http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.20, No.4, November 2015, pp.241-256
http://dx.doi.org/10.7838/jsebs.2015.20.4.241

정부의 정보 보안 대책 법제화의 사전 효과성 분석 방법

An Ex Ante Evaluation Method for Assessing a Government Enforced Security Measure

심우현(Woohyun Shim)*

초 록

기업의 정보 보안을 보장하기 위해, 많은 정부가 다양한 보안 관련 대책을 의무화해오고 있다. 하지만 이러한 보안 대책의 실행에 앞서, 이의 잠재적 효과성을 분석하는 연구는 부족한 실정이다. 본 연구는 안전벨트의 착용 법제화가 자동차 사고 사망자 감소에 미치는 효과에 대한 연구를 응용하여, 정부의 다양한 보안 대책의 사전 효과성 평가가 가능한 모형을 개발하는 것을 목적으로 한다. 또한, 인터넷 진흥원의 정보보호실태조사(기업편) 데이터를 개발된 모형에 적용하여 어떠한 보안대책의 법제화가 사회 및 산업 전반의 보안위험을 줄이는데 효과적인지 사전평가를 시행하였다. 그 결과 보안교육의 법제화가 다른 보안대책에 비해 효과적임을 확인하였다.

ABSTRACT

In order to ensure that all firms are cyber-secure, many governments have started to enforce the implementation of various security measures on firms. Prior to the implementation, however, it is vague whether government enforced security measures will be effective for mitigating cyber-security risks. By applying a method for estimating the effectiveness of a mandatory seatbelt law in reducing fatalities from motor vehicle accidents, this study develops an ex ante evaluation method that can approximate the effectiveness of a government enforced security measure in reducing country-wide or industry-wide cyber-security risks. Using data obtained from the Korean Internet and Security Agency, this study then explores how to employ the developed method to assess the effectiveness of a specific security measure in mitigating cyber-security risks, if enforced by the government, and compares the effectiveness of various security measures. The comparison shows that compulsory security training has the highest effectiveness.

키워드 : 사이버보안, 보안사고, 보안대책, 사전평가
Cyber-Security, Security Incidents, Mandatory Security Measure, Ex Ante Evaluation

* Department of Information Engineering and Computer Science, University of Trento, Trento, Italy (shim.woohyun@unitn.it)
Received: 2015-10-14, Review completed: 2015-11-09, Accepted: 2015-11-24

1. Introduction

In the last decades, as one of the most wired countries in the world, Korea has witnessed the rapid increase in the number of cyber-security incidents, driven by various types of cyber-attacks. For example, in March 2014, Korean Telecom (KT) Corp. experienced a significant data breach caused by anonymous hackers breaking into its systems and compromised estimated 12 million customer information including names, personal identification numbers and bank account details [22]. There were also a series of data breaches in several credit card companies in January 2014: three credit card companies, KB Kookmin, NH Nonghyup and Lotte, were attacked by a group of hackers, and around 80 million client information including credit card and bank account information was leaked [12]. In the news article, a security expert said that hackers can sell each client's information for $23-$135 depending on the types of the information [1].

It is therefore beyond doubt that tactics and strategies of cyber perpetrators are sufficient and efficient for circumventing or incapacitating implemented security measures through exploiting identified software vulnerabilities [2]. Accordingly, in order to achieve the sustainable cyber-security environment, many governments have enacted several security rules and regulations which enforce the implementation of a series of technical, managerial and organizational security measures. For example, the Korean government revised the e-Financial Transaction Act (EFTA) and the information communications network act (ICNA) which were issued in 2006 and 1986, respectively, to reflect a rapidly changing cyber-security environment. In the revisions of these regulations, certain types of businesses such as financial firms were stipulated to employ a chief security officer (CSO).

While security measures enforced by regulations might foster a sustainable cyber-security infrastructure by setting a bar for a sound cyber-security environment, they are generally very expensive from society's point of view as they may require huge resources to be invested. Therefore, if a government imposed security measure is ineffective or there is a potentially better alternative security measure, it might result in misaligned resource allocation and generate social waste. The issue here is that a method to assess the effectiveness of a government enforced security measure prior to its implementation have been largely overlooked and still remain understudied. A lack of thorough investigations on the effectiveness of government mandated security measures might lead a policy-maker to develop insubstantial and undesirable security rules and policies.

