보안책임과 규제가 기업의 보안활동에 미치는 영향 분석

Analysis of the Impact of Security Liability and Compliance on a Firm's Information Security Activities

심우현(Woohyun Shim)*

초 록

각종 정보보안 관련 사고의 증가에 따라, 세계 각국에서는 지속가능한 정보보호를 위한 다양한 보안책임 및 규제에 관한 법률들을 발전시켜왔다. 본 연구에서는 이러한 정책의 실효성을 분석하기 위하여 2007년 제정된 전자금융거래법이 기업의 정보보안 활동에 미치는 영향에 대한 실증적인 분석을 실시하였다. 연구 결과에 따르면, 전자금융거래법의 실효성에 대한 다양한 비판에도 불구하고, 이러한 법률의 제정이 기업의 정보보안 활동의 증가에 긍정적인 영향을 미치는 것으로 나타났다. 즉, 본 연구는 정보보호를 위한 보안책임 및 규제에 관한 법률이 정보보안의 지속적인 발전에 공헌한다는 것을 밝혀냈다.

ABSTRACT

Many governments have tried to develop a liability and compliance law that can improve cyber security in a sustainable way. This paper explores whether a liability and compliance law is effective in motivating firms' information security activities. In particular, I empirically investigate the impact of the 2007 Electronic Financial Transaction Act (EFTA), a liability and compliance law in Korea, on the information security activities of financial institutions and services providers. In spite of various criticisms of the effectiveness of EFTA, the empirical findings of this study clearly show that EFTA is having a positive impact on information security activities. From these findings, this article concludes that a liability and compliance law is likely to contribute to a certain degree to the achievement of sustainable development of cyber security.

키워드 : 전자금융거래법, 정보보호, 보안투자, 금융 및 보험산업, 보안책임, 보안규제
Electronic Financial Transaction Act (EFTA), Cyber-Security, Information Security Investment, Financial and Insurance Industry, Liability, Compliance

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

* Senior Researcher, Synthesys, Inc., East Lansing, MI 48823, USA

2011년 10월 17일 접수, 2011년 10월 26일 심사완료 후 2011년 11월 11일 게재확정.

1. Introduction

Dramatically increased cyber-attacks led by highly organized cyber perpetrators have resulted in a need for more effective and sustainable security measures and strategies to respond effectively to these attacks. Accordingly, in order to achieve sustainable development of cyber-security, many developed and developing countries have enacted cyber security laws which enforce compliance with higher security standards in certain information technology (IT) related activities [17]. For example, in the U. S., the Gramm-Leach-Bliley Act's security regulation and the HIPAA security regulation, which require certain types of firms such as financial institutions to employ sustainable security management standards, were issued in 2001 and 2003, respectively [17]. In addition, several countries began to impose stricter liability rules on firms particularly with databases of financial and credit information as well as private information. In Korea, a proactive country in terms of cyber-security, the e-Financial Transaction Act (hereinafter referred to as EFTA) was enacted in 2007. This act tried to foster a sustainable information security infrastructure by prescribing higher legal standards for financial institutions and service providers, and imposing responsibilities for lossescaused by cyber financial accidents.

While one can witness the evolution of national compliance and liability regulations as a response to the needs for sustainable development of cyber-security, there has been considerable debate over whether these regulations are effective in promoting firms' cyber security activities. According to Schneier [23] and Varian [26], for example, poor information security in business practice is mainly caused by ill-distributed liability and compliance, and can be fixed by assigning the liability to the party that is in the best position to manage security risks. More specifically, Schneier [23] argues that the key element for security improvement is liability, and therefore, liable parties are motivated to put forth their best efforts to protect their security. In a similar vein, Varian [26] also argues that, in the case of the U. K. and the U. S., organizations with security liability have an incentive to invest in information security with due care and attention. In contrast, however, other researchers claim that security liability and compliance might not result in effective enforcement. Hoo [11] for instance, argues that even if compliance and liability rules are in effect, firms would not increase information security activities if the net payoff from the increase in information security activities is lower than the losses from cyber incidents, including legal fees from an ensuing liability lawsuit, regulatory violation penalties and lost earnings due to a diminished reputation. Johnson [12] further introduces examples of several security Acts which do not provide clear guidelines as to exactly what a firm must do

to protect information security, and argues that the vagueness of the Acts in providing a firm's obligation to protect information security might lower the firm's incentive to conduct proper information security activities. In such cases, imposing compliance and liability regulations might be ineffective and impractical. Whether or not a liability Act is effective for increasing firms'information security activities and can help achieve sustainable development of information security is therefore an empirical issue.

With one notable exception [10], there has been only limited research which focuses on empirical investigation on the impact of a compliance and liability regulation on firms' information security activities. Gordon et al. in reference [10] provide indirect evidence that security activities are drawing more attention from organizations since the passage of a compliance law than before it was enacted. This study builds on and expands reference [10] by empirically exploring the impact of a compliance and liability regulation on firms' information security activities in the case of Korea. More explicitly, the primary objective of this study is to investigate direct empirical evidence on the impact of EFTA, a Korean compliance and liability law targeting financial institutions and service providers, on firms' information security activities (i.e., the changes in firms' information security activities before and after the passage of EFTA) and to identify whether EFTA helps to create a sustainable national system for cyber security. I proceed with this investigation using the 2007 and 2008 Korean Information Security Surveys published by the Korean Internet and Security Agency (KISA) [13, 14]. As will be seen, the empirical results indicate that EFTA is generating a positive impact on financial institutions and service providers' information security activities: financial institutions and service providers significantly increased information security related activities after the enactment of EFTA. The findings from this analysis, therefore, provide strong evidence that EFTA is helping build an effective and sustainable national system of cyber-security.

