Asia Pacific Journal of Information Systems
Vol. 21, No. 4, December 2011

Vulnerability and Information Security Investment Under Interdependent Risks: A Theoretical Approach*

Woohyun Shim**

This article explores economic models that show the optimal level of information security investment in the presence of interdependent security risks. Using particular functional forms, the analysis shows that the relationship between the levels of security vulnerability and the levels of optimal security investments is affected by externalities caused by agents' correlated security risks. This article further illustrates that, compared to security investments in the situation of independent security risks, in order to maximize the expected benefits from security investments, an agent should invest a larger fraction of the expected loss from a security breach in the case of negative externalities, while an agent should spend a smaller fraction of the expected loss in the case of negative externalities.

Keywords : IS Management, Information Security Investment, Security Vulnerability, Interdependent Security Risk, Externalities, Cyber Attacks

* The author appreciates comments and suggestions from Lawrence Gordon, Martin Loeb at the University of Maryland, and Steve Wildman and Johannes Bauer at Michigan State University.

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

I. Introduction

Given the increased interconnectivity of the new Internet-based economy, the protection of intangible information assets has become as crucial as the protection of other tangible traditional assets [Gordon and Loeb, 2002]. Firms have increased their spending on information security and have employed an increased amount of security solutions to protect information systems [Zhao *et al.*, 2009]. Despite the enhanced quality and quantity of security solutions, various types of new cyber attacks have been continuously evolving and the number of security breaches has, correspondingly, continued to increase [Majuca *et al.*, 2006]. This implies that, as Gordon and Loeb [2002] stated, even if many firms have increased their investments in the security of information systems, the investments are not adequately allocated to protect information systems efficiently. This inadequacy of the investments leaves organizations significantly vulnerable to cyber threats.

One of the main reasons for inadequate security investment that has drawn a great deal of recent attention from an economic perspective is interdependent security risk. Because of integrated and interconnected information systems, an organization's decisions regarding security investment not only affect its security risks but also those of others [Grance *et al.*, 2002; Varian, 2004; Zhao *et al.*, 2009]. According to Anderson [2001], Kunreuther and Heal [2003], Ogut *et al.* [2005] and Zhao *et al.* [2010], the interdependent nature of information security risks distorts the decisions of economic parties about investment in information security. They argued that when interdependent information security risks cause positive externalities, firms are likely to invest less in information security than the socially optimal level. On the other hand, they also illustrated that when interdependent security risks generate negative externalities, firms are like to invest more than the socially optimal level. As a result, interdependent information security risks make it difficult to achieve the socially optimal level of security investment from a social planner's viewpoint.

The main interest of this study is this interdependent feature of information security risks. Unlike the previous literature which mostly focused on independent information security risks, the aim of this study is to develop an economic model that sheds light on the relationship between an organization's security vulnerability and its information security investment in the situation of interdependent security risks. By expanding the analytical modeldeveloped by Gordon and Loeb [2002] (hereinafter referred to as the 'G-L model'), this study integrates the interdependent nature of information security risks into Gordon and Loeb's model and explores how interdependent risks affect the analysis resulting from their model.

The remainder of the study is organized as follows. The next section, section 2, reviews the G-L model. In the third section, I discuss the theoretical model developed here that includes the characteristics of interdependent security risks based on the G-L model, and derive a number of new propositions that shows the effects of interdependent security risks on security investment strategies. Discussion and implication of the study are presented in the concluding fourth section.

Ⅱ. The G-L Model: Independent Information Security Risks

In this section, I review the G-L model which investigates the relationship between a vulnerability level and a level of information security investment in the case where security risks are independent. In the G-L model, Gordon and Loeb [2002] showed how vulnerability affects the additional investment in information security for a given information set. They considered a one-period economic model of identical risk-neutral firms with the expected or potential monetary loss conditioned on a breach occurring, the vulnerability of the information set, and the monetary investment in information security. In more detail, firm i's potential loss, L_i, is the product of the probability of a threat occurring and the monetary loss conditioned on a security breach; the vulnerability, v_i, is firm i's probability that an attempted attack of the given information set would be breached[1]; and the investment, z_i, is firm i's pecuniary investment in information security to reduce the probability that an attempted breach of the given information set will be successful. z_i is assumed to have the same unit with the potential loss, L_i. In addition, in the G-L model, firm i's security breach probability function, denoted by $B_i(z_i, v_i)$, is defined as the probability that firm i's information set with vulnerability, v_i, will be breached given that firm i has made an information security investment of z_i to protect that information. $B_i(\cdot)$ is assumed to be continuously twice differentiable and to have declining returns with respect to z_i (i.e., $B_i'(\cdot) < 0$ and $B_i''(\cdot) > 0$). Note that, for notational simplicity, the subscript, i, is omitted.

