How Can Organizations Improve Cybersecurity?
Implementing Security Controls in the Presence of Moral Hazard

Woohyun Shim[1], Johannes M. Bauer[2]

[1]Michigan State University, USA, shimwoo@msu.edu
[2]Michigan State University, USA, bauerj@msu.edu

Abstract

Many organizations are utilizing Internet technologies to be more efficient and productive. However, stronger dependence on the Internet has also increased their vulnerability to information security breaches and cyber attacks. Gains from the use of advanced information and communication technologies are offset by sometimes substantial losses due to cyber security incidents. Given the incomplete understanding of the characteristics of effective cybersecurity strategies and the challenges of creating proper organizational security incentives a considerable number of firms struggle with the design and implementation of effective security measures. This paper provides a conceptual and empirical analysis of the characteristics of effective security measures in the presence of moral hazard. We distinguish two types of attack strategies (targeted, untargeted) and discuss how problems of moral hazard (a misalignment of individual and organizational security incentives) might affect defense efforts. The empirical research uses detailed data from 2,401 organizations that participated in the Korea Internet & Security Agency's 2007 and 2008 information security surveys. Our findings confirm that technical security controls, while necessary, are not sufficient to achieve information security due to the presence of moral hazard. The data also suggest that raising security awareness and motivation, for example, by deploying a security training program, contributes to overcoming these moral hazard problems.

1. Introduction

Internet-based applications and services have become important sources of technological and organizational innovation. An increasing number of firms realized that these general purpose technologies are critical to increase efficiency and productivity. Consequently, firms are becoming ever-more dependent on Internet technologies. This dependency has also increased organizations' vulnerability to Internet-based fraudulent and criminal activity. Potential gains from Internet-based technological innovation have been partially offset by losses from cybersecurity incidents (Baker & Wallace, 2007). Although the magnitude of direct and indirect costs of information security breaches is not well known (Bauer, Van Eeten, Chattopadhyay, & Wu, 2008), there is an emerging consensus that steps need to be taken to control malicious activities (Moitra, 2005; OECD, 2009). Management in organizations across various sectors of the economy has started to consider information security as a critical activity. A broad range of technical solutions, ranging from simple anti-virus software to complex mathematical cryptographic technologies, is increasingly employed (Baker & Wallace, 2007; Bolot & Lelarge, 2008).

Although many technical security solutions have been developed and continue to be an important defense, sole reliance on technical fixes is neither effective nor adequate to protect organizations against cyber attacks. A number of studies (Anderson, 1994; Baker & Wallace, 2007; Besnard & Arief, 2004; Glisson & Welland, 2005) in economics, computer science, and telecommunications have shown that attackers and defenders are in a constant technology race. Possible intruders adapt to new security technologies and find new ways to circumvent them. In response, management has become more aware of the complexities of information security. In a growing number of organizations, information security concerns are addressed not only as a technical but also as an economic, managerial, and strategic problem (Gordon & Loeb, 2004; Kotulic & Clark, 2004; Kovacich & Halibozek, 2006).

Unfortunately, knowledge of these areas is relatively limited. Much of the available information is based on anecdotes, individual case studies, and survey data with limited generalizability (Moitra, 2005). Taking appropriate actions to protect information technology-supported business functions would be facilitated if more systematic data were available on which combinations of measures are capable of mitigating security breaches. This might help overcome the difficulties managers have experienced in identifying adequate measures to cope effectively with cybersecurity threats (Baker & Wallace, 2007).

Several authors (Anderson, 1994, 2001; Anderson & Moore, 2006; Anderson, Moore, Nagaraja, & Ozment, 2007; Varian, 2000) have also pointed out that many difficulties in the implementation of information security have arisen because of misaligned incentives between organizations. They demonstrated that, since it is difficult to identify which organizations are responsible for security breaches in many cases, organizations' incentives to invest in information security are often distorted. They also argued that, because of a characteristic of interdependency inherent in information security risk, the security investment decision by one organization affects those of other organizations. They therefore conclude that these characteristics of information security hinder the successful protection of information systems against cyber attacks and jeopardize entire system security.

Despite the extensive studies related to the problems of misaligned incentives and interdependent security risks among organizations, however, there has been little consideration of these problems within an organization. For example, because of the lack of appropriate liability regimes and incentives, poorly motivated employees in a firm may pay little attention to the proper configuration of information systems or to the maintenance of correct security procedures. Such behavior may be the outcome of the fact that individual employees may not suffer directly from damages caused by cyber incidents, and hence have little incentives to work hard for preventing security breaches. Such “moral hazard” may undermine cybersecurity and render the whole information system more vulnerable.

The study reported in this paper explores the experience of organizations with a broad range of measures adopted to enhance information security protection, and the actual effects of these measures on a firm’s level of security. This is done by assessing the effectiveness of cybersecurity measures on mitigating various forms of attacks (e.g., viruses/worms/Trojan horses, spyware, Denial of Service attacks, and hacking). This study also shed light on the possible presence of a moral hazard problem caused by misaligned liabilities and incentive in the provision of cybersecurity. We argue here that failure of effective implement of technical security measures is caused by misbehavior of poorly motivated employees (i.e., a moral hazard problem), and can be overcome by providing appropriate motivation through a training program. Therefore, this topic is tested by examining interaction effects between technical security measures and the existence of security training program. It should be noted that the ineffectiveness of technical security controls can be caused by diverse reasons.[1] However, one can infer that there may be moral hazard issues in implementing technical security solutions, if the technical solutions which are alone ineffective become effective by combining these with a security training program. The insights obtained from these analyses could help managers in shaping better security strategies.

Our empirical findings are based on survey data of 2,401 Korean firms obtained from the Korean Internet & Security Agency (KISA). While the major focus of the paper is the identification of effective technical security measures and the existence of moral hazard in cybersecurity, contextual factors, such as industry type and website type, are taken into account as control variables. We found that, similarly with the argument of the existing literature that dealt with a moral hazard problem between organizations, even within an organization, moral hazard caused by misaligned incentives and ill-defined liabilities can explain many of the challenges in implementing effective technical security measures. The empirical findings indicate that even if technical security solutions do not work as intended due to moral hazard issues, an increase in security awareness through a security training program can help firms overcome this problem, and a balanced emphasis on various security controls would reduce security breaches. These insights might be used to improve security decisions and investment in organizations’ information security.

[1] Technical security solutions might become ineffective, for example, because malicious software can mutate on their own in response to technical security measures, and malicious attackers can learn how to circumvent deployed security solutions.

The paper is organized as follows. Prior research is reviewed in the second section. Section three describes the study background illustrating the types of cyber threats and security controls that will be used throughout the paper. In the fourth section, we describe data and variables. In the fifth section, results of the empirical analysis will be presented. Implications and limitations of the study are discussed in the concluding segment.