The remainder of this study is organized as follows. In Section 2, the background of EFTA and the basic provisions of the Act will be summarized in order to set the stage for an empirical assessment of the effect of the act on information security activities by firms. In Section 3, the study turns to a discussion of the main research hypothesis, research method and its results. Section 4 concludes the study with a discussion of our empirical findings and their implications.

2. Background

As is the case with other developed countries, Korea, one of the world's leading countries in the Internet, has experienced a series

of severe cyber-attacks. For example, around 250 major servers were breached by a series of cyber-attacks in 2000. Through these attacks, major businesses as well as Korean government agencies were hacked and experienced an outage of services in compromised servers. In 2003, the Slammer Internet worm caused a shot-down of most Internet services in public and private sectors. In the subsequent years of the first decade of this century, there has been an increased number of cyber incidents, exemplified by the leakage of roughly 10 million customers' private information through hacking attacks on Internet Auction Co., Ltd, the national affiliate of eBay, in 2008, and the leakage of private information on about 20 million customers of the major Korean retailers in 2010. The increased number of cyber-attacks and the increased amount of the losses highlighted the need for more detailed and sophisticated policies and strategies in both public and private domains.

Given this series of extensive cyber incidents, there has been a growing effort to develop a sustainable legal system for cyber security and to set enhanced information security compliance and liability regulations for firms. EFTA was one of the resulting legislative Acts. EFTA which went into effective in January 2007, attempted to update standards for highly networked environment and clarify liability rules. It is one of the most important pieces of legislations affecting firms engaged in electronic financial transactions since this act required firms to comply with higher legal standards, particularly financial institutions which manage databases of detailed financial and credit information as well as private information of customers. EFTA has also been considered a proactive regulation since it prescribed not only higher legal standards but also shifted responsibility for losses caused by cyber financial accidents from customers to financial institutions. Furthermore, it mandated that all financial institutions purchase cyber insurance in order to protect customers from potential losses caused by hacking or theft of personal data.

EFTA regulates all types of electronic financial transactions and all types of enterprises conducting electronic financial services, and provides standards for engaging in electronic financial transactions [20]. The main objectives of this Act are to achieve sustainable development in information security by clarifying legal responsibilities and establishing a strong foundation for electronic financial systems by securing the safety and reliability of electronic financial transactions. While there are numerous provisions to EFTA, Sections 9, 10 and 21 of EFTA are of most interest to this study. Section 9 of EFTA entitled "Responsibilities of Financial Institutions and Financial Service Providers" imposes responsibility on financial institutions for recovering damages caused by electronic financial accidents. Section 21 of EFTA entitled "Duty to Secure Safety", requires financial institutions and fi-

nancial service providers to implement security procedures, to exercise due care in electronic financial transactions, and to comply with certain security standards and requirements in order to protect the customer information from unauthorized use. The Act therefore establishes more stringent responsibilities on financial institutions and financial service providers for protecting their customers against cyber incidents; imposes liability on financial institutions or service providers if damages are caused by misconduct of the institutions or service providers; and makes customers feel safer and securer in using electronic financial services by imposing stricter compliance requirements [20].

Although EFTA does not expressly require financial institutions and service providers to increase their information security activities, it would seem reasonable to expect that they would increase their security activities since they now have higher responsibility and liability for damages caused by cyber incidents. There has been, however, a considerable amount of criticism about the Act. Several practitioners have claimed that EFTA left many matters unsettled, pointing to several areas of vagueness in EFTA's language and content: first, while EFTA leaves no doubt that financial institutions and service providers have a legal duty under EFTA to protect customers' electronic transactions and need to recover damages if they breach the duty, it does not make attempt to define what constitutes "due care in electronic financial transactions"; second, while EFTA stipulates that damages of customers caused directly by the breaches of electronic transactions can be recovered, it does not give any indications as to whether other types of damages (e.g., a breach of private information) can be recovered; lastly, EFTA does not prescribe whether a breach of the duties imposed by the act is actionable in a private lawsuit. Due to these flaws, these practitioners believed that EFTA might not make financial institutions and service providers increase information security related activities.

Consequently, whether or not the enactment of EFTA can induce sustainable development in information security and can achieve the expected effects on firms' security related activities is an empirical issue.

3. Empirical Study

3.1 Hypothesis

EFTA will turn five years old on January 2012 after its enactment, yet there has been no systematic effort since its 2007 enactment directed towards the investigation of the effectiveness of this Act. This section is devoted to empirically investigate the effect of EFTA on firms' information security activities.

EFTA clearly addresses the necessity that

financial institutions and service providers need to exercise due care toward the security of their systems and have responsibility for protecting their customers against damages in electronic financial transactions. As mentioned in the previous section, however, EFTA does not explicitly advise financial institutions and service providers to increase information security activities. Therefore, it depends on each firm's decision whether or not to increase information security activities in response to EFTA.

Nevertheless, there may be at least two possible scenarios in which the enactment of EFTA would lead financial institutions and service providers to increase information security related activities : the first scenario is that, as EFTA imposes stricter liability and compliance rules on financial institutions and service providers, financial institutions and service providers would need to signal to the market that they are paying sufficient attention to their information security; and the second scenario is that financial institutions and service providers would react to EFTA by increasing their information security related activities. These two scenarios might lead us to believe that, after the passage of EFTA, financial institutions and service providers are likely to focus more on information security activities than they did prior to EFTA. Accordingly, it seems reasonable to hypothesize that financial institutions and service providers tend to increase their level of information security activities under EFTA more than they did prior to the enactment of EFTA. The null hypothesis therefor can be stated as :

H_0 : The Electronic Financial Transaction Act of 2007 did not lead financial institutions and service providers to increase information security activities.