In order to determine the optimal level of information security investment, the model solved the maximization problem of the expected net benefit function from an information security investment. That is,

$$\max_z [v - B(z, v)]L - z \qquad (1)$$

where $[v - B(\cdot)]L$ is the expected benefit of an investment in information security and z is the cost of the investment.[2] The first-order condition for an information security investment, therefore, is

$$-B'(z^*, v)L = 1 \qquad (2)$$

which shows, on the left hand side, the marginal benefits from IT security investment, equals, on the right hand side, the marginal cost of the investment. This implies that a firm can maximize the expected net benefits of information security investment when the difference between benefits and costs are maximized. z^* denotes the value which solves this maximization problem.

Since the optimal security investment equals zero if the marginal benefits are less than or equal to the marginal costs of the investment, it can

1) Following Gordon and Loeb [2002], this study assumes that $0 < v_i < 1$ since completely invulnerable information (i.e., $v_i = 0$) such as perfectly unachievable information is not only undesirable but also very costly to be achieved, and it is not necessary to protect completely vulnerable information (i.e., $v_i = 1$) such as public information.

2) According to Gordon and Loeb [2002], this is the expected net benefits from an investment in information security.

be identified from equation (2) that:

$$L \leq \frac{1}{-B'(0,\ v)} \tag{3}$$

Since equation (2) does not provide further insights regarding the relationship between the levels of security vulnerability and investment, the G-L model employed two broad classes of security breach probability functions, which make it possible to identify a closed form solution for z^*. The model first considered the first class of security breach probability functions (hereinafter referred to as 'Class I') which is given by:

$$B^{I}(z,\ v) = \frac{v}{(\alpha z+1)^{\beta}} \tag{4}$$

where both the parameters, α and β, are the productivity measures of information security ($\alpha > 0$ and $\beta \geq 1$). Therefore, as α and/or β increases, the probability of a security breach becomes lower. The superscript I on $B(z,\ v)$ indicates the case in which security breach probability functions belong to Class I. Using equation (4), the first order condition given by equation (2) can be changed to a closed form and therefore the optimal security investment level denoted by z^{I^*} can be expressed as[3]:

$$z^{I^*} = \frac{(v\alpha\beta L)^{\frac{1}{(\beta+1)}} - 1}{\alpha} \tag{5}$$

From equation (3), it can be identified that z^{I^*} equals zero when $0 \leq v \leq 1/\alpha\beta L$, and increases at a decreasing rate (see <Figure 1>). As a result, a firm which has a breach probability function belonging to this class would be better off increasing its security investment as security vulnerability increases. The G-L model also examined the second class of security breach probability functions (hereinafter referred to as 'Class II'). This class of security breach probability functions has the characteristic that, as the vulnerability of information set becomes extremely large, the protection of the information set can only be achieved at an extremely high cost. Therefore, the optimal investment in information security first increases and then decreases in vulnerability. Gordon and Loeb [2002] proposed the second class of security breach probability functions as:

$$B^{II}(z,\ v) = v^{\alpha z+1} \tag{6}$$

where α denotes the productivity of information security ($\alpha > 0$). Using equation (2), the expression for the optimal level of security investment for Class II can be expressed as[4]:

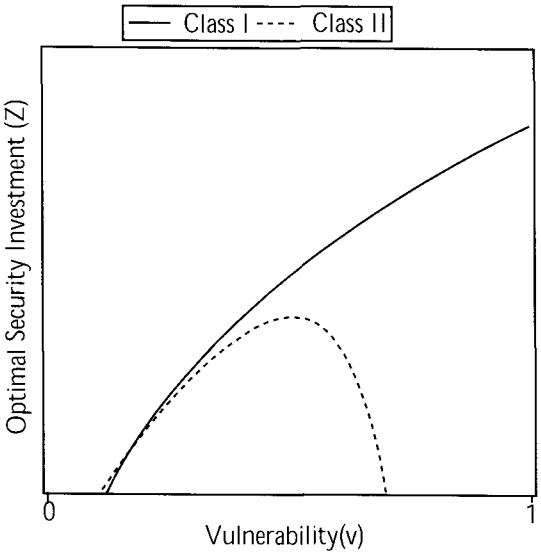
$$z^{II^*}(v) = \frac{\ln\left(\frac{1}{-\alpha v L(\ln v)}\right)}{\alpha \ln v} \tag{7}$$

For this class, equation (3) can be reorganized into $1/L > -\alpha v \ln v$. By plotting equation (7), the optimal security investment level can be presented as shown in <Figure 1>. Unlike the first class of security breach probability functions with constantly (weakly) increasing optimal investment level, the second class of security breach probability functions achieves the optimal

3) Note that $B^{I'}(\cdot) = \frac{\alpha\beta v}{(\alpha z+1)^{\beta+1}}$.

4) Note that $B^{II'} = \alpha v^{(\alpha z+1)} \ln v$.

level of security investment, which is first increasing and then decreasing in the vulnerability.



<Figure 1> Optimal level of security investments for Class I and II (Adapted from Gordon and Loeb [2002])[5]

Ⅲ. The Extended Model: Interdependent Information Security Risks

3.1 Interdependent Security Risks

Many researchers, including Grance *et al.* [2002], Ogut *et al.* [2005] and Zhao *et al.* [2009], have argued that, despite the masive investments in information security, a residual risk still remains because of the existence of the interdependence of information security risks: an agent's investment in information security affects its own security risks as well as those of other agents [Grance *et al.*, 2002; Zhao *et al.*, 2009].

This interdependent feature of information security risks causes externalites in various contexts. First, an agent's investment in information security may generate a positive externality problem to other agents: an agent's increased information security by investing more in the security may decrease the security risks faced by the firm's business partners via its computer network [Ogut *et al.*, 2005]. In contrast, an agent's security investment may also cause negative externalities to other agents: an agent's increased level of information security may divert attacks to other agents, and hence raise the security risks of other agents [Zhao *et al.*, 2009]. Therefore, one conclusion that the previous literature has reached is that self-interested agents are likely to either under-invest in information security (i.e., positive externalities) or over-invest in information security (i.e., negative externalities) [Camp and Wolfram, 2000; Lakdawalla and Zanjani, 2005; Muermann and Kunreuther, 2008; Zhao *et al.*, 2009].

The Extended G-L Model Considering Interdependent Security Risks

I now expand the case of independent security risks used in the G-L model to the case of interdependent security risks. With interdependent security risks, a firm's information security risks are often correlated with those of others [Zhao *et al.*, 2009]. This characteristic of interdependent security risks generates either positive or negative externalities onto firms' security investments. First, a firm's security investment often generates negative externalities such as the case where cyber attacks targeted at a highly secured server are diverted to other servers, and hence increase

5) For this figure, I use $\alpha = 0.00001$, $\beta = 2$ and $L = 400,000$.

the risks of other firms. In contrast, a firm's security investments can also generate positive externalities onto other firms. For example, if a firm raises its level of information security by investing more in technical security solutions, it may lower the chances of security breaches of the firm's business partners via its computer network.

I first consider Class I security breach probability functions in the case of interdependent security risks. In order to simplify the model, I assume there are only two symmetric firms (i.e., $i=1, 2$) with a single period. If information security investments result in negative externalities, firm 1's higher security investment than the investment of firm 2 is likely to drive away attacks on it. In contrast, if firm 1 invests less than does firm 2, firm 1 is more likely to attract attacks than is firm 2. Therefore, following Zhao [2007], I use the term z_1/z_2 to characterize the relative effectiveness of firm 1's security investment and model the breach probability function as:

$$B_1(z_1, z_2, v_1) = p_1\left(z_1 \cdot \frac{z_1}{z_2}, v_1\right) \quad (8)$$

where $p_i(\cdot)$ is assumed to have the same properties with $B_i(\cdot)$, that is, $p_i'(\cdot) < 0$ and $p_i''(\cdot) > 0$. This probability function implies that, if firm 1 makes a higher level of information security than does firm 2 (i.e., $z_1/z_2 > 0$), firm 1's security investment is more effective in decreasing its probability of a security breach. Therefore, from equation (8), the first class of security breach probability functions given by equation (4) can be rewritten by:

$$B_1^I(z_1, z_2, v_1) = \frac{v_1}{\left\{\alpha\left(z_1 \cdot \frac{z_1}{z_2}\right)+1\right\}^{\beta}} \quad (9)$$