2. Prior Research

Since Martine (1973) and Madnick (1978) discussed the links between computer-related risks and countermeasures, a vast amount of research has been published dealing with the protection of systems against information and computer security threats. Measures discussed in this literature range from technical threat detection, identification, mitigation, to forms of self-protection using managerial and organizational controls. In this section, we touch upon three areas of work that are closely related to this study: (a) traditional information system security (without much focus on the network), (b) the perspectives of computer science and telecommunications on network security, and (c) the economics of information security.

The literature on traditional information system security aimed at increasing our understanding of computer abuse[2] and at developing effective countermeasures. A large number of conceptual studies conducted by scholars, such as Parker (1981, 1983) and Hsaio et al. (1979) and Friedman (1988), have explored the effectiveness of security countermeasures in reducing the risk of computer abuse. For example, Parker (Parker, 1981, 1983) argued that guidelines, policy statements, tight security environment and the existence of security staff are effective measures of organizations aiming at lowering computer abuse. On the other hand, Hsaio et al. (1979) and Friedman (1988) argued in their conceptual works that security software and facilities help reduce the level of computer abuse. In addition, Straub Jr. (1990), Straub Jr. & Nance (1990) and Straub Jr. & Welke (1998) conducted empirical analysis using previous conceptual works indicating that security staff, security policies and guidelines, security awareness training, and security software are all effective countermeasures against computer abuse. However, these studies mostly consider incidents within an organization.

As the Internet developed and information systems became more connected, another research area emerged driven by researchers who were concerned with network security issues stemming from both inside and outside threats. A significant portion of the current studies in the

[2] According to Straub and Nance (Straub Jr. & Nance, 1990), computer abuse can be defined as "unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational information systems by individuals."

fields of computer science and telecommunications reflects these concerns focusing on issues such as the vulnerability of computer systems to cyber attacks, the detection of attacks, and preventative technologies (Cohen, 1995; Denning & Denning, 1997; Mukherjee, Heberlein, & Levitt, 1994). Contributors to this literature have discussed the detection and investigation of cyber attacks mostly from a technical point of view with only a secondary interest in managerial aspects.

Since the early 2000s, the economics of information security has emerged as a new research area, with pioneering contributions by authors such as Varian (2000), Anderson (2001), Camp & Wolfram (2000), and Gordon & Loeb (2002). This research has revealed many examples where security measures failed to deliver cybersecurity. A large part of this work 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 (Anderson, 2001; Camp, 2005; Gordon & Loeb, 2006a, 2006b). For example, Varian (2000) and Anderson (2001) were among the first to point out that moral hazard hinders successful deployment of security measures. They argued that moral hazard problems caused by misaligned incentives are one of the most critical reasons of security failures and should be taken into account in the study of information security. Anderson & Moore (2006) and Anderson (2007) subsequently argued that, even if there is more spending on information security, incidents cannot be avoided when misaligned incentives and moral hazard exist, as may be the case if the individuals and organizational units who are responsible for system security do not suffer directly from the losses of cyber attacks. Without proper liability assignment, they therefore concluded, moral hazard could jeopardize system security.[3] However, the existing literature has generally focused on a moral hazard problem among organizations rather than within an organization which is the focus of our study.

Despite certain limitation, contributions in these three research traditions have established a foundation for the investigation of information security. They form the basis for our analysis of the factors that affect the effectiveness of defenses against cyber threats and the additional problem of moral hazard.

[3] In addition, there have been several surveys of the impact of cyber incidents on business organizations (Department of Trade and Industry, 2002; Ernst & Young, 2007; Rankine, Rothery, Webster, & Wisniewski, 2003; Richardson, 2007). There was also a number of surveys which focus on specific cyber crimes such as virus attacks (Kaspersky Labs, 2006) or Internet fraud (Paget, 2009). These efforts have generated valuable data and descriptive analyses, such as frequency distributions of security incidents by dollar loss, offender motivation, and the victim industry.

3. Study Background and Research Questions

The increasing number, variety, and aggressiveness of cyber attacks can cause significant losses to organizations. These losses can stem from, but are not limited to, misuse of computers, infections with malicious software, attacks by outside hackers, or current or former employees defrauding an information system (Guttman & Roback, 1995). Schudel & Wood (2000), Bier & Abhichandani (2003) and Bier et al (2005) reason that organizations must consider the characteristics of cyber threats when selecting defensive security measures. Because of the vast number of different types of threats, we had to limit the range of cyber threats included in our empirical work. We hypothesized that two broad classes of attacks, targeted and untargeted attacks, would required different defense strategies. Therefore, we selected four different types of cyber threats based on their current and expected future prevalence and significance, and categorized them as targeted and untargeted attacks.[4]

An attack can be defined as *targeted* if it aims at damaging a specific information system or an organization's assets and reputation, such as for purposes of industrial espionage or pecuniary gains (Dzung, Naedele, Von Hoff, & Crevatin, 2005; Turk, 2005). Adversaries in such strategies typically gather information about the target and, therefore, know who will be attacked (Dzung, et al., 2005; Turk, 2005). Common types of targeted attacks include:

- Malicious hacking: intrusion into computer systems without authorization for a particular reason (Guttman & Roback, 1995).
- Denial of service (DoS): an attack that causes huge degradation of network resources and decreases the availability of the network (Moore, Shannon, Brown, Voelker, & Savage, 2006).[5]

In contrast, *untargeted* attacks intend to harm any vulnerable information system which can be discovered on a network (Dzung, et al., 2005; Turk, 2005). Examples of untargeted attacks are:

- Viruses, worms and trojan horses: malicious codes or software that manipulates legitimate uses to circumvent authentication and access systems (Turk, 2005)[6]

[4] Even if there are similarities, the definition of targeted and untargeted attacks is different from the definition of determined and opportunistic attacks used by Bier & Abhichandani (2003) and Bier et al (2005). In our study, the distinction between the two types of attacks is made by whether adversaries know who they will attack, whereas the distinction used in the works of Bier & Abhichandani (2003) and Bier et al. (2005) is made by whether the attacks are determined by the ease with which an attack can be carried out.

[5] DoS attacks can only be caused by outside adversaries whereas hacking can occur both by outsiders and by insiders.

- Spyware: programs that gather information illegally from legitimate users for a variety of purposes (Turk, 2005)

Since adversaries launching untargeted attacks may not care which systems they intrude but will assail any vulnerable system that can be found, they may be prevented by security measures that are proven to be difficult or costly to intrude. Defending against targeted attacks may be much more difficult and costly because perpetrators of targeted attacks may have great technical skills. Good defensive strategies, therefore, will have to be aligned with the types of attacks faced by organizations.