To test the hypothesis, I use a pooled cross section technique since pooling the data from different years is the most commonly used technique for investigating the effects of a government law [27]. Specifically, I test the null hypothesis that nothing has happened to information security activities of financial institutions and service providers after the enactment of EFTA (i.e., $H_0 : P(Pre-EFTA) = P(Post-EFTA)$) : the alternative is that financial information security activities in institutions and service providers after the enactment of EFTA is greater than before (i.e., $H_1 : P(Pre-EFTA) \leq P(Post-EFTA)$).

3.2 Sample

In order to measure the impact of EFTA on information security activities by financial institutions and service providers, this paper uses the data extracted from the 2007 and 2008 Korean Information Security Surveys published by the KISA [13, 14]. While the 2007 survey gathered detailed information on information security practices for fiscal year

2006, which was prior to the enactment of EFTA, the 2008 survey gathered the information for fiscal year 2007, after the enactment of EFTA.

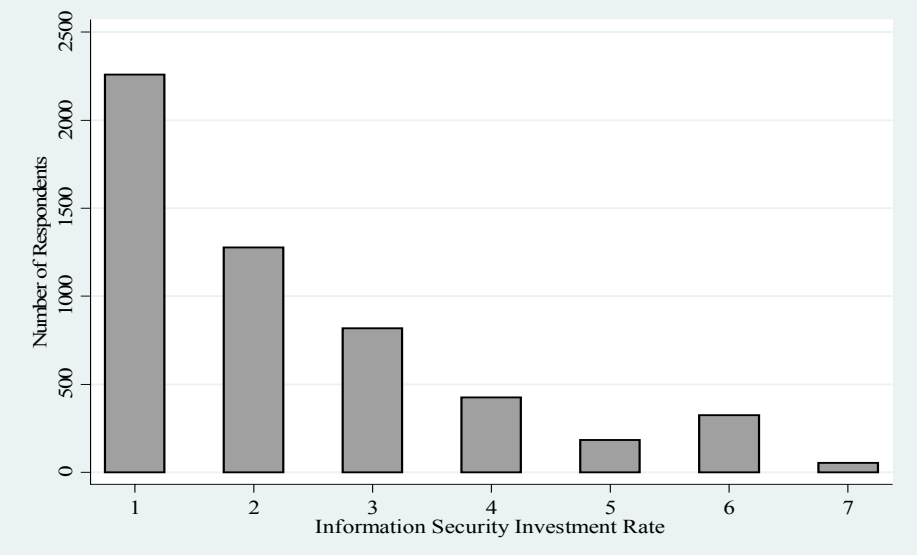
The population consisted of firms with a computer network and more than five employees. Using 2006 Information Society Statistics [18] for the 2007 Korean Information Security Survey and 2006 Korean Census on Basic Characteristics of Establishments [24] for the 2008 survey, 272,702 and 290,069 firms were identified as the populations for each survey. In order to have a large enough sample of firms which can provide statistically reliable results for analysis of subgroups, KISA established target sample sizes of 2,500 firms for the 2007 survey and 2,800 firms for the 2008 survey. The surveys used a stratified two-stage sampling methodology, based on firm size and industry type. Within each stratum, survey respondents were randomly selected. Over a period of two years, the surveys collected data on 2,508 organizations in 2007 and 2,828 organizations in 2008. In order to conduct an empirical analysis, this study pooled the data from both years.

The 2007 survey was conducted using personal interviews whereas the 2008 survey was conducted primarily by in-person interviews, with an Internet-based survey for respondents who were not available for in person interviews. The survey respondents were the participating firms' information system or finance directors who had full time security responsibilities.

3.3 Variables

Our dependent variable is an organization's security activities. An organization's security activities can be measured in many ways. Tanaka et al. [25], for example, used a binary choice variable (use or no use of the information security policy) to measure an organization's security activities. According to the authors, they employed this measure because it is extremely difficult to measure security activities directly, which are related to many different security controls including security software and hardware. Liu et al. [16] used the number of security measures as a proxy of security activities. In their study, rather than using the real number of security measures employed, the authors categorized security activity levels into two groups : a group with a low security activity (i.e., the number of security measures is four and below) and a group with a high security activity (i.e., the number of security measures is seven and above).