By assuming firm 1 and firm 2 are identical, the first-order condition of equation (2) can be expressed by[6]:

$$z_1^{I^*}(v_1) = \frac{(2\alpha\beta v_1 L_1)^{\frac{1}{\beta+1}} - 1}{\alpha} \quad (10)$$

In contrast, there can be the case where security risks are interdependent and information security investments generate positive externalities: a firm's security investment for protecting systems against cyber attacks can reduce not only its probability of a security breach, but also that of others. To consider this situation, again, I assume that there are two symmetric firms with interdependent risks ($i=1, 2$). I model the positive externalities by classifying the effects of security investment into direct effects and indirect effects following Ogut *et al.* [2005] and Zhao *et al.* [2009]. Direct effects refer to the effects of a firm's security investment on its own breach probability function, whereas indirect effects refer to the effects of other firms'security investments on the firm's breach probability. To model indirect effects, I use the parameter δ which measures the degree of interconnection between the two firms' information systems ($0 \le \delta \le 1$). A higher δ indicates a higher degree of interconnection. Therefore, the breach probability function for firm 1 can be expressed by:

$$B_1^I(z_1, z_2, v_1) = p_1(z_1 + \delta z_2, v_1) \quad (11)$$

6) Note that $B_1^{I'} = 1 - \frac{2\alpha\beta v_1 (z_1/z_2)}{\{\alpha(z_1^2/z_2)+1\}^{\beta+1}}$. Hence, when firm 1 and 2 are identical, $B_1^{I'} = -\frac{2\alpha\beta v_1}{(\alpha z_1 + 1)^{\beta+1}}$.

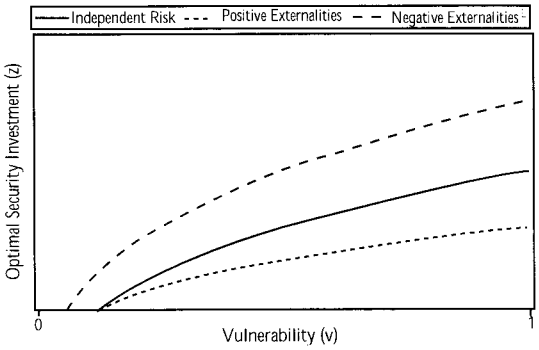
From this equation, the first class of security breach probability functions given by equation (4) can be rewritten by:

$$B_1^I(z_1, z_2, v_1) = \frac{v_1}{\{\alpha(z_1+\delta z_2)+1)\}^\beta} \quad (12)$$

When firm 1 and firm 2 are identical, the optimal level of security investment is the solution to the following equation[7]:

$$z_1^{I^*}(v_1) = \frac{(\alpha\beta v_1 L_1)^{\frac{1}{\beta+1}} - 1}{\alpha(1+\delta)} \quad (13)$$

In order to get insights into the relationship among the optimal levels of investments in information security and vulnerability, I confer numerical values on α, β, δ and L_1, and plot $z_1^{I^*}(v_1)$ in equations (10) and (13) as shown in <Figure 2>.[8] For this first class of security breach probability functions, condition (3) yields $z_1^{I^*}(v_1) = 0$ for $0 \le v_1 \le 1/2\alpha\beta L_1$ if information security investments generate negative externalities, and for $0 \le v_1 \le \alpha\beta L_1$ if information security investments generate positive externalities or if information security risks are independent. It should be noted that, in the case of positive externalities, as δ approaches to zero, the optimal security investment level approaches to the line of the independent security risk case.