The conditions for designing effective security measures have changed over time. In the early Internet era, information security programs commonly depended on technical solutions. This strategy was rational at that time since most of the assets that required protection were also highly technical (Baker & Wallace, 2007). However, as the security environment and technologies have become more sophisticated and mature, and as intruders have developed entirely new attack vectors, technical measures alone are insufficient to protect organizations effectively. Rather, information security needs to involve social and organizational measures in addition to technical ones (Baker & Wallace, 2007; Dhillon & Backhouse, 2000). Given the increasing complexity of the problem, organizations need a map they can follow in their security practices. The National Institute of Standards and Technology (NIST), for example, has published a series of special publications, such as 'An Introduction to Computer Security: The NIST Handbook (1995)' and the 'Risk Management Guide for Information Technology Systems (2002)'. Similarly, the International Organization of Standardization (ISO) has published a 'Code of Practice for Information Security Management (ISO/IEC 17799, 2000)' that attempts to provide guidelines and principles for implementing an information security program. With an emphasis on the economic and organizational aspects, the OECD has issued Information Security Guidelines (OECD, 2002).

In this study, following the approach adopted in the NIST special publications, we categorize security measures into three types: management, technical and operational controls. Management controls are the techniques and concerns that concentrate mainly on the management of information system security and related risks. Security policy and user security guidelines are examples of management controls.[7] Technical controls include security products and services that are executed by the computer systems, such as firewalls, antivirus software, and other intrusion detection programs. Operational controls are enforcement mechanisms and

[6] Although infections of information systems with viruses, worms, and trojan horses are untargeted, once infected, machines might launch targeted attacks, for examples, as members of a botnet (Turk, 2005).

[7] The management controls are very similar to general deterrence theory in criminology. Deterrence theory studies deterrents and effects of these deterrents against committing criminal acts (Straub Jr., 1990). According to Madnick (Madnick, 1978), Martin (Martin, 1973), Parker (Parker, 1981, 1983) and Straub Jr. (Straub Jr., 1990), the examples of deterrents include guidelines for acceptable system use and policies for system use.

measures which often rely on technical expertise and both technical and management controls. Examples include physical access controls, employee training, and staffing of security-related functions.[8]

Organizations need to select and deploy proper security controls for their information systems to meet the security requirements of efficient operation (National Institute of Standards and Technology, 2005). A first question that therefore needs to be asked by managers and that we explore in this paper is:

> *RQ (1).* What, if any, are the most effective security controls for coping with different types of cyber threats?

Another question is related to the potential moral hazard problem as indicated in the previous sections. If a firm's security policy is afflicted with a moral hazard problem, the adopted security measures may not reduce system vulnerability to various cyber attacks; they may even increase it. In the presence of moral hazard, personnel in an organization will become less concerned about security, lulled by the belief that enough security measures are in place. A second research question explored in the paper is therefore:

> *RQ (2).* Is there a moral hazard problem that disturbs the proper functioning of employed security measures?

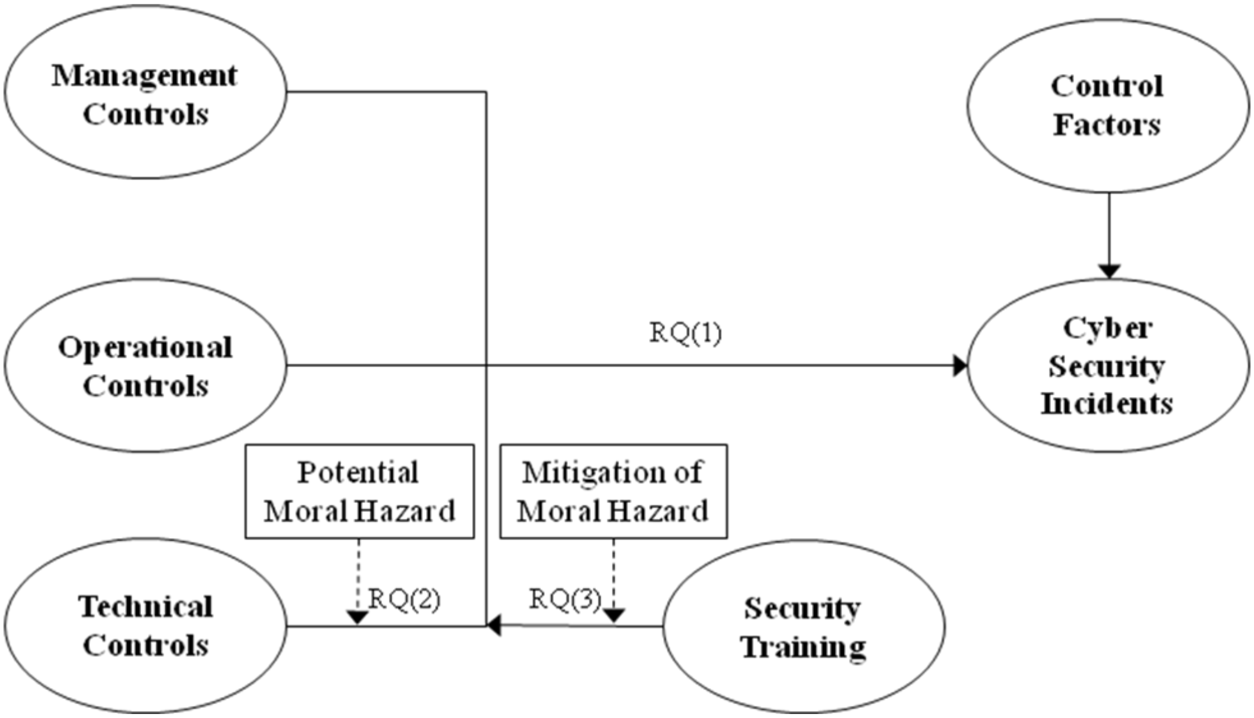
The moral hazard problem may be mitigated or overcome by providing a security training problem to raise personnel's awareness and motivation. This leads us to phrasing a third research question:

> *RQ (3).* Does raising security awareness and motivation mitigate the moral hazard problem?

In attempting to provide answers to these questions, the paper will also provide guidance for selecting and specifying security controls for information systems. The following figure depicts the conceptual framework that will be used in this study.

[8] In the field of criminology, the technical and operational controls are analogous to security countermeasures known as preventives. Examples of preventives include physical security of facilities and security software (Hsiao, et al., 1979; Straub Jr., 1990).

Figure 1: Conceptual Framework



4. Data and Variables

Data for this study was extracted from the 2007 and 2008 Korean Information Security Surveys published by the Korea Internet & Security Agency (2007, 2008). 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 (Statistics Korea, 2006). The 2007 survey was conducted using personal interviews and the 2008 survey combined internet-based and personal interview techniques for data collection. Survey respondents were the 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. The survey also included several questions related to information security management policies, employee training, as well as the number and magnitude of incidents. Over the period of two years, the surveys collected data on 5,336 organizations (2,508 in 2007 and 2,828 in 2008). In the case of businesses that did not use their own servers, the surveys collected less detailed information. Therefore, we only used information on the 2,401 organizations (894 in 2007 and 1,507 in 2008) for which in-depth information was available. 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 1 shows the variables and measures used.