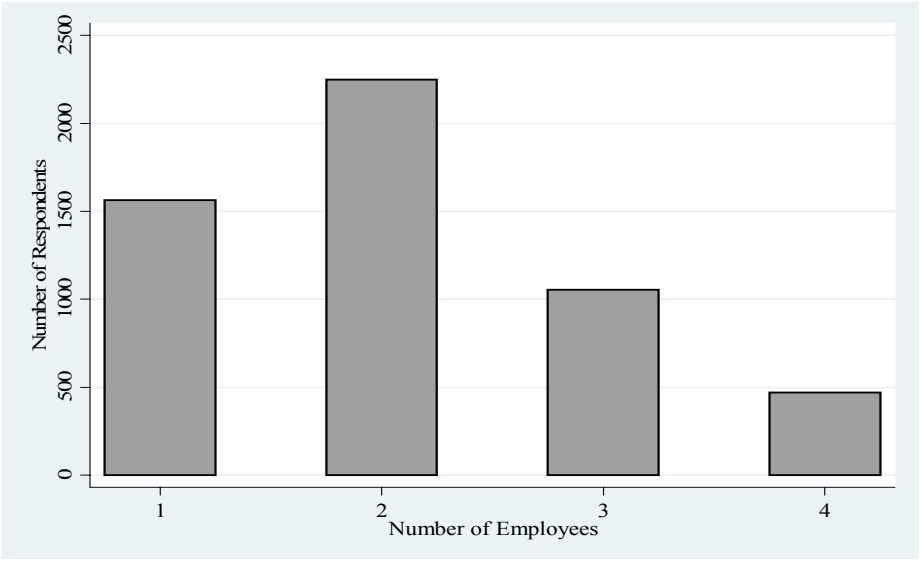
In this study, I use the percentage of the total IT budgets allocated to information security, sec_inv_rate, as a proxy for a firm's information security activities (hereinafter referred to as "information security investment rate")[6] : this measure can be defined as the relative percentage of a firm's total IT budget which is given to the firm's activities on in-



〈Figure 1〉 Frequency Plot of Information Security Investment Rate

formation security. In spite of certain limitations such as not all the funds in the security budget comes from IT budget (i.e., some funds can come from audit or other departments), this variable is widely used in the security literature [2, 7-9, 21, 22]. The KISA surveys categorize the information security investment rate into seven categories : 0%, 0~less than 1%, 1~less than 3%, 3~less than 5%, 5~less than 7%, 7~less than 10% and 10% or more. I assign 1 through 7 to each category, respectively. Figure 1 shows the information security investment rate of respondent firms.

The independent variables can be categorized into two groups : research variables and control variables. Research variables are necessary to empirically test the hypothesis. These variables include the industry type and year and the interaction term of the industry type and year. Since EFTA intends to target financial institutions and service providers, it would cause industry-specific differences; that is, financial institutions and service providers might be influenced more by EFTA than firms in other industries. Therefore, I take these differences into account by including an industry-type dummy variable in the models. Although the KISA surveys group organizations into 10 different industries, I create one dummy variable, finance, which is coded '1' if an organization is included in the 'financial and insurance' industry and '0' otherwise. Of the total sample, 10.51% (561) of the firms are included in the financial and insurance industry, while 89.49% (4,775) of the firms are included in other industries.



〈Figure 2〉 Frequency Plot of Size of Respondent Firms

In order to examine the effect of EFTA, I also include the 'year' dummy variable and the interaction term of the industry dummy variable and the year dummy variable. The year dummy variable, *y*08, captures the changes in the information security investment rate from the 2007 survey to the 2008 survey. Therefore, *y*08 is coded '1' if the observation is from the 2008 survey and '0' otherwise. The interaction term, $y08\ finance$, which is the main interest of this study, is used to measure the changes in the level of the information security investment rate in the financial and insurance industry due to the enactment of EFTA.

In addition to the research variables, I also employ several control variables which may influence the dependent variable. In particular, I use two control variables : firm size and collection of private information. I include the firm size since there has been empirical evidence on the positive relationship between the size of businesses and the level of information security investment [3, 25]. For example, Tanaka et al. [25] shows that a lack of IT resources in small businesses may be associated with low level of information security investment. I use the number of employees, emp, as a proxy for firm size. The KISA surveys categorize firms into four categories : 5~9 employees, 10~49 employees, 50~249 employees, and 250 employees or more. This study assigned 1 through 4 to each category, respectively. The following figure shows the number of employees of the respondent firms.

With respect to the second control variable, I control for the collection of private information in the analysis because firms collecting private information will have to ensure a

〈Table 1〉 Dependent and Independent Variables

Variables	Measures	Names	Description
Dependent variables	◦ Information security activities	sec_inv_rate	◦ Proxied by information security investment rate. ◦ 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	◦ Industry type	finance	◦ Firms in the financial and insurance industry vs. firms not in the financial and insurance industry. ◦ Coded '1' if a firm is a financial institution or a financial service provider, and '0' otherwise.
	◦ Year	yr08	◦ The changes in information security investment rate from the pre- to post-EFTA periods. ◦ Coded '1' if the observation is from the 2008 survey and '0' otherwise.
	◦ Industry type *Year	y08finance	◦ The changes in information security investment rate in the financial and insurance industry in the post-EFTA period. ◦ The interaction term of industry type and year variables
	◦ Firm size	emp	◦ Proxied by the number of employees ◦ Five categories; 1(5~9 employees), 2(10~49 employees), 3, 50~249 employees), 4(250~299 employees), and 5(300 employees or more)

higher level of confidentiality than firms that do not collect private information. According to Campbell et al. [4] and Acquisti et al. [1], since 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 for firms, firms collecting private information have a higher incentive to invest in information security that firms that do not collect private information. I code the collection of private information, *pri_info*, '1' if an organization collects private information through their website and '0' otherwise. Of the total sample, 69.90% (3,730) of the firms do not collect private information, while 30.10% (1,606) of the firms collect private information. <Table 1> lists the variables used in this study.

3.4 Analysis

To test the hypothesis of the impact of EFTA on information security activities, I regard the sample in the Pre- and Post-EFTA periods. That is, I define the data for Pre-EFTA as the sample from the 2007 survey which comprises the security practices of firms in 2006 and define the data for Post-EFTA as the sample from the 2008 survey which constitutes the security practices in 2007. The total number of Pre-EFTA observations is 2,508 of which 239 (9.53%) belong to the financial and insurance industry. The total number of Post-EFTA observa-

tions is 2,828 of which 332 (11.39%) belong to the financial and insurance industry. Thus, for pooled cross-sectional testing, the effective sample size for Pre- and Post-EFTA years is comprised of a total of 5,336 observations, which includes a total of 561 observations of firms that are included in the financial and insurance industry.