Therefore, unlike previous studies on cyber-security which mainly sought to make an ex post assessment of the effectiveness of a voluntarily implemented security measure

in reducing security risks of an individual actor (e.g, [5, 16]), this study aims at developing an ex ante evaluation method that can estimate the country-wide or industry-wide effectiveness of a government enforced security measure before its enactment. A traditional regression model is not appropriate for this evaluation since it can only measure the ex post effect of the implementation of a security measure on an individual level (e.g., firm or user). The contribution of this study is therefore to devise a method for ex ante evaluation of the effectiveness of a government enforced security measure which can estimate "expected diminishment of security risks if all individual entities in a country or an industry sector employ a government enforced security measure." More specifically, the devised method adapted from a series of studies on the effectiveness of compulsory seatbelt wearing (e.g., [7, 8]) shows how muchcountry-wide or industry-wide security reduction can be achieved if the government mandates to implement a specific security measure.

This study is structured as follows: Section 2 provides the background information and reviews the relevant literature. Section 3 presents a method that is attuned to estimating the effectiveness of a security measure which may be enforced by the government in the future. Section 4 uses data offered by the Korean Internet and Security Agency (KISA) and empirically presents a procedure for estimating the effectiveness of a government enforced security measure based on a series of scenarios. Section 5 concludes with some final remarks and discussion.

2. Background and Relevant Literature

Since early 2000, a series of cyber incidents have resulted in extensive damage on the whole society as well as on government agencies and organizations. Many governments and industry trade associations have made an extensive effort to develop a framework for information security risk management (e.g., ISO/IEC 27005:2011 and NIST 800-30).

As one of the most proactive countries with respect to cyber-security, the Korean government has also made a growing effort to mitigate cyber-security risks and enacted various security regulations and rules. For instance, in 2006, the government established the EFTA to enhance a cyber-security infrastructure and enforced higher legal standards on financial institutions. The EFTA imposed strict security compliance rules on firms engaging in electronic financial transactions on the ground that these firms have highly detailed databases of customers'private and financial information which can greatly undermine their well-being if compromised. Therefore, it prescribed that all financial firms need to employ appropriate security controls and procedures to ensure the

security in electronic transactions, and to take higher liabilities for customers' financial losses caused by cyber incidents [17]. The revision of the EFTA in 2014 further imposed stricter compliance requirements on financial firms by providing that a CSO should be appointed at director level and is prohibited from holding a chief information officer position concurrently.

Another example is the ICNA issued in 1986. Inthe ICNA, certain information and communications (IC) businesses, including IC service providers, IC facility operators and Internet service providers, with average daily users more than a million or with the previous year's sales more than 10 billion won, are obliged to obtain the information security management system (ISMS) certificate issued by the KISA [15]. The ISMS certification system aims at evaluating a firm's various security measures and policies for maintaining sustainability and reliability of its networks [15], and includes 5 requirements for information security policies (a total of 12 items) and 13 requirements for information security measures (a total of 92 items). In order to get the ISMS certificate, a firm needs to have various managerial and organizational security measures, including a formal information security policy and security training, as well as technical security controls including a firewall and an intrusion detection system. Similarly with the EFTA, the revision of the ICNAin 2014 further stipulated that firms, which need to obtain the ISMS certificate or have more than a thousand employees, should appoint a CSO who participates in the decision making process for the firm's information security strategies and activities.

While there is no doubt that the implementation of security measures enforced by national regulations, in response to the needs for developing sustainable and resilient information security systems, would make firms invest more on information security, there has been considerable debate over whether these regulations are actually effective in mitigating firms' cyber-security risks. For instance, Varian [21] and Schneier [19] argue that ill-distributed liability and compliance rules may undermine the soundness of information security in a firm, and conclude that well-designed security regulations, aligning with a firm's incentives, can resolve this problem. In the empirical analysis, Shim [20] also finds that a national security regulation contributes to the improvement of firms' information security. In contrast, other researchers including Hoo [10] and Johnson [11] claim that security regulations would not improve information security as long as the net benefit from the increased activities on information security is lower than the losses caused by security incidents. Gordon et al. [9] further indicate that, if a security regulation does not provide appropriate incentive mechanisms to firms, it might weaken firms' information security.