Table 1: Dependent and Independent Variables

	Categories	Measures
Dependent variables	Cyber Incidents	• Number of hacking attacks • Number of DoS attacks • Number of virus/worm/trojan horse infections • Number of spyware infections
Independent variables	Management Controls	• Policy for information security • Guidelines for acceptable system use
	Technical Controls	• Number of technical security solutions • Use of authentication controls
	Operational Controls	• Physical Access Control • Security training • Organization employs Chief Information Officer • Organization employs Chief Security Officer
	Control Variables	• Company size • Industry type (10 industries were distinguished) • Website type (4 types were distinguished) • Outsourcing of Information Security
	Interaction Effects	• Security training * Number of technical security solutions • Security training * Use of authentication controls

The impacts of cybercrime are multi-faceted ranging from damages to systems, loss of data, reductions of productivity, to direct and indirect financial and/or technical damage. Selecting proper dependent variables is therefore not straightforward. To overcome this challenge, we generated a scale for the seriousness of an incident, that is, a measure of the degree of victimization. We use the number of incidents caused by four different types of cyber attacks (i.e., malicious hacking, DoS, viruses/worms/trojan horses, and spyware) as dependent variables. Two aspects of the surveys need to be noted: First, they counted incidents only when they caused actual damages or losses. Therefore, incidents which did not result in damages or losses are not included in the survey. Second, the survey categorized the number of the incidents into five categories (labeled 0-5) using the following boundaries: 0, 1, 2~3, 4~5, 6~9 and over 10 incidents.

Independent variables were categorized into three groups, following the classification suggested by NIST (National Institute of Standards and Technology, 1995, 2002, 2005). If these controls are effective, organizations using them would suffer fewer cyber incidents. From the broad range of security measures described by NIST, we could only use those focusing on deterrence and prevention (rather than recovery), since the KISA surveys did not include items related to recovery measures.

In the empirical model, management controls are measured by two items: (1) whether or not the organization uses a formal information security policy, and (2) whether it uses formal guidelines for acceptable system use. These two items are coded as 0-1 dummy variables.

Technical controls are comprised of several items. As described above, technical controls are related to the investment in products and processes designed to lower vulnerabilities. Their importance in an organization is captured in three dimensions: security solutions, network controls, and system access controls. As a proxy for these components, we use the number of specialized technical security solutions that are in use. The following measures are accounted for: firewalls, intrusion detection system (IDS), use of virtual private networks (VPN), intrusion prevention system (IPS), secure OS, enterprise security management (ESM), anti-virus software, smartcards, biometrics, network access controls (NAC), and web-firewalls.[9] In addition, the use of authentication controls is also included as a dummy variable, indicating whether or not organizations use specific network and system login methods (i.e., passwords, tokens, smartcards, and biometrics).

Four items, each constructed as a 0-1 dummy variable, were used as operational controls: whether an organization relies on physical access controls, the existence of formal employee training programs, the employment of a chief information officer (CIO), and the employment of a chief security officer (CSO). Physical access control is an enforcement mechanism that focuses mainly on the protection of the physical components of the information systems. It is operationalized as a dummy variable that takes on the value of 1 if an organization has a designated secured area for its information system that uses authentication such as a smartcard and biometrics. Reliance on formal employee training programs is coded as 1 if there is a formal employee training program and zero otherwise. Likewise, the employment of designated senior managers is coded using dichotomous dummies. The presence of the positions of CIO and CSO could indicate a stronger security orientation.

To explore whether raising security awareness can mitigate potential moral hazard problems in the use of technical security controls, we introduce selected interaction terms. If moral hazard is a problem, the presence of technical security measures alone is not sufficient. Although the language of moral hazard is not used, NIST special publication (2005) and Peltier (2005) argue along these same lines stating that for technical security measures to be effective complementary security training programs are needed to raise the awareness and motivation of personnel. However, it is difficult or even impossible to align an incentive to a specific individual in an organization because cybersecurity is interdependent and it may not be possible to identify who was responsible for a security breach. In this case, implementation of security training programs that raise personnel's awareness might be the appropriate choice to reduce moral hazard

[9] Some of these security solutions are not directly but only indirectly relevant in the prevention of cyber incidents.

problems. We test whether our data allow such a conclusion by using interaction terms between security training and the number of technical security solutions, and between security training and the use of authentication controls. If security training programs lower the possibility of improper maintenance of information systems and thereby mitigate moral hazard problems the coefficient of these interaction terms should be negative.

Cybersecurity incidents may also be influenced by other factors, such as firm size, industry type, website type, and whether or not information security protection is outsourced. We take these differences into account in the form of four control variables. Firm size is measured by the number of employees. This variable is included because of empirical evidence on the positive relationship between the size of businesses and the level and quality of security control implementation as identified by Baker & Wallace (2007). The KISA surveys categorize firms into four categories: 5~9 employees, 10~49 employees, 50~249 employees, and over 250 employees. We assigned 1 through 4 to each category, respectively. Industry type is included to control for industry-specific differences that may affect the occurrence of cyber incidences. The surveys group organizations 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 created nine dummy variables indicating the industry type of the organization using "other services" as the default category (this convention does not influence the outcomes). Website type is a measure that indicates whether an organization host its website on its own server, on its headquarters' server, or using a hosting service. These options were captured by three dummy variables (website on its own server, website on its headquarters' server, and website using a hosting service) and used "no website" as the default category. The potential effect of security outsourcing was addressed by including a dummy variable.