Since our dependent variable, *sec_inv_rate*, has an ordered discrete scale, I perform an ordered logit analysis. The ordered logit is widely used to deal with a discrete dependent variable which is measured on an ordinal scale. The economic specification of the ordered logit model applied here can be denoted as :

$$\log\{P_{ij}/(1-P_{ij})\} = \alpha_0 + \beta x_{i,} \qquad (3.1)$$

where P_{ij} is the cumulative probability of the i th firms in the j th or higher category of the dependent variable and x_i is a vector of the independent variables. In this study, the term $\log\{P_{ij}/(1-P_{ij})\}$ specifically predicts the probability of higher information security investment rate with changes in the relevant independent variables.

Since our main interest is to analyze whether the enactment of EFTA increases the level of information security investment of firms in the financial and insurance industry compared to firms in other industries, the key element is to look at the difference in the average rate of information security investment of firms in the financial and insurance industry between Pre- and Post-EFTA years. I therefore estimate the difference-in-differences estimator which has the following specification :

$$\hat{\beta}_2 = (\overline{sec\_inv\_rate}_{post,\ f} - \overline{sec\_inv\_rate}_{post,\ nf}) - (\overline{sec\_inv\_rate}_{pre,\ f} - \overline{sec\_inv\_rate}_{pre,\ nf}) \qquad (3.2)$$

where "f" stands for "a firm in the financial and insurance industry" and "nf" stands for "a firm not in the financial and insurance industry"; and "$Post$" stands for "in the Post-EFTA year" and "Pre" stands for "in the Pre-EFTA year". Therefore, $\hat{\beta}_2$ is the difference over time in the average rate of information security investment between the financial and insurance industry and other industries. In order to investigate whether $\hat{\beta}_2$ is statistically different from zero, I estimate the following ordinal logit regression model using the data pooled over both Pre- and Post-EFTA years :

$$\log\{P_{ij}/(1-P_{ij})\} = \alpha_0 + \beta_0 y08 + \beta_1 finance + \beta_2 y08 finance + u. \qquad (3.3)$$

As can easily be identified, the intercept α_0, is the average rate of information security investment of firms not in the financial and insurance industry in the Post-EFTA year. The parameter β_0 captures changes in the average rate of information security investment in all industries from the Pre-EFTA year to Post-EFTA year. The coefficient on $finance$, β_1,

measures the industry-specific effect on firms in the financial and insurance industry that is not due to the presence of EFTA. The parameter β_2, which is the central interest of this study, measures the increase in the average rate of information security investment in firms in the financial and insurance industry due to the enactment of EFTA, provided I assume that firms both in and outside of the financial and insurance industry did not make different levels of information security investments for other reasons. In other words, this model allows the contribution of the firm's characteristics to information security investment to be constant over the entire time period but the effect of the enactment of EFTA to change.

The estimates of Equation (3.3) are given in <Table 2>. As can be identified by the likelihood ratio chi-square statistic and the p-value from the likelihood ratio chi-square test, since the model has a good fit to our data, the coefficient estimates can be seen as appropriate. The coefficient of the variable $finance$ is positive but statistically insignificant. This indicates that firms in the financial and insurance industry are not statistically likely to have higher information security investment rate than do firms in other industries. As for the coefficient of $y08$ $finance$, however, it has a positive sign and is statistically significant at the 0.001 significance level. This suggests that after the enactment of EFTA, firms in the financial and insurance industry started to make higher information security investment than did firms in other industries. Conse-

〈Table 2〉 Ordered Logit Results for Information Security Investment Rate (Without Control Variables)

Order logistic regression — Number of obs = 5336
LR chi2(3) = 124.70
Prob > chi2 = 0.0000
Log likelihood = -8079.9247 — Pseudo R2 = 0.0077

sec_inv_rate	Coef.	Sed. Err.	z	P > |z|	[95% Conf.	Interval]
yr08	.3379209	.0529874	6.38	0.000	.2340675	.4417743
finance	.1315041	.1279892	1.03	0.304	-.1193501	.3823583
yr08finance	.6592457	.1659435	3.97	0.000	.3340024	.9844889
/cut1	-.0897545	.0396559			-.1674787	-.0120304
/cut2	.912102	.0416232			.8305221	.9936819
/cut3	1.743179	.047292			1.650488	1.835869
/cut4	2.412178	.0552237			2.303941	2.520414
/cut5	2.851701	.0627973			2.72862	2.974781
/cut6	4.88188	.1420738			4.60342	5.160339

* cut1 to cut6 are the estimated cut points, which exist for each value of the dependent variable.

quently, I reject the null hypothesis, which states that EFTA did not lead financial institutions and service providers to increase information security activities, and find empirical support that the information security activities in the financial and insurance industry has indeed increased from the Pre- EFTA year to the Post-EFTA year. One might however argue that the increase in the information security investment rate in the financial and insurance industry is not due to the enactment of EFTA, but due to other reasons such as the increase in the public concern regarding cyber safety and the correspondingly increased public pressure urging firms to invest more in information security. To verify this argument, I perform a further regression analysis that can be found in the appendix.