In my knowledge, however, there has been no research that investigates the effect of a security regulation or a security measure enforced by the government on mitigating country-wide or industry-wide security risks, particularly prior to its enforcement. Applying a method used in a series of studies on the effect of mandatory seatbelt wearing on reducing fatalities in car accidents (e.g., [3, 7, 8, 18]), this study devises an ex ante evaluation method that can assess how well the mandatory implementation of a security measure reduces country-wide or industry-wide security risks, and which one of the alternative security measures should be enforced by a regulation to obtain the socially optimal results.

3. Effectiveness of a Mandated Security Measure

This section introduces a formal ex ante evaluation method that estimate the effectiveness of the implementation of a government enforced security measure in reducing country-wide or industry-wide security risks. The method developed in this section is an application of a method used in a series of studies on the effect of a mandatory seatbelt regulation in preventing motor vehicle fatalities. In this study, mandatory seatbelt wearing is equivalent to the implementation of a security measure enforced by a security regulation, and the presence of a fatality can be considered as the experience of a security incident. For example, Evans [8] estimates that, by enforcing seatbelt wearing, a country can reduce drivers'chances of death from motor vehicle accidents by 43%. In a similar vein, the method applied here will show to what degree firms' chances of experiencing a security incident decrease if all firms in a country or in an industry sector implement a specific security measure enforced by the government.

Before starting with the detailed discussion on the method, one point should be noted. Unlike a regression model which can employ various types of variables, the method considered here only uses dichotomous variables. For example, a security measure used in the estimation is regarded as a binary variable (i.e., coded '1' if a firm employed the measure, and '0' otherwise). Similarly, a security incident is also considered to have binary values (i.e., coded '1' if a firm experienced a security incident (or more than once, and '0' otherwise). Using binary variables in the estimation has pros and cons. One prominent advantage would be that the method can be easily understood and used by a policy-maker or regulator and requires minimal data collection. The most important disadvantage of using binary values might be the loss of detailed information as the method does not take into account a different level or aspect

within a variable. For example, while a security incident may cause different levels of losses to firms, this information is not reflected in the estimation. The estimation using this method should therefore be used by a policy-maker or regulator as a preliminary complementary evaluation method, when available information is limited.

I now present the calculation procedures. For an illustrative purpose, the method is presented with the detailed calculation procedures adopted from [7, 8, 18]. Assume that the probability that firms with a security measure, A, experience a security incident is $\Pr_A$, and the probability that firms without A experience a security incident is $\Pr_{NA}$. The risk ratio $\Pr_A$ of the probability of a security incident with A to the probability of a security incident without A can then be given as:

$$R_A = \frac{\Pr_A}{\Pr_{NA}} = \frac{\dfrac{\text{Numter of firms with } A \text{ experiencing a security incident}}{\text{Numter of firms with } A}}{\dfrac{\text{Numter of firms without } A \text{ experiencing a security incident}}{\text{Numter of firms without } A}} = \frac{\dfrac{\alpha}{\beta}}{\dfrac{\delta}{\gamma}} \quad (1)$$

For example, if A is security training, R_A gives the ratio of the probability that firms with security training are actually breached, compared to the corresponding probability that firms without security training are actually breached. Therefore, if the government enforces the implementation of security training on all firms in the country and this can change a population of firms with high security risks to one with low security risks, R_A measures the risk ratio of new status (i.e., government enforced security training) to old status (i.e., voluntary security training) with high security risks, with nothing else changing.

Subtracting the risk ratio, R_A, from 1 and multiplying by 100 gives us the commonly known "percent effectiveness" of the implementation of A. This measure provides the value of percentage reduction of security incidents when all of the firms currently without A employ it. The percent effectiveness can be given as:

$$E_A = 100\left(\frac{\Pr_{NA} - \Pr_A}{\Pr_{NA}}\right) = 100(1 - R_A) \quad (2)$$

Therefore, E_A can be interpreted as the percentage reduction of the expected level of security incidents that the society gains, when the implementation of a specific security measure A is enforced by the government. A higher value of E_A indicates the greater effectiveness of A.