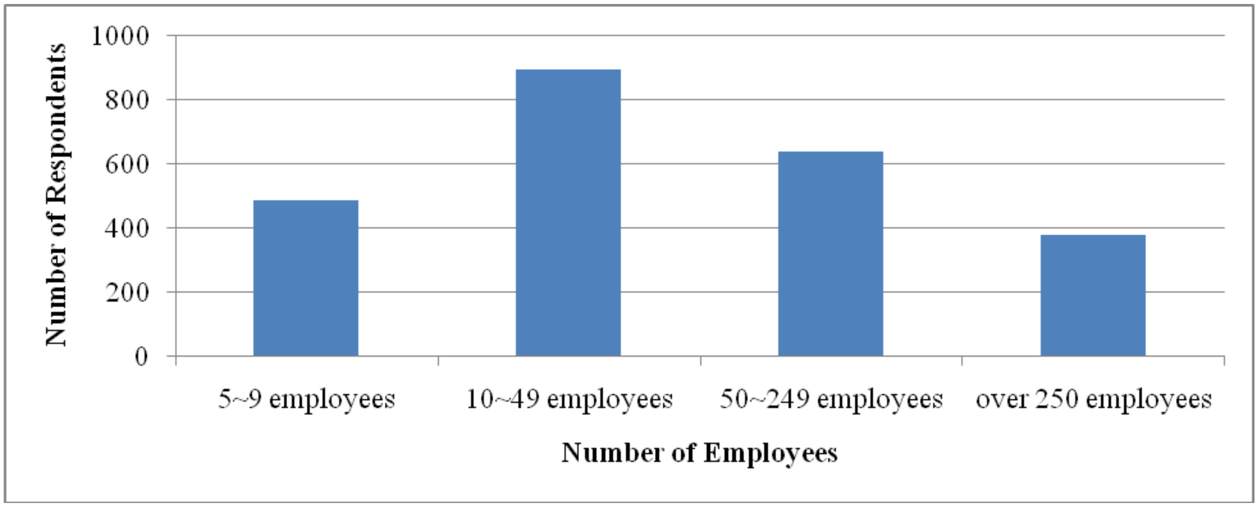
5. Empirical Analysis

Parameters for the empirical model discussed in section 3 were estimated using multivariate regression. Before details from the regression analysis will be discussed, it is useful to briefly review the characteristics of the sample. Table 2 and Figure 2 show a breakdown of the sample by industry type and size. Table 2, reporting the percentage of firms without security incidents during the reporting period suggests that the financial and insurance industry implements stronger or more effective security measures, and hence suffers less from cyber attacks (see Figure A in the appendix for more detail). Figure 2 reports the number of firms in the four size categories. Small and medium-sized businesses with less than 50 employees comprise about 71 percent of the total number of firms in the sample.

Table 2: Industry Subsamples and Security Record

Industrial Type	N	Percentage with No Security Incidents
Agriculture, Forestry & Fisheries	68	52.9%
Manufacturing	378	42.6%
Construction	134	45.5%
Wholesaling	211	44.1%
Retailing	212	46.7%
Restaurant & Lodging	106	44.3%
Logistics & Telecommunications	185	53.5%
Financial and Insurance	363	70.0%
Real estate, Renting & Business Activities	313	44.7%
Other Services	431	54.5%

Figure 2: Respondent Firm Size Characteristics



Many of the independent variables are operationalized as dichotomous variables. Although this is a common modeling approach, it is well known that models with many dummy variables as explanatory variables often result in peculiar overall test statistics, in particular a low R-square (a statistic measuring the amount of variance explained by the regression). This effect is also visible in our findings. However, due to the large sample size, the explanatory variables remain reliable predictors of the dependent variable. Table 3 displays the coefficient estimates for the four different types of cyber incidents.[10] Bold numbers indicate statistically significant variables. Each model was significant at the .01 level overall. The regression models use interaction terms

[10] Baseline models which only include control variables are contained in the appendix.

which may cause multicollinearity problems. As suggested by Yu(2000), we orthogonalized these terms to avoid problems associated with multicollinearity.[11,12]

R-square values for the models range from 0.028 to 0.072.[13] In addition to the use of dummy variables, there are several possible explanations. R-square values are normally lower for cross-section data than for time series data. The use of various qualitative and binary variables with limited variability is an additional constraining factor. Whereas our paper was constrained by the available data, this suggests that the three groups of security measures only have limited effects on the overall level of security. Moreover, it suggests that other factors need to be included in future research. Whereas low R-square values reflect that the models might be incomplete, their explanatory power needs to be evaluated by the statistical significance of the individual independent variables, rather than the overall R-square values, as explained by Christie (1990). Significance of many parameter estimates at the 0.01 level and the large sample size (n=2,401) imply that the findings reflect a good estimate of the ceteris paribus effect of variations in the predictors on the number of cyber incidents (Wooldridge, 2008).

Several conclusions can be drawn from the results presented in Table 3. Some security controls turn out to be effective for all types of attacks whereas others are only effective for either targeted or untargeted types of attacks. In the category of management security controls, only the coefficients of the guidelines for acceptable system use for untargeted attacks have the predicted signs and statistical significance. The coefficients suggest that an organization’s likelihood of security breaches caused by untargeted attacks is reduced if an organization implements guidelines for acceptable system use. However, in our data set, such guidelines do not have a statistically significant mitigating effect in the case of targeted attacks (although the coefficient has a negative sign as theory would predict). Having policies for information security does not show a statistically significant mitigating effect for any type of cyber attack.

[11] Orthogonalization is a widely used method when the product of two variables (say $X_1 X_2$), which might be strongly correlated with either X_1 or X_2, is used in regression analysis. An orthogonalization method can create a new variable which is conceptually equivalent to $X_1 X_2$, but not closely correlated to X_1 and X_2 (Yu, 2000).

[12] A test statistic, the variance inflation factor (VIF), ranges from 1.03 to 4.49, which indicates that multicollinearity is not a problem.

[13] Compared to the R-square values of the baseline models displayed in Table B in the appendix, we get higher R-square values which indicate better explanatory power.

Table 3: Results of Regression Analyses

	Variable	Untargeted Attacks		Targeted Attacks	
		(1)Virus /worm /trojan horse	(2)Spyware	(3)Hacking	(4)DoS
Management Controls	Policy for information security	-0.016	0.140	0.004	0.008
	Guideline for acceptable system use	-0.199***	-0.360***	-0.004	-0.011
Technical Controls	Number of security solutions	0.017*	0.029**	0.012**	0.010*
	Use of authentication controls	0.232**	0.208**	0.124**	0.125**
Operational Controls	Physical access control	-0.094	-0.071	-0.046	-0.023
	Security training	-0.219***	-0.307***	-0.065*	-0.068*
	Chief Information Officer	-0.046	0.099	0.020	0.071**
	Chief Security Officer	0.063	0.104	0.019	0.045
Interaction Effects	# of security solutions * Security training	-0.044**	-0.051**	-0.023**	-0.032***
	Use of authentication controls*Security training	-0.421*	-0.698***	-0.065	0.016
Control Variables	Company size	0.058**	0.089***	-0.016	0.004
	Agriculture, forestry and fisheries	0.197	0.136	0.120	0.108
	Manufacturing	0.173**	0.366***	0.084*	0.055
	Construction	0.220*	0.352**	0.216**	0.084
	Wholesaling	0.095	0.116	0.082	0.029
	Retailing	0.235**	0.244**	0.093	0.058
	Restaurant & lodging	0.154	0.168	0.222**	0.124
	Logistics & telecommunications	-0.007	0.157	0.109*	0.105*
	Financial & insurance	-0.215**	-0.170	-0.008	-0.035
	Real Estate, renting & business activities	0.153*	0.306***	0.203**	0.104**
	Website operated by headquarters	0.052	0.105	0.076*	0.078*
	Website using web hosting services	0.332***	0.452***	0.115**	0.072
	Website operated by own web-server	0.169**	0.262***	0.155**	0.153***
	Outsourcing of Information security	0.146**	0.097	0.050	0.066
R-Square		0.060	0.072	0.028	0.028
F (p value)		6.26(.0001)	7.68(.0001)	2.84(.0001	2.80(.0001)

