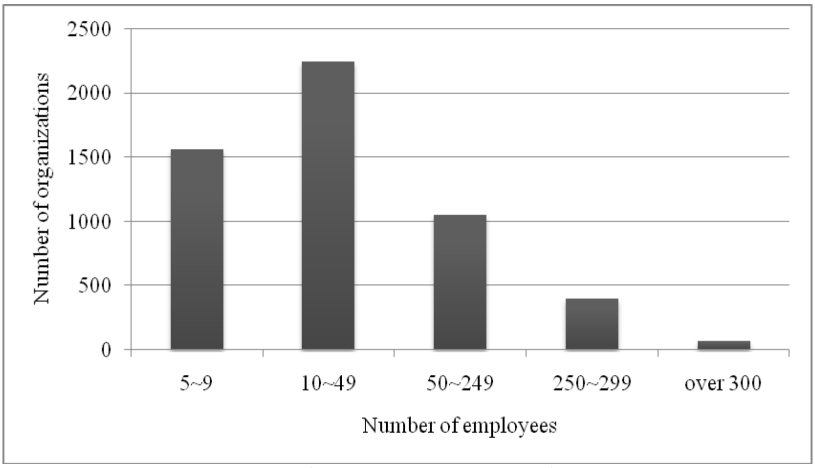

Fig 6. Number of organizations by number of employees

Second, we control for industry type in the regression analysis since industry-specific differences may influence the vulnerability and hence 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 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.

## 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 Greene (2003) and Long (1997), if the dependent variable shows these characteristics, the coefficient estimates of ordinary least squares regression are asymptotically biased and inconsistent. Therefore, we employ a negative binomial regression model with a maximum likelihood estimation developed by Hausman, Hall and Griliches (1984).[12] This model can be specified as:

[12] Under these characteristics of the dependent variable, Poisson or negative binomial models can be applied.

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

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, $P\left(\frac{k_i}{\varepsilon}\right)$ indicates the probability that firm *i* will make information security investment in *k*th category; $\mu_i$ 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 $\alpha^2$. 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 IV 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 and not collecting private 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 when firms do not collect customers' private information.[13]

Several interesting conclusions can be drawn from the results in Table IV. 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, information security investment rate, resulted by a one-unit change in the independent variable.[14] Therefore, the coefficient of the variable, 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, very high vulnerability is interpreted to mean that a change of vulnerability from the low level to the 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. Also, it can be identified 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

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.

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

[14] 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.

increase information security investment with a decreasing rate as the firms’ vulnerability level increases.

Table IV. 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***<br>(0.053) | 0.622***<br>(0.066) | 0.315***<br>(0.042) | 0.255***<br>(0.044) |
| Medium to high vulnerability | | 0.135**<br>(0.053) | | 0.179***<br>(0.031) |
| Very high vulnerability | | 0.231***<br>(0.057) | | 0.169***<br>(0.041) |
| Firm size | 0.111***<br>(0.016) | 0.098***<br>(0.016) | 0.175***<br>(0.013) | 0.154***<br>(0.014) |
| Agriculture, forestry & fisheries | 0.223***<br>(0.082) | 0.202**<br>(0.081) | 0.080<br>(0.082) | 0.059<br>(0.081) |
| Manufacturing | 0.016<br>(0.063) | 0.024<br>(0.063) | 0.167***<br>(0.042) | 0.141***<br>(0.042) |
| Construction | -0.095<br>(0.099) | -0.074<br>(0.098) | 0.035<br>(0.053) | 0.029<br>(0.053) |
| Wholesaling | -0.050<br>(0.068) | -0.036<br>(0.068) | 0.177***<br>(0.049) | 0.152***<br>(0.049) |
| Retailing | -0.105*<br>(0.059) | -0.114*<br>(0.059) | 0.038<br>(0.056) | 0.018<br>(0.056) |
| Restaurant & lodging | 0.007<br>(0.074) | 0.026<br>(0.074) | -0.084<br>(0.066) | -0.090<br>(0.066) |
| Logistics & telecommunications | -0.014<br>(0.066) | -0.019<br>(0.066) | 0.158***<br>(0.055) | 0.127**<br>(0.055) |
| Financial & insurance | 0.092**<br>(0.047) | 0.084*<br>(0.047) | 0.223***<br>(0.057) | 0.163***<br>(0.058) |
| Real estate, renting & business services | 0.001<br>(0.059) | -0.001<br>(0.059) | 0.189***<br>(0.047) | 0.172***<br>(0.047) |
| N | 1600 | 1600 | 2778 | 2778 |
| $\chi^2$ | 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

For Model 4 which includes firms not collecting private information, the results suggest the presence of similar propensities as those shown in the previous analysis: the coefficient of the variable, 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, it is identified 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. Also, we 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.

## 6. IMPLICATIONS AND LIMITATIONS

The research reported in this paper revealed evidence in support of the relationship between the vulnerability level and information security investment claimed at a conceptual level by Gordon and Loeb (2002) and Tanaka et al. (2005). Differently from the study of Tanaka et al. (2005) which assumed firms' security breach probability functions belong to Class II, this study separated the cases where firms' security breach probability functions belong to Class I or Class II based on their collection of private information. In addition, this study differs from Tanaka et al. (2005) by using a more direct measure for the dependent variable, the percentage of total information technology budgets on information security.