Whereas E_A can measure the overall effectiveness of the implementation of a government enforced security measure A, there may be several confounding factors that undermine the accuracy of E_A. For example, firms in different industry sectors and with different sizes would have different risk ratios since they have heterogeneous characteristics that affect the probabilities of a cyber-attack and a security breach. By taking into account confounding factors, it is possi-

ble to identify a real impact of the implementation of a government imposed security measure.

In order to incorporate a confounding effect in the method, assume a case where there is a confounding factor, x, which may cause an error in assessing the effectiveness of the implementation of a security measure. I regard x as a categorical variable such as a firm's industry sector (e.g., retailing, financial or manufacturing sector) or size (e.g., small, medium or large). The standard error caused by x can be defined as:

$$\Delta R_{(A,x)} = R_{(A,x)} \sqrt{(\sigma_\mu^2 + 1/\alpha + 1/\beta + 1/\delta + 1/\gamma)} \quad (3)$$

where $R_{(A,x)}$ is the risk ratio for each category of x and σ_μ is an estimate of unpredictable uncertainty. While σ_μ can have an arbitrary value between 0 and 1, following [7, 8], I assume that $\sigma_\mu = 0.1$. This implies that, due to an unpredictable confounding effect, the estimation of $R_{(A,x)}$ has an error of ±10%. As explained previously, α, β, δ and γ are the number of firms with A security measure experiencing a security incident, the number of firms with A, the number of firms without A experiencing a security incident, and the number of firms without A, respectively. As the standard error for each category in x is included in the estimation, the percent effectiveness of each category in x can be denoted as $E_{(A,x)} \pm 100\Delta R_{(A,x)}$, where $E_{(A,x)}$ is the percent effectiveness of the mandatory implementation of A for each category in x. For example, if A is government enforced security training and a confounding effect x is caused due to different industry types, $E_{(A,x)} \pm 100\Delta R_{(A,x)}$ gives the percent effectiveness of the implementation of security training in each industry sector. It should be noted that, while I only consider a single confound factor, multiple confounding factors can also be used in the estimation by combining the confounding factors.

In order to estimate the overall percent effectiveness with a confounding effect, we need to calculate the average value of $R_{(A,x)}$ for different categories. As $R_{(A,x)}$ is a ratio, however, computing the arithmetical mean would not be desirable. I therefore use the weighted average based on the corresponding values of $R_{(A,x)}$ for different categories, which can be given as:

$$\overline{R}_A = \exp\left[\sum_x (w_x \times \log(R_{(A,x)}) / \sum_x w_x\right], \quad (4)$$

where w_x is an assigned weight for each category in x and is given by $(R_{(A,x)}/\Delta R_{(A,x)})^2$. As $\overline{R}_A$ is also influenced by a confounding effect, the standard error of $\overline{R}_A$ should be taken into account as well and can be defined as:

$$\begin{aligned} \Delta \overline{R}_A &= \overline{R}_A / \sqrt{\Sigma_x (R_{(A,x)}/\Delta R_{(A,x)})^2} \quad (5) \\ &= \overline{R}_A / \sqrt{\Sigma_x w_x} \end{aligned}$$

Therefore, the estimate of the overall percent effectiveness can be given as

$$E_A^{\dagger} = 100(1 - \overline{R}_A \pm \Delta\overline{R}_A)$$

If A is government enforced security training, $E_A^{\dagger}$ is the effectiveness of government enforced security training on reducing country-wide security risks.

The next section explores how the developed method can be applied in a real-world scenario by using actual data obtained from the KISA.

4. Data and Scenarios

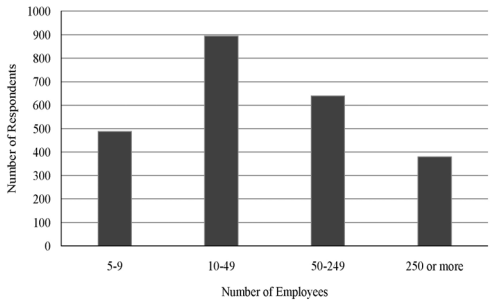
This section provides various scenarios on the implementation of government enforced security measures and estimates the percent effectiveness of these measures using data obtained from the KISA. This section further compares the percent effectiveness of various alternative security measures enforced by the government. It should be noted that the scenarios presented in this section are developed for illustrative purpose, and should be construed as examples.