Note: Significance levels are as follows: * p<.1, **p < .05 and ***p < .01

The most striking results are revealed in the category of technical security controls. The coefficients of both the number of security solutions and the use of authentication controls reveal positive and statistically significant signs (although at different levels). This can be interpreted as a strong hint that technical security controls alone are not effective. In line with NIST (2005), the signs and statistical significance of the coefficients can be seen as evidence that technical security solutions only work as minimum security controls that need complementary measures and actions to become effective. In other words, the use of technical security controls is not a sufficient condition to achieve information security but only a necessary one. The positive coefficients suggest that technical security controls even go hand in hand with an increased number of cyber incidents. Paradoxically, an organization with more technical security measures is more likely to have more cyber incidents. This implies that there is a moral hazard problem in implementing security controls effectively. Poorly motivated IT personnel may configure technical security solutions incorrectly or do not perform proper maintenance for the solutions (e.g., patches and updates). Under such moral hazard conditions, more cyber incidents would occur despite the technical security measures that are in place.

In the case of operational security controls, the coefficients of security training show the expected negative signs and are statistical significant for all four types of attacks. At least in our data set, security training turns out to be an effective security measure. However, the other independent variables, including the use of physical access controls and the presence of CIOs or CSOs, do not show statistical significance or the signs predicted by theory: none of the coefficients of the CSO variable displayed statistically significant or the expected negative signs; for the CIO variable, only the coefficient in the model with the number of DoS attacks shows statistical significance although not the expected negative sign.

An interesting picture emerges from the interaction effects. The combined presence of security training and a higher number of security solutions is highly significant across all types of cyber attacks and mitigates their number. In contrast, the coefficients of the combined presence of authentication controls and security training only has the expected effect in the case of untargeted attacks but is not statistically significant in the case of targeted attacks. Thus, although various technical security controls alone cannot lower the success rate of cyber attacks, technical security controls together with security training may be a sufficient condition to achieve this goal. At the same time, the effect of security training may be to reduce or even eliminate moral hazard problems.

With respect to the control variables, the coefficients of organization size show statistically significant and positive relationships for untargeted attacks. This could imply that efficient implementation of security controls becomes more difficult in larger organizations. The signs of the coefficients of the dummy variables for the industry types indicate whether organizations in a specific industry are more likely or less likely to experience cyber incidents than the default group (i.e., the ‘other services’ industry). For example, the statistically significant negative sign of the financial and insurance industry for the number of virus/worm/trojan horse infections suggests organizations in this industry have the lowest number of virus/worm/trojan horse infections. The magnitude of the coefficients reveals whether organizations in a specific industry are more likely or less likely to experience cyber incidents than other industries. For instance, the magnitude of the coefficients of ‘manufacturing’, ‘construction’, ‘retailing’ and ‘real estate, renting & business activities’ indicates that organizations in the manufacturing industry are the most likely to have spyware infections. Organizations in construction and real estate are next, followed by renting & business activities. Firms in the retailing industry are the least likely to experience spyware infections.

Regarding the operation of an organization's website, websites operated by web hosting services are the more likely to experience untargeted cyber attacks, followed by websites operated by the organizations' own web-servers. For targeted attacks, except for 'website operated by web hosting services' in the model with the number of DoS attacks as dependent variable, all coefficients display statistically significant and positive relationships with the number of targeted attacks. It is also visible that, in most cases, organizations with their own website are more likely to have cyber attacks than organizations without a website.

Lastly, only the coefficients of outsourcing of information security in the model of the number of virus/worm/trojan horse infections show a positive and statistical significant relationship. Outsourcing information security seems to make an organization more vulnerable to virus/worm/trojan horse infections.

6. Implications and Limitations

Our purpose in this research has been to investigate the potential effect of various information security measures and to explore whether there is empirical evidence of the existence of a moral hazard problem. The paper extends previous research on cybersecurity, which has often been limited to conceptual studies, by using organizational-level data obtained from the Korean Internet & Security Agency for 2007 and 2008. The paper also attempts to illustrate that a more refined conceptualization can provide better insights into understanding the effective measures for cybersecurity. Although we find that the logic used by previous studies for computer abuse (e.g., Hsiao et al. (1979) and Straub Jr. (1990)) can be adapted to explore cybersecurity concerns, earlier findings should be treated cautiously since cybersecurity involves more complex stakeholder and environmental relationships.

The empirical results of our study reveal several potentially significant implications in understanding the effective implementation of security measures. First, we identified that various variables do not show statistical significance (and in this sense can be deemed ineffective) or even display statistically significant positive relationships with the number of cyber incidents (possibly because of the presence of moral hazard problems). Even if organizations employ various security controls, strong cybersecurity cannot be achieved without addressing the moral hazard problem.

Second, our data indicate that security training is critical for mitigating all types of cyber threats and even reducing moral hazard problems. The statistically significant and negative coefficients of security training in all models indicate the effectiveness of security training programs in decreasing cyber threats. This finding echoes a report published by Symantec (2008) indicating that investments in employee training and development are among the most effective paths to improve security. Implementing security programs can also serve as remedy for organizations which experience a lack of effectiveness of various technical security measures. For example, given the rapid development of intrusion technologies, many technical solutions may become less effective without regular updates or patches, proper configuration and adequate maintenance. Similarly, if an organization's personnel are poorly motivated to protect information security, information security will suffer. Therefore, together with investing in various baseline technical security measures, organizations should try to overcome the moral hazard problem by deploying security training programs which will raise personnel's security awareness and motivation to protecting information systems.

Third, this paper also identified that guidelines for acceptable system use contribute to effective defenses in the case of untargeted cyber attacks. Compared to an overall policy for information security, which typically provides only general and rather abstract principles of information security, guidelines that give direct tips and rules for system use and that raise awareness of safe use of the system, are a more effective measure of cybersecurity, at least for untargeted attacks. Therefore, organizations that experience a larger number of untargeted attacks might benefit from introducing guidelines for acceptable system use as a security measure.

Fourth, we also found that there are fundamental differences between targeted attacks and untargeted attacks. In detail, the magnitudes and statistical significance of the coefficients of the variables, such as guidelines for acceptable system use, security training, and interaction terms, indicate that the ceteris paribus effect of the variables on reducing untargeted attacks is higher than their effect on reducing targeted attacks. Also, the comparison of R-square values between untargeted and targeted attacks reveals that there are more factors affecting the occurrence of targeted attacks which are not taken into account in our model specifications. Therefore, together with Figure A and Table A in the appendix, it can be interpreted that, although the frequency of targeted attacks is much less than the frequency of untargeted attacks, the actual defense against targeted attacks is more difficult than the defense against untargeted attacks.