Our findings for firms working with the two different classes of information shed new light on issue of the level of investment in information security. The empirical results illustrated above suggested 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 invest in information security only at a moderate level (Gordon & Loeb, 2002).

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., Camp, 2005; Kunreuther & Heal, 2003; Ogut, Raghunathan, & Menon, 2004). Such considerations offer possible avenues for further research.

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.

## REFERENCE

Acquisti, A., Friedman, A., & Telang, R. (2006). *Is there a cost to privacy breaches? An event study*.

Ahn, N. (2010). Information Security Market Increases 10% to 800 Billion in 2009. *Maeil Business Newspaper*. Retrieved from http://news.mk.co.kr/v3/view.php?year=2010&no=112247

Anderson, J. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.

Anderson, R. (2001). *Why Information Security is Hard - An Economic Perspective.* Paper presented at the 17th Annual Conputer Security Applications Conference, New Orleans, LA.

Camp, L. J. (2005). The State of Economics of Information Security. *I/S A Journal of Law and Policy in the Information Society, 2*(2), 189-205.

Camp, L. J., & Wolfram, C. (2000). *Pricing security*. Paper presented at the The CERT Information Survivability Workshop, Boston.

Campbell, K., Gordon, L., Loeb, M., & 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.

Cohen, F. B. (1995). *Protection and security on the information superhighway*. New York: John Wiley & Sons, Inc.

Denning, D., & Denning, P. J. (1997). *Internet besieged: Countering cyberspace scofflaws*. Reading, MA: ACM Press.

Gordon, L., & Loeb, M. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security, 5*(4), 438–457.

Gordon, L., & Loeb, M. (2006a). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers, 8*(5), 335-337.

Gordon, L., & Loeb, M. (2006b). *Managing Cybersecurity Resources: A Cost-Benefit Analysis*. New York: McGraw-Hill.

Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2004). 2004 CSI/FBI Computer Crime and Security Survey. *Computer Security Journal, 20*(3), 33-51.

Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI Computer Crime and Security Survey*: Computer Security Institute.

Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2006). 2006 *CSI/FBI Computer Crime and Security Survey*: Computer Security Institute.

Greene, W. H. (2003). *Econometric analysis* (5th ed.). Upper Saddle River, NJ: Pearson Education Inc.

Hausman, J., Hall, B. H., & Griliches, Z. (1984). Econometric Models for Count Data with an Application to the Patents-R & D Relationship. *Econometrica, 52*(4), 909-938.

Hsiao, D. K., Kerr, D. S., & Madnick, S. E. (1979). *Computer security*. New York: Academic Press.

International Telecommunication Union. (2009). *Measuring the Information Society: The ICT Development Index*. Geneva, Switzerland: International Telecommunication Union (ITU).

Johnson, M., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, 16-24.

Korean Internet & Security Agency. (2007). *2007 Korean Information Security Survey*. Seoul, Korea: Korean Internet & Security Agency.

Korean Internet & Security Agency. (2008). *2008 Korean Information Security Survey*. Seoul, Korea: Korean Internet & Security Agency.

Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty, 26*(2), 231-249.

Long, S. (1997). *Regression models for categorical and limited dependent variables*. Thousand Oaks, CA: Sage Publications, Inc.

Majuca, R. P., Yurcik, W., & Kesan, J. (2006). *The evolution of cyberinsurance. In ACM Computing Research Repository (CoRR), Technical Report cs.CR/0601020*.

Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network intrusion detection. *IEEE network, 8*(3), 26-41.

Muntermann, J., & Roßnagel, H. (2009). On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market. *Identity and Privacy in the Internet Age,* 1-14.

Ogut, H., Raghunathan, S., & Menon, N. (2004). Self Protection and Insurance in IT security: The case of Interdependencies. The University of Texas at Dallas.

Parker, D. B. (1981). *Computer security management*. Reston, VA: Reston.

Parker, D. B. (1983). *Fighting computer crime*. New York: Scribner.

Richardson, R. (2007). *2007 CSI computer crime and security survey*: Computer Security Institute.

Richardson, R. (2008). *2008 CSI computer crime and security survey*: Computer Security Institute.

Statistics Korea. (2006). *Korean Census on Basic Characteristics of Establishments*. Daejon, Korea: Statistics Korea.

Straub Jr, D. (1990). Effective IS Security. *Information Systems Research, 1*(3), 255-276.

Straub Jr., D., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly, 14*(1), 45-60.

Straub Jr., D., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 441-469.

Tanaka, H., Matsuura, 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*(1), 37-59.

World Bank. (2010). *World Development Indicators 2010*. Washington, DC: World Bank.

Zhao, X., Xue, L., & Whinston, A. (2009). *Managing Interdependent Information Security Risks: An Investigation of Commercial Cyberinsurance and Risk Pooling Arrangement*. Paper presented at the Thirtieth International Conference on Information Systems.