4.1 Data

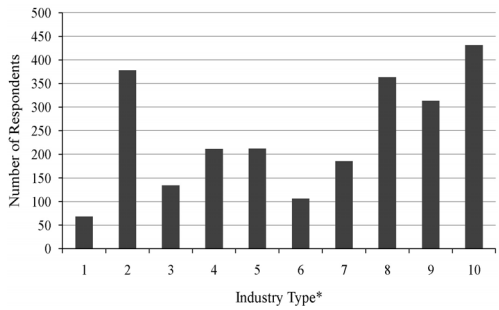
The scenarios use data from the 2007 and 2008 Korean Information Security Surveys published by the KISA [13, 14]. The data includes the security-related information on 5,336 firms with more than 5 employees. In this study, I utilize the records on the 2,401 firms (894 in 2007 and 1,507 in 2008) as the records on the firms without their own servers contain less detailed information. For the purpose of the scenario analysis, I pool the 2007 and 2008 data together. It should be noted that, while more recent survey reports have been published by KISA, the raw data are not publicly available because of the change in the government policy with respect to the release of data. The data used in this study is however sufficient for illustrating the estimation procedures.

There are various security measures that can be employed as scenarios, yet this study considers scenarios with the following security measures: security training, CSO, official security policy and official security department. Note that other security measures including a series of technical security controls can also be easily applied to the analysis. With respect to a security incident, for the illustrative purpose, I consider an incident caused by a virus infection. Again, a security incident caused by other types of attacks (e.g, spyware, distributed denial of services and hacking) or a different type of security incident (e.g., breach of customer information and system paralysis) can also be used to estimate the percent effectiveness of a specific security measure. In other to take into account a confounding effect, this study uses two factors: a firm's size proxied by the number of employees and its industry type. <Figure 1> and <Figure 2> show the

characteristics of respondent firms by size and industry type. The detailed information on the variables used in the study is presented in <Table 1>.



〈Figure 1〉 Size of Respondent Firms



* (1) agriculture, forestry, & fisheries, (2) manufacturing, (3) construction, (4) wholesaling, (5) retailing, (6) restaurant & lodging, (7) logistics & telecommunications, (8) financial & insurance, (9) real estate, renting & business activities, and (10) other services.

〈Figure 2〉 Industry Type of Respondent Firms

〈Table 1〉 Variables used in the Scenario Analysis

Variable	Description
Security incident	• Coded '1' if the firm experienced a security incident caused by a virus infection, and '0' otherwise.
Security training	• Coded '1' if the firm provides security training to its employees, and '0' otherwise.
Chief security officer	• Coded '1' if the firm has a CSO, and '0' otherwise.
Official security policy	• Coded '1' if the firm has an official security policy, and '0' otherwise.*
Official security department	• Coded '1' if the firm has an official security department, and '0' otherwise.
Firm size	• Proxied by the number of employees. • Grouped by five categories: 1 (5~9 employees), 2 (10~49 employees), 3 (50~249 employees), 4 (250 or more employees).
Industry type	• Categorized into 10 industries: agriculture, forestry, and fisheries (AG), manufacturing (MF), construction (CR), wholesaling (WS), retailing (RT), restaurant and lodging (HT), logistics and telecommunications (LO), financial and insurance (BK), real estate, renting and business activities (RE), and other services (ET).

* An official security policy is a document that broadly defines the company's baseline security rules; stipulates expected behavior of system users and the consequences of their system misuse or abuse; and defines the company's requirements for complying with the government regulations.

4.2 Scenarios

The percent effectiveness presented in the previous section provides us with a way to determine the influence of the government enforced adoption of a security measure on mitigating country-wide or industry-wide security risks. In order to streamline the exposition of the method, this subsection presents several realistic scenarios in which a firm's probability of being breached is affected by the implementation of a security measure enforced by the government.

Scenario 1: Mandatory implementation of a security training program

As identified by various studies, security training is essential for mitigating security risks and increasing effectiveness of an employed security measure [4, 6]. As a result, various governments require firms in a specific industry sector to provide security training to their employees. For example, firms in the financial or critical infrastructure industry in many developed countries (e.g., Germany, U.K, U.S and Korea) are now enforced to offer a series of security training programs to their employees. Some researchers (e.g., [5]) argue that mandatory security training actually helps reduce the number of security incidents. If their argument is true, the question then becomes whether expanding this enforcement to firms in other industry sectors or all industry sectors is fruitful and beneficial for improving cyber-security in the country.