The Pseudo R-squared value for the model is 0.0077. There are several possible reasons for this low R-squared value. First, the use of various discrete variables, which are either dichotomous or polytomous, with limited variability causes a low R-squared value. Second, the R-squared value is normally lower for cross-section data than for time series data [27]. While the low R-squared value might suggest the model used here is incomplete and additional variables need to be included in the model, its explanatory power should be evaluated not by the R-squared value but by the statistical significance of each independent variable[5, 27]. In other words, based on the large sample size (n = 5336), the statistically significant independent variables remain consistent predictors of the ceteris paribus effect on the dependent variable.

In addition to the low R-squared value, the model has another limitation. That is, the model, which assumes the contributions of the firm's characteristics are constant over time, is somewhat restricted since those contributions can change over time : the pattern of information security investment rate of Pre- and Post-EFTA might be sensitive to a firm's characteristics. To overcome these limitations, this study expands the model by including the two control variables described above (i.e., firm size and the collection of private information). The inclusion of the control variables allows us to avoid the systematic differences between the Pre- and Post-EFTA years and can reduce the error variance, which in turn can lead to shrink the standard error of β_2 [27]. As can be seen in <Table 3>, the inclusion of the control variables raises the R-squared value from 0.0077 to 0.0357 by decreasing the residual variance. Compared to the above model with no control variables, therefore, this model has a higher test statistic $z$on $y08$ $finance$.

Like the previous result, the coefficient on the interaction term shows that firms in the financial and insurance industry invested more in information security after the enactment of EFTA than did firms in other industries, and thus I reject the null hypothesis. It should be noted that, in this model, $finance$ has a small-

〈Table 3〉 Ordered Logit Results for Information Security Investment Rate (Without Control Variables)

Order Logistic regression — Number of obs = 5336
LR chi2(5) = 580.57
Prob > chi2 = 0.0000
Log likelihood = -7851.9887 — Pseudo R2 = 0.0357

sec_inv_rate	Coef.	Sed. Err.	z	P > |z|	[95% Conf.	Interval]
yr08	.4204033	.0540643	7.78	0.000	.3144393	.5263673
finance	-.0623196	.1314878	-0.47	0.636	-.3200309	.1953918
yr08finance	.7523455	.1679435	4.48	0.000	.4231822	1.081509
emp	.4767461	.0288236	16.54	0.000	.4202529	.5332393
pri_info	.5422299	.0579317	9.36	0.000	.4286858	.655774
/cut1	1.057952	.0734198			.9140517	1.201852
/cut2	2.12876	.0777924			1.97629	2.28123
/cut3	3.014195	.0835563			2.850427	3.177962
/cut4	3.714184	.0897638			3.53825	3.890118
/cut5	4.16938	.0953276			3.982542	4.356219
/cut6	6.22657	.1599393			5.913095	6.540045

* cut1 to cut6 are the estimated cut points, which exist for each value of the dependent variable.

er coefficient than the previous model and is still statistically insignificant while the control variables *emp* and *pri_info* are statistically significant at the 0.001 level. This result implies that the control variables included in this model capture the firm's characteristics that are most important for determining the level of information security investment. The positive sign of the coefficient of *emp* suggests that the information security investment increases as the size of a firm rises. Similarly, the positive coefficient of *pri_info* indicatesthat the amount to invest on information security rises if a firm collects private information from its customers. The likelihood ratio chi square test shows a good fit of the model to the data.

4. Concluding Comments

While EFTA addressed the increased responsibility and liability of financial institutions and service providers for their customers, it did not settle the question of whether those businesses are required to increase information security activities to meet compliance rules imposed by EFTA. Even if it is rational to assume that increased responsibility and liability in protecting customers' information seems to lead firms to invest more in information security related activities, as explained in the previous section, several practitioners have argued that EFTA has not worked as intended since various ambiguities in EFTA did not lead financial institutions and

service providers to increase their information security activities. Therefore, the way financial institutions and service providers respond to EFTA is totally an empirical question.

In this study, I have shed light on this question through empirical evidence that EFTA actually has a significant impact on the increase in information security activities of financial institutions and service providers and contributes to achieve sustainable information security to a certain degree. More explicitly, this article identifies that information security activities, proxied by the information security investment rate, of financial institutions and service providers have meaningfully increased after the enactment of EFTA when compared to the year prior to the enactment of the law. Based on the findings from the regression analysis, therefore, I believe that the compliance and liability provisions stipulated in EFTA have a positive impact on information security activities of firms in the financial and insurance industry.

These findings do not, however, prove that EFTA is effective in motivating financial institutions and service providers to invest sufficient resources in information security activities. Indeed, several practitioners have argued that, due to the unsettled issues explained in the previous section, various financial institutions and service providers have not invested sufficient resources in information security activities, and thus experienced cyber incidents which could have been avoided had there been sufficient security investments. Therefore, the government needs to know that the enactment of a liability and compliance law is necessary but not sufficient, and a sustainable solution for cyber security is only possible if adequate incentives are given to firms and reliable mechanisms are established to enforce compliance. To do this, the government needs to address the issues that currently remain unsettled in EFTA and devise proper monitoring and enforcement mechanisms to ensure the effectiveness of EFTA.

On the other hand, the exclusion from EFTA of firms in other industries performing electronic financial services, together with the interdependent characteristics of information security identified by several authors [e.g., 15, 19, 28], might hinder firms in making socially optimal security investments; the increase in information security activities only of firms in the financial and insurance industry will lead firms in other industries to make socially inefficient investment in information security (i.e., externality problems). To achieve a sustainable development continuum in information security, therefore, in revising EFTA in the future, the government might need to target a wider range of firms in various industries, particularly firms managing customers' private and financial information, and to stipulate a firm's liabilities on damages caused not only by breaches of financial transactions but by other types of breaches (e.g., breaches of private information) which are

not directly related to financial transactions.