<Figure 2> Optimal level of Security Investments for Class I by the Types of Security Risks

I now consider the second class of security breach probability functions in the case of interdependent security risks. Employing the same notations used above, if firm 1's security investment cause negative externalities, the breach probability function presented in equation (6) can be rewritten as:

$$B_1^{II}(z_1, z_2, v_1) = v_1^{\left\{\alpha\left(z_1 \cdot \frac{z_1}{z_2}\right)+1\right\}} \quad (14)$$

By assuming firm 1 and firm 2 are identical, the first-order condition of equation (2) can be presented by[9]:

$$z_1^{II^*}(v_1) = \frac{\ln\left(\frac{1}{-2\alpha v_1 L_1(\ln v_1)}\right)}{\alpha \ln v_1} \quad (15)$$

In contrast, if information security investments result in positive externalities, the second class of the security breach probability functions can be rewritten using equations (6) and (11) as:

7) Note that $B_1^{I'} = -\frac{\alpha\beta v_1}{\{\alpha(z_1+\delta z_2)+1\}^{\beta+1}}$. Hence, when firm 1 and firm 2 are identical, $B_1^{I'} = -\frac{\alpha\beta v_1}{(\alpha z_1(1+\delta)+1)^{\beta+1}}$.

8) Iuse $\alpha = 0.0001$, $\beta = 2$, $\delta = 0.7$ and $L_1 = 400{,}000$ for the illustrative purpose.

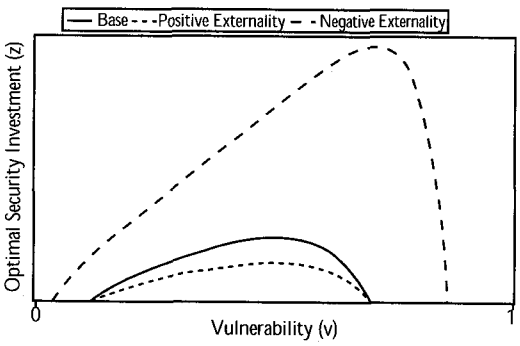
9) Note that $B_1^{II'} = 2\alpha \cdot \frac{z_1}{z_2} v_1^{\left\{\alpha\left(z_1 \cdot \frac{z_1}{z_2}\right)+1\right\}} \ln v_1$ and, if firm 1 and 2 are identical, $B_1^{II'} = 2\alpha v_1^{(\alpha z_1+1)} \ln v_1$.

$$B_1^{II}(z_1,\ z_2,\ v_1) = v_1^{\alpha(z_1+\delta z_2)+1} \quad (16)$$

When firm 1 and firm 2 are identical, the optimal level of security investment is the solution to the following equation[10]:

$$z_1^{II*}(v_1) = \frac{\ln\left(\frac{1}{-\alpha v_1 L_1(\ln v_1)}\right)}{\alpha(1+\delta)\ln v_1} \quad (17)$$

In order to compare the optimal levels of information security investment for the second class of security breach probability function in case of the different types of the externalities, I confer numerical values on α, δ and L_1 in equations (7), (15) and (17) and plot them as shown in <Figure 3>.[11] Although one cannot find a close form expression for a lower and upper limit of v_1 which yields $z_1^{II*}(v_1)=0$, by plotting $z_1^{II*}(v_1)$ with the conferred numerical values, it can be identified that the area of zero investment in the case of negative externalities is smaller than those of other cases.



<Figure 3> Optimal level of security investments for Class II by the Types of Security Risks

The analysis identifies several important points. First, as shown in <Figure 2> and <Figure 3>, if information security investments generate negative externalities, the area of zero security investment is different with the other cases: for the first class of security breach probability functions, equations (3) and (10) yield $z_1^{I*}(v_1)=0$ for $0 \le v_1 \le 1/2\alpha\beta L_1$ while equations (3), (5) and (13) yield $z_1^{I*}(v_1)=0$ for $0 \le v_1 \le \alpha\beta L_1$. For the second class of security breach probability functions, we cannot identify a close form expression for a lower and upper limit of v_1 which brings in $z_1^{II*}(v_1)=0$. However, as shown in <Figure 3> generated by the conferred numerical values, the range of zero investment in the case of negative externalities is narrower than those of other cases.[12] This observation is stated in the following proposition.