In order to find an answer for this question, I examine the percent effectiveness of the government enforced implementation of security training in a specific industry sector as well as whole industry sectors. I assume that the Korean government wants to impose security training to all firms and, prior to the enforce-

〈Table 2〉 Estimated Percent Effectiveness of Mandatory Security Training

Industry Sector	$R_{(A,x)}$	$E_{(A,x)}$	$\Delta R_{(A,x)}$	$E_{(A,x)} \pm 100\Delta R_{(A,x)}$
AG	0.60	40.45	0.30	40.45 ± 30.48
MF	1.04	-4.00	0.27	-4.00 ± 26.58
CR	0.54	45.96	0.29	45.96 ± 29.06
WS	0.86	14.30	0.29	14.30 ± 29.23
RT	1.07	-7.00	0.31	-7.00 ± 31.32
HT	1.08	-7.50	0.48	-7.50 ± 47.67
LO	0.64	35.72	0.22	35.72 ± 21.58
BK	0.77	22.82	0.20	22.82 ± 20.03
RE	0.68	31.69	0.20	31.69 ± 20.02
ET	0.64	35.76	0.15	35.76 ± 14.56
Weighted Average Value				21.21 ± 7.77

ment, seeks to identify the effectiveness of the training in mitigating a security incident caused by a virus infection. <Table 2> shows the values estimated using equations (1) to (6).

From <Table 2>, it can be seen that, if the government enforces the implementation of security training to all firms, the overall percent effectiveness is between 13.44% to 28.98%. However, the enforcement would not be effective to improve cyber-security of firmsin some industry sectors including MF, RT and HT, as they might have the negative percent effectiveness. As a result, the government would be better to enforce security training only on firms in some specific industry sectors. For example, if the government enforces security training on firms in the LO, BK, RE and ET sectors, security incidents in these industry sectors caused by virus infections will be reduced by 22.36% to 40.83%.

Scenario 2: Mandatory CSO employment

Similarly with the previous scenario, the effectiveness of a government enforced CSO appointment can also be estimated. For example, through EFTA and ICNA, the Korean government have imposed firms in specific industry sectors to hire a CSO to mitigate security risks. While there is no sufficient evidence of the effectiveness of having a CSO in a firm on reducing security risks, the developed method can provide the information on the effectiveness in mitigating industry-wide or country-wide security incidents caused by virus infections. In order to estimate the effectiveness, I again use equations (1) to (6). The industry-wide and country-wide percent effectiveness of appointing a COS is presented in <Table 3>.

The results show that, unfortunately, the government enforced appointment of a CSO is not effective in reducing security incidents

〈Table 3〉 Estimated Percent Effectiveness of Mandatory CSO Employment

Industry Sector	$R_{(A,x)}$	$E_{(A,x)}$	$\Delta R_{(A,x)}$	$E_{(A,x)} \pm 100\Delta R_{(A,x)}$
AG	0.73	26.96	0.38	26.96 ± 37.75
MF	1.30	-29.84	0.32	-29.84 ± 31.84
CR	1.03	-2.84	0.51	-2.84 ± 51.05
WS	1.09	-9.05	0.36	-9.05 ± 36.47
RT	0.99	1.00	0.31	1.00 ± 30.60
HT	1.48	-48.48	0.61	-48.48 ± 60.60
LO	0.52	48.43	0.19	48.43 ± 19.12
BK	1.23	-22.79	0.32	-22.79 ± 31.81
RE	0.77	23.35	0.23	23.35 ± 23.06
ET	1.02	-2.30	0.23	-2.30 ± 22.57
Weighted Average Value				-2.04 ± 10.02

in most of the industry sectors except for LO and RE. Furthermore, the overall percent effectiveness is between -12.07 and 7.98, which indicates that it might not helpful to improve the country-wide security environment. Taken together, this implies that, if the government seeks to enforce a CSO employment on firms, it might be better to implement the policy only to firms in a specific industry sector such as LO and RE.

Scenario 3: Selecting the Most Effective Security Measure

Another possible scenario is a situation where the government seeks to select the most effective security measure from various alternative ones. For instance, the government may want to compare the effectiveness of various security measures and to select one with the highest effectiveness in reducing country-wide security incidents, prior to the imposition.