Lastly, businesses need to know that information security cannot be achieved by a one-time effort and adherence to security standards for the sake of compliance might be meaningless. Therefore, rather than sticking to a rigid checklist, they should have a process that can continually improve their institutional capacity to protect their resources against cyber-attacks.

Despite the interesting findings, the analysis conducted here has some limitations. The first limitation is inherent in the data. Although more detailed data would give a clearer insight into information security, the data used in this study was mostly based on categorized values, rather than qualitative and quantitative values. Second, this study did not consider other security activities such as security training programs, the deployment of new security solutions and hiring more employees who devote their effort to information security. Such considerations would offer possible avenues for further research. In sum, since the security investment can only be a partial mechanism for information security activities, I suggest that further research consider a more comprehensive approach which incorporates technology-based, management-based and policy-based security risk management activities. By considering alternative security activities in combination, one would be able to gain more robust results overcoming the current limitation.

References

[1] Acquisti, A., Friedman, A., and Telang, R., "Is there a cost to privacy breaches? An event study," in 5th Workshop on the Economics of Information Security, Cambridge, England, 2006.

[2] Anderson, J., "Why We Need a New Definition of Information Security," Computers and Security, Vol. 22, pp. 308-313, 2003.

[3] Baker, W. H. and Wallace, L., "Is information security under control? : Investigating quality in information security management," Security and Privacy, IEEE, Vol. 5, pp. 36-44, 2007.

[4] Campbell, K., Gordon, L., Loeb, M., and Zhou, L., "The economic cost of publicly announced information security breache s : empirical evidence from the stock market," Journal of Computer Security, Vol. 11, pp. 431-448, 2003.

[5] Christie, A. A., "Aggregation of test statistics : An evaluation of the evidence on contracting and size hypotheses," Journal of Accounting and Economics, Vol. 12, pp. 15-36, 1990.

[6] Gordon, L. and Loeb, M., "The economic of information security investment," in Economics of Information Security, Camp, L. and Lewis, S., Eds., pp. 105-127, Boston : Kluwer Academic Publishers, 2004.

[7] Gordon, L., Loeb, M., Lucyshyn, W., and

Richardson, R., “CSI/FBI computer crime and security survey,” COMPUTER SECURITY JOURNAL, Vol. 20, pp. 33-51, 2004.

[8] Gordon, L., Loeb, M., Lucyshyn, W., and Richardson, R., “CSI/FBI computer crime and security survey,” Computer Security Institute, 2005.

[9] Gordon, L., Loeb, M., Lucyshyn, W., and Richardson, R., “CSI/FBI Computer crime and security survey,” Computer Security Institute, 2006.

[10] Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Sohail, T., “The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities,” Journal of Accounting and Public Policy, Vol. 25, pp. 503-530, 2006.

[11] Hoo, K. J. S., “How Much Security is Enough : A Risk Management Approach to Computer Security,” Ph. D. Dissertation, Stanford University, Stanford, California, 2000.

[12] Johnson, V. R., “Cybersecurity, Identity Theft, and the Limits of Tort Liability,” South Carolina Law Review, Vol. 53, pp. 255-311, 2005.

[13] Korean Internet and Security Agency, “Korean Information Security Survey,” Korean Internet and Security Agency, Seoul, Korea, 2007.

[14] Korean Internet and Security Agency, “2008 Korean Information Security Survey,” Korean Internet and Security Agency, Seoul, Korea, 2008.

[15] Kunreuther, H. and Heal, G., “Interdependent security,” Journal of Risk and Uncertainty, Vol. 26, pp. 231-249, 2003.

[16] Liu, W., Tanaka, H., and Matsuura, K., “Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms,” Information and Media Technologies, Vol. 3, pp. 464-478, 2008.

[17] Majuca, R. P., “Three essays on the law and economics of information technology security,” University of Illinois at Urbana-Champaign, 2006.

[18] National Information Society Agency, “Information Society Statistics,” National Information Society Agency, Seoul, Korea, 2006.

[19] Ogut, H., Menon, N., and Raghunathan, S., “Cyber insurance and IT security investment : Impact of interdependent risk,” University of Texas at Dallas, 2005.

[20] Reich, P. C., “Cybercrime, Cybersecurity, and Financial Institutions Worldwide,” in Cyberlaw for Global E-business : Finance, Payments and Dispute Resolution, Kubota, T., Ed., ed Hershey, PA : IGI Global, 2008.

[21] Richardson, R., “CSI computer crime and security survey,” Computer Security Institute, 2007.

[22] Richardson, R., “CSI Computer Crime and Security Survey,” Computer Security Institute, 2008.

[23] Schneier, B., “Computer security : It’s the economics, stupid,” in 1st Annual Workshop on Economics of Information Security, Barkeley, CA, 2002.

[24] Statistics Korea, “Korean Census on Basic Characteristics of Establishments,” Statistics Korea, Daejon, Korea, 2006.

[25] Tanaka, H., Matsuura, K., and Sudoh, O., “Vulnerability and information security investment : An empirical analysis of e-local government in Japan,” Journal of Accounting and Public Policy, Vol. 24, pp. 37-59, 2005.

[26] Varian, H., “Managing Online Security Risks,” in The New York Times, ed, 2000.

[27] Wooldridge, J., Introductory econometrics : A modern approach, 2nd ed. Mason, OH : Thomson South-Western, 2003.