These findings suggest that an organization's cybersecurity cannot be achieved solely by investment in technical security measures. Rather, the most effective way for enhancing cybersecurity is to increase awareness and motivation of an organization's personnel by providing appropriate guidelines and security training programs. This is in line with results that one would expect from applying principal–agent theory to problems of the effective implementation of information security in organizations.

In spite of interesting findings, however, there are some limitations in this study. As Baker & Wallace (2007) pointed out, a study which deals with the complexity of control implementation would give a clearer insight for the information security management. Because of the lack of detailed data, however, this study measures implementation in quantitative terms, mostly based on binary variables, rather than implementation quality. Therefore, similarly with other studies such as Straub Jr. (1990) and Hsiao et al. (1979), the effects of implementation quality could not be examined in our study design. While this study goes further than previous work on cybersecurity in its specific focus on different types of security controls and cyber attacks, as shown by the low R-square values, the development of more micro-analytic quantitative data would clearly be a useful undertaking for future study.

Lastly, 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. It would be highly desirable and assist research on the factors enhancing information security in organizations to have a more standardized and more detailed information basis available across nations.

Appendix

Figure A. Relative Frequencies of Untargeted and Targeted Attacks

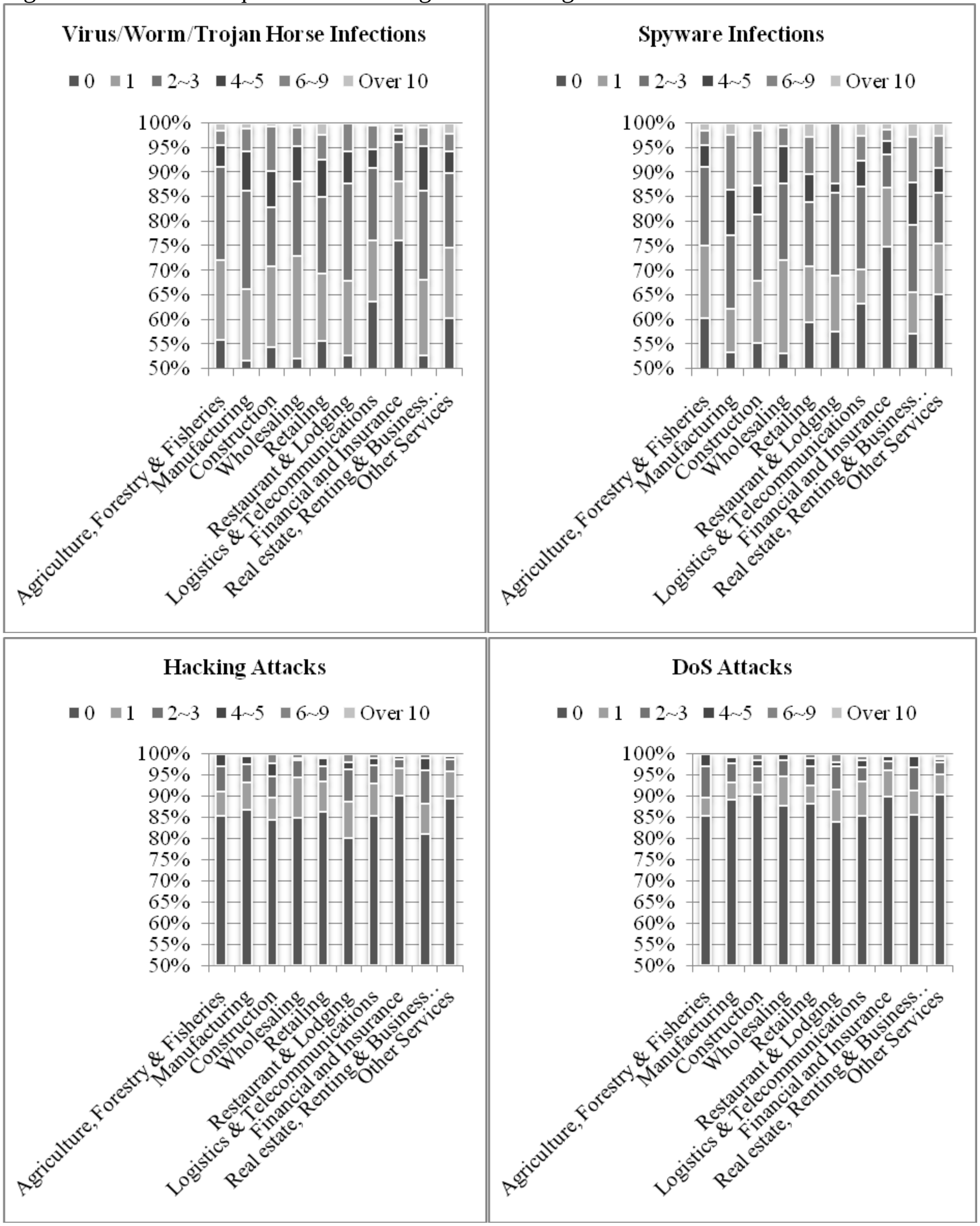


Table A. Simple Statistics

Variable	Mean	S.D.
Virus/worm/trojan horse	0.85631	1.23279
Spyware	0.93503	1.39551
Hacking	0.23948	0.68717
DoS	0.21824	0.69691
Policy for information security	0.55519	0.49705
Guideline for acceptable system use	0.62849	0.48331
Number of security solutions	2.75552	2.92856
Use of authentication control	0.92003	0.27130
Email usage control	0.94169	0.23438
Physical access control	0.30321	0.45974
Security training	0.29488	0.45608
Chief Information Officer	0.26031	0.43889
Chief Security Officer	0.25448	0.43566
Company size	2.40691	1.03792
Agriculture, forestry and fisheries	0.02832	0.16592
Manufacturing	0.15743	0.36429
Construction	0.05581	0.22960
Wholesaling	0.08788	0.28318
Retailing	0.08830	0.28378
Restaurant & lodging	0.04415	0.20547
Logistics & telecommunications	0.07705	0.26673
Financial & insurance	0.15119	0.35831
Real Estate, renting & business activities	0.13036	0.33677
Website operated by headquarters	0.32153	0.46716
Website operated by web hosting services	0.20367	0.40281
Website operated by own web-server	0.28405	0.45105
Outsourcing of Information security	0.15244	0.35952