Here, I assume that a confounding factor is the size of a firm measured by the number of employees (see <Table 1> for the details). I consider that there are three alternative security measures that the government has in mind: security training, official security policy and official information security department. These are all expensive from firms'and social points of view and the effectiveness of these securitymeasures is largely unknown. The government therefore needs to carefully identify which security measure is most effective for mitigating security risks, before the selection of a security measure to be imposed.

From <Table 4>, it can be identified that security training has the highest effectiveness in reducing security incidents caused by software virus infection. More specifically, while imposing a firm to have its official security policy is effective for mitigating security risks of firms with different sizes, firms with a large workforce (i.e., more than 250 employees) might experience no improvement in their security. Similarly, enforcing the establishment of an official security department would not increase the effectiveness of security for all firms, particularly firms with more than 50 employees. These results imply that, if a security policy is not imposed carefully, it might not only be

〈Table 4〉 Estimated Percent Effectiveness of Various Security Measures

Firm Size	Security Training	Security Policy	Security Department
1	33.46 ± 16.70	23.95 ± 15.33	32.20 ± 18.47
2	36.84 ± 11.81	20.46 ± 12.93	11.79 ± 18.22
3	30.71 ± 13.26	17.04 ± 14.52	-0.56 ± 20.65
4	26.63 ± 15.69	8.62 ± 22.37	-22.93 ± 30.14
Weighted Average Value	32.21 ± 7.00	18.60 ± 7.70	5.80 ± 10.72

waste of social resources but also even undermine the overall security.

5. Conclusions

This study intends to develop a simple ex ante evaluation method that can estimate the potential effectiveness of a government enforced security measure in reducing industry-wide or country-wide security risks. Specifically, my approach seeks to identify how many security risks can be reduced if all firms currently without a specific security measure are enforced to employ the measure by the government. This is an important question to be answered before the government enacts any security rules and regulations. The benefits of using this method would be that 1) it does not require detailed information on security measures and accidents, 2)it can be easily applied and understood by a policy-maker and 3) it can produce an industry- or country-level estimate using firm-level data.

While the Korean government is one of the most proactive countries in cyber-security and has enacted various security regulations, ex ante and ex post evaluation methods for estimating the effectiveness of the regulations in reducing security risks are not likely to be well taken into account by the government. Furthermore, even in the field of cyber-security, these evaluation methods are not well studied. By applying a method developed and used in a series of studies for measuring the effectiveness of mandatory seatbelt wearing, this study would present a way to evaluate the potential effectiveness of a government enforced security measure before its implementation.

Using actual data obtained from KISA, the scenarios provide examples of how to estimate the effectiveness of a security measure if it is enforced by the government. It is shown that, if a policy-maker or regulator has only limited data on various security-related parameters and targets a specific security risk, the method offered in the study could be a valid technique that provides him/her with guidance for selecting a security measure that can be most effective in mitigating the specific security risk.

However, some words of caution are in order. First, as previously stated, there could be a question on whether a security incident can be regarded as equivalent to a motor vehicle fatality. While a consequence of a car accident can be considered to have binary outcomes (i.e., survive vs. die), a result of a security incident may be diverse depending on, for example, a firm size, an industry type and a launched attack which causes an incident. Similarly, while seatbelt wearing can be regarded to have binary values (i.e., wear vs. not wear), a security measure may be adopted and tailored differently by different industries and firms. As a result, the estimation should be used with caution (i.e., for ini-

tial ex ante evaluation). Notwithstanding the limitation, the method can be very useful to get an insight on the effectiveness of the security measure in a case where detailed information on security measures and incidents is rare and difficult to obtain as a firm tends to hesitate to share information regarding security measures and incidents.

Second, while the method proposed in this study can also use a combination of various confounding factors (e.g., combining firm sizes, industry sectors and other characteristics of firms), this may result in an issue: if some values in a category of a combination of confounding factors are zero, a risk ratio cannot be obtained and therefore the percent effectiveness cannot be estimated. In addition, in presenting the scenarios, a panel data perspective cannot be taken into account since it was not verifiable whether a security incident was occurred before or after implementation of a security measure. These limitations can however be overcome as more and more observations become available (e.g., combine more observations and adopt a panel data perspective from the KISA's subsequent surveys).