[28] Zhao, X., “Economic analysis on information security and risk management,” Ph. D. Dissertation, The University of Texas at Austin, Texas, 2007.

〈Appendix〉

In order to investigate whether the increased information security activities is caused by other reasons, such as the increased public pressure for information security, and is pervasive in firms in other industries which conduct electronic financial services without being subject to EFTA, I further divide the industry type into four categories (i.e., financial and insurance industry; logistics and telecommunications industry; real estate, renting and business services industry; and other industries) and use other industries as the default category. The logistics and telecommunications industry (*logtel*), and the real estate, renting and business services industry (*realtor*) were chosen since many firms in these industries are considered to be firms that conduct electronic financial services and have recently been requested to put more effort into information security. Therefore, I estimate the following ordered logit regression model using the pooled cross-section data :

$$\log\{P_{ij}/(1-P_{ij})\} = \alpha_0 + \beta_0 y08 + \beta_1 finance + \beta_2 \log tel + \beta_3 realtor + \delta_1 y08\, finance + \delta_2 y08 \log tel + \delta_3 y08\, realtor + u. \quad \text{(a.1)}$$

where *logtel* is a binary variable equal to one if the firm is in the logistics and telecommunications industry and zero otherwise, and *realtor* is a binary variable equal to one if the firm is in the real estate, renting and business activities industry. $y08\,logtel$ and $y08\,realtor$ are the interaction terms of the year dummy variable, and the 'logistics and telecommunications' and 'real estate, renting and business services' industry dummy variables, respectively.

The estimates of Equation (a.1) are given in <Table a.1> It can be identified that the variables $y08\,logtel$ and $y08\,realtor$ are not statistically significant, suggesting that information security activities of firms in the logistics and telecommunication industry and in the real estate, renting and business services industry in the Post-EFTA year do not show the systematic difference with the activities in the Pre-EFTA year. <Table a.2>, which includes the additional control variables, also shows the similar result. These results suggest strong indirect evidence that the increased activities of information security in the financial and insurance industry is caused by the enactment of EFTA rather than other reasons.

〈Table a.1〉 Ordered Logit Results for the Expanded Model (Without Control Variables)

Ordered logistic regression — Number of obs = 5336
LR chi2(7) = 130.10
Prob > chi2 = 0.0000
Log likelihood = -8077.2239 — Pseudo R2 = 0.0080

sec_inv_rate	Coef.	Sed. Err.	z	P>|z|	[95% Conf.	Interval]
yr08	.310643	.0595976	5.21	0.000	.1938338	.4274523
finance	.1435824	.1294312	1.11	0.267	-.1100981	.397263
logtel	.1496655	.1438817	1.04	0.298	-.1323374	.4316684
realtor	.0035232	.1180027	0.03	0.976	-.2277577	.2348042
yr08finance	.6871328	.1682152	4.08	0.000	.357437	1.016829
yr08logtel	.0684572	.1930277	0.35	0.723	-.3098701	.4467845
yr08realtor	.1485517	.1598739	0.93	0.353	-.1647955	.4618989
/cut1	-.0782254	.0440163			-.1644958	.008045
/cut2	.9244318	.0458351			.8345968	1.014267
/cut3	1.756406	.0511227			1.656207	1.856604
/cut4	2.425885	.0585645			2.311101	2.54067
/cut5	2.865598	.0657651			2.736701	2.994496
/cut6	4.896023	.1434247			4.614916	5.17713

* cut1 to cut6 are the estimated cut point, which exist for each value of the dependent variable.

〈Table a.2〉 Ordered Logit Results for the Expanded Model (Without Control Variables)

Order logistic regression — Number of obs = 5336
LR chi2(9) = 585.80
Prob > chi2 = 0.0000
Log likelihood = -7849.3723 — Pseudo R2 = 0.0360

sec_inv_rate	Coef.	Sed. Err.	z	P>|z|	[95% Conf.	Interval]
yr08	.3801617	.0605593	6.28	0.000	.2614676	.4988558
finance	-.0633325	.1329404	-0.48	0.634	-.3238909	.1972259
logtel	-.017981	.1476506	-0.12	0.903	-.3073708	.2714088
realtor	-.0024973	.1193753	-0.02	0.983	-.2364686	.2314739
yr08finance	.7938127	.170247	4.66	0.000	.4601347	1.127491
yr08logtel	.2989851	.196963	1.52	0.129	-.0870552	.6850254
yr08realtor	.1141386	.1618054	0.71	0.481	-.2029941	.4312713
emp	.4787021	.0289135	16.56	0.000	.4220327	.5353715
pri_info	.5403849	.0579615	9.32	0.000	.4267825	.6539874
/cut1	1.059747	.0754799			.911809	1.207685
/cut2	2.131382	.0797481			1.975078	2.287685
/cut3	3.017529	.0854084			2.850132	3.184927
/cut4	3.717891	.0914879			3.538578	3.897204
/cut5	4.17318	.0969482			3.983166	4.363195
/cut6	6.230325	.1609105			5.914946	6.545704

* cut1 to cut6 are the estimated cut point, which exist for each value of the dependent variable.

저 자 소 개

Woohyun Shim	(E-mail : shimwoo@msu.edu)
1996	B.A. in Economics, Sungkyunkwan University
2002	M.A. in Economics, Seoul National University
2010	Ph.D. in Media and Information Studies, Michigan State University
2011~present	Senior Researcher, Synthesys, Inc., East Lansing, MI, USA
Interested Area	Cyber-security, Privacy, Digital Ecosystem and Convergence, Innovation and Regulation