Table B. Results of Regression Analysis using Control Variables Only

Variable	Untargeted Attack		Targeted Attack	
	(1) Virus/worm /trojan horse	(2) Spyware	(3) Hacking	(4) DoS
Company size	0.034	0.074**	-0.014	0.010
Agriculture, forestry and fisheries	0.186	0.142	0.133	0.129
Manufacturing	0.215**	0.407***	0.091*	0.055
Construction	0.261**	0.377***	0.218***	0.079
Wholesaling	0.142	0.166	0.089	0.032
Retailing	0.259**	0.278**	0.106*	0.072
Restaurant & lodging	0.189	0.214	0.231***	0.133*
Logistics & telecommunications	-0.002	0.169	0.111*	0.105*
Financial & insurance	-0.281***	-0.185*	0.003	-0.011
Real Estate, renting & business activities	0.194**	0.345***	0.206***	0.104**
Website operated by headquarters	-0.042	0.046	0.088**	0.107**
Website operated by web hosting services	0.309***	0.456***	0.130***	0.099**
Website operated by own web-server	0.119	0.267***	0.182***	0.204***
Outsourcing of Information security	0.123	0.091	0.059	0.080**
R-Square	0.040	0.047	0.020	0.016
F (p value)	7.07(.0001)	8.36(.0001)	3.39(.0001)	2.78(.0004)

Note: Significance levels are as follows: * p<.1, **p < .05 and ***p < .01

Acknowledgements

The authors 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

Anderson, R. (1994). Why cryptosystems fail. *Communications of the ACM, 37*(11), 32-40.

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

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610-613.

Anderson, R., Moore, T., Nagaraja, S., & Ozment, A. (2007). Incentives and information security. In N. Nisan, T. Roughgarden, E. Tardos & V. Vazirani (Eds.), *Algorithmic Game Theory*: Cambridge University Press.

Baker, W. H., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *IEEE Security & Privacy,* 36-44.

Bauer, J., Van Eeten, M., Chattopadhyay, T., & Wu, Y. (2008). *ITU Study on the Financial Implication of Network Security: Malware and Spam*. Geneva, Switzerland: International Telecommunication Union (ITU).

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security, 23*(3), 253-264.

Bier, V. M., & Abhichandani, V. (2003). Optimal allocation of resources for defense of simple series and parallel systems from determined adversaries *Risk-Based Decision Making in Water Resources* (pp. 59-76). Reston, VA: American Society of Civil Engineers.

Bier, V. M., Nagaraj, A., & Abhichandani, V. (2005). Protection of simple series and parallel systems with components of different values. *Reliability Engineering and System Safety, 87*(3), 315-323.

Bolot, J., & Lelarge, M. (2008). Cyber Insurance as an Incentive for Internet Security. In E. Johnson (Ed.), *Managing Information Risk and the Economics of Security* (pp. 269-290): Springer.

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.

Christie, A. A. (1990). Aggregation of test statistics: An evaluation of the evidence on contracting and size hypotheses. *Journal of Accounting and Economics, 12*(1-3), 15-36.

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.

Department of Trade and Industry. (2002). Information Security Breaches Survey. London: Department of Trade and Industry (DTI).

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.

Dzung, D., Naedele, M., Von Hoff, T., & Crevatin, M. (2005). Security for industrial communication systems. *Proceedings of the IEEE, 93*(6), 1152-1177.

Ernst & Young. (2007). *Global Information Security Survey 2006*.

Friedman, M. (1988). Access-control software. *Information Age, 10*(3), 157-161.

Glisson, W. B., & Welland, R. (2005). *Web development evolution: the assimilation of web engineering security*. Paper presented at the 3rd Latin American Web Congress.

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

Gordon, L., & Loeb, M. (2004). The economic of information security investment. In L. Camp & S. Lewis (Eds.), *Economics of Information Security* (pp. 105-127). Boston: Kluwer Academic Publishers.

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.

Guttman, B., & Roback, E. (1995). *An introduction to computer security: The NIST Handbook*: National Institute of Standards and Technology.

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

ISO/IEC 17799. (2000). *Information Technology - Code of Practice for Information Security Management*. Switzerland: International Organization for Standardization (ISO).

Kaspersky Labs. (2006). *Malware Evolution 2006: Executive Summary*.

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.

Kotulic, A., & Clark, J. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

Kovacich, G., & Halibozek, E. (2006). *Security Metrics Management. How to Manage the Cost of an Asset Protection Program*. New York: Elsevier.

Madnick, S. (1978). Management policies and procedures needed for effective computer security. *SLOAN MANAGEMENT REVIEW, 20*(1), 61.

Martin, J. (1973). *Security, accuracy, and privacy in computer systems*. Englewood Cliffs, NJ: Prentice-Hall.

Moitra, S. (2005). Developing Policies for Cybercrime. *EUROPEAN JOURNAL OF CRIME CRIMINAL LAW AND CRIMINAL JUSTICE, 13*(3), 435.

Moore, D., Shannon, C., Brown, D., Voelker, G., & Savage, S. (2006). Inferring Internet denial-of-service activity. *ACM Transactions on Computer Systems (TOCS), 24*(2), 115-139.

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

National Institute of Standards and Technology. (1995). *An introduction to computer security: The NIST Handbook*: National Institute of Standards and Technology (NIST).

National Institute of Standards and Technology. (2002). *Risk management guide for information technology systems*: National Institute of Standards and Technology (NIST).

National Institute of Standards and Technology. (2005). *Recommended security controls for federal information systems*: National Institute of Standards and Technology (NIST).

OECD. (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* Paris, France: Organization for Economic Co-operations and Development.

OECD. (2009). *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy* Paris, France: Organisation for Economic Co-operation and Development.

Paget, F. (Cartographer). (2009). *Financial Fraud and Internet Banking: Threats and Countermeasures*.

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

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

Peltier, T. (2005). Implementing an information security awareness program. *Information Systems Security*, *14*(2), 37-49.

Rankine, T., Rothery, M., Webster, K., & Wisniewski, T. (2003). Australian Computer Crime and Security Survey: AusCERT.

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

Schudel, G., & Wood, B. (2000). *Modeling behavior of the cyber-terrorist.* Paper presented at the Countering Cyberterrorism Workshop, Marina del Rey, CA.

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

Straub Jr., D. W. (1990). Effective IS Security. *INFORMATION SYSTEMS RESEARCH, 1*(3), 255-276.

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

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

Symantec. (2008). *IT Risk Management Report 2: Myths and Realities*. Cupertino, CA: Symantec Corporation.

Turk, R. J. (2005). *Cyber incidents involving control systems*: Idaho National Engineering and Environmental Laboratory.

Varian, H. (2000). Managing Online Security Risks. *The New York Times*. Retrieved from http://www.nytimes.com/library/financial/columns/060100econ-scene.html

Wooldridge, J. (2008). *Introductory econometrics: A modern approach*. Madison, OH: South-Western Cengage Learning.

Yu, C. H. (2000). *An overview of remedial tools for collinearity in SAS.* Paper presented at the 2000 Western Users of SAS Software Conference, Tempe, AZ.