References

[1] Bort, J., "Security Blogger Brian Krebs Is Trying To Track Down The Target Hacker By Talking To Suspected Credit Card Thieves," in Business Insider, ed. New York, NY: Business Insider Inc., 2013.

[2] Bratus, S., "Hacker curriculum: How hackers learn networking," IEEE Distributed Systems Online, Vol. 10, p. 2, 2007.

[3] Chipman, M. L., Li, J., and Hu, X., "The effectiveness of safety belts in preventing fatalities and major injuries among school-aged children," in Annual proceedings of the Association for the Advancement of Automotive Medicine, 1995, pp. 133-145.

[4] Colwill, C., "Human factors in information security: The insider threat - Who can you trust these days?," Information security technical report, Vol. 14, No. 4, pp. 186-196, 2009.

[5] D'Arcy, J., Hovav, A., and Galletta, D., "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," Information Systems Research, Vol. 20, No. 1, pp. 79-98, 2009.

[6] Eminağaoğlu, M., Uçar, E., and Eren, Ş., "The positive outcomes of information security awareness training in companies-A case study," information security technical report, Vol. 14, No. 1, pp. 223-229, 2009.

[7] Evans, L., "Double pair comparison-a new method to determine how occupant characteristics affect fatality risk in traffic

crashes," Accident Analysis & Prevention, Vol. 18, No. 3, pp. 217-227, 1986.

[8] Evans, L., "The effectiveness of safety belts in preventing fatalities," Accident Analysis & Prevention, Vol. 18, No. 3, pp. 229-241, 1986.

[9] Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Sohail, T., "The impact of the Sarbanes-Oxley Act on the corporatedisclosures of information security activities," Journal of Accounting and Public Policy, Vol. 25, No. 5, pp. 503-530, 2006.

[10] Hoo, K. J. S., "How much is enough? A risk management approach to computer security," Consortium for Research on Information Security Policy (CRISP) Working Paper, Stanford University, 2000.

[11] Johnson, V. R., "Cybersecurity, Identity Theft, and the Limits of Tort Liability," South Carolina Law Review, Vol. 57, pp. 255-311, 2005.

[12] Kim, R., "Card firms may see over W1 tril. in losses," in The Korea Times, ed. Seoul, Korea: The Korea Times, 2014.

[13] KISA, "2007 Korean Information Security Survey," Korean Internet & Security Agency, Seoul, Korea, 2007.

[14] KISA, "2008 Korean Information Security Survey," Korean Internet & Security Agency, Seoul, Korea, 2008.

[15] Lee, C.-S. and Park, W., "Enhancing industrial security management system for multimedia environment," Forthcoming in Multimedia Tools and Applications.

[16] Merete Hagen, J., Albrechtsen, E., and Hovden, J., "Implementation and effectiveness of organizational information security measures," Information Management & Computer Security, Vol. 16, No. 4, pp. 377-397, 2008.

[17] 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.

[18] Robertson, L. S., "Estimates of motor vehicle seat belt effectiveness and use: implications for occupant crash protection," American Journal of Public Health, Vol. 66, No. 9, pp. 859-864, 1976.

[19] Schneier, B., "Computer security: It's the economics, stupid," in 1st Workshop on Economics of Information Security, Barkeley, CA, 2002.

[20] Shim, W., "Analysis of the Impact of Security Liability and Compliance on a Firm's Information Security Activities," The Journal of Society for e-Business Studies, Vol. 16, No. 4, pp. 53-73, 2011.

[21] Varian, H., "Managing online security risks," in New York Times, ed. New York, N.Y., 2000.

[22] Yonhap News, "Personal data of 12 million KT customers stolen: police," in Yonhap News, ed. Seoul, Korea: Yonhap News Agnecy, 2014.

저 자 소 개

Woohyun Shim	(E-mail: shim.woohyun@unitn.it)
2010	Ph.D., Department of Media and Information, Michigan State University
2011~2012	Senior Researcher, Synthesys, Inc., East Lansing, Michigan, US
2012~present	Research Fellow, Department of Information Engineering and Computer Sciences, University of Trento, Trento, Italy
Research interests	Quantitative and qualitative socio-economic analysis of cyber-security, Security management strategy and policy, ICT innovation and governance arrangements