Proposition 1: Suppose security risks are interdependent and information security investments generate negative externalities, then the area of zero investment (i.e., $z_1^{I*}(v_1)=0$ and $z_1^{II*}(v_1)=0$) is smaller comparing to the other cases.

This proposition implies that, although information sets have either extremely low or high vulnerability, information security investment with negative externalities can be justified because the marginal benefits of expending money on information security of this area is relatively high compared to the other cases.

10) Note that $B_1^{II'} = \alpha v_1^{\{\alpha(z_1+\delta z_2)+1\}} \ln v_1$ and, if firm 1 and 2 are identical, $B_1^{II'} = \alpha v_1^{\{\alpha(1+\delta)z_1+1\}} \ln v_1$.

11) Iuse $\alpha = 0.00001$, $\delta = 0.7$ and $L_1 = 400{,}000$ for the illustrative purpose.

12) Using the conferred numerical values, it is identified that, in the case of negative externalities, $z_1^{II*}(v_1)=0$, when $0 < v_1 < 0.038$ or $0.866 < v_1 < 1$, while $z_1^{II*}(v_1)=0$, when $0 < v_1 < 0.116$ or $0.669 < v_1 < 1$ in the other cases.

Second, in addition to the impact on the size of zero investment area, interdependent security risks affect the optimal level of investment in information security as shown in <Figure 3> and 4: if security investments generate negative externalities, the optimal security investment is higher than or equal to the other cases, whereas the optimal level of security investment is lower than or equal to the other cases if security investments bring in positive externalities. This relationship between the optimal level of investment in security and interdependent security risks can be stated as:

Proposition 2: The optimal level of investment in the case of negative externalities is higher than or equal to the optimal level of investment in the case of independent security risks, while the optimal level of investment in the case of positive externalities is lower than or equal the optimal level of investment in the case of independent security risks (See Appendix for a formal proof).

The next proposition provides insight into the relationship between the optimal level of investment in security and the loss that would be expected in the absence of any investment in security when the security breach probability functions belong to class I or class II.

Proposition 3: Suppose information security risks are interdependent, then, regardless of the classes of security breach probability functions, $z_1^*(v_1) < 2(e^{-1})v_1L_1$ if information security investments generate negative externalities, and $z_1^*(v_1) < (1+\delta)^{-1}(e^{-1})v_1L_1$ if information security investments generate positive externalities (A formal proof appears in the appendix).

This proposition indicates that, compared to the maximum investment level, 36.97% of the loss, in the G-L model, the maximum information security investment in the case of negative externalities is less than or equal to 73.58% of the loss that would be expected in the absence of any investment in security. In contrast, in the case of positive externalities, the maximum security investment is always less than or equal to $(1+\delta)^{-1} \cdot 36.97\%$ of the loss.[13]

Consequently, the analysis presented here can be summarized as follows: The optimal amount of information security investment, under the cases where interdependent risks exist, differs from the investment with independent risks of information security. While the interdependent risks with positive externalities cause lower investment in information security, the interdependent risks with negative externalities cause higher investment in information security, compared to the independent risks. Furthermore, for two broad classes of security breach probability functions, while the optimal investment in information security should not exceed 36.97% of the expected loss due to a security breach in the case of G-L model (i.e., independent security risks), under interdependent security risks, the optimal amount of security investment should not exceed 73.58% of the expected loss in the case of negative externalities and $(1+\delta)^{-1} \cdot 36.97\%$ of the expected loss in the case of positive externalities. Lastly, if negative security externalities exist, for both Classes I and II, firms start to make the information security investment at the lower vulnerability level than the other cases, and for

13) For example, if $\delta = 0.5$, the optimal security investment is lower than or equal to 24.64% of the loss.

class II, the firms stop investing in information security at the higher vulnerability level than the other cases. For the positive externality case, firms reduce the amount of information security investment as the level of interconnection increases.

Ⅳ. Conclusion and Future Work

The rapid development of networking technologies has been important enablers of highly productivity business processes. However, as organizations become more reliant on these technologies, they become highly susceptible to information security breaches and associated losses. Therefore, the protection of information assets has become at least as critical as is the protection of traditional tangible assets [Gordon and Loeb, 2002]. While a growing body of research has studied the issues of information security from a technical point of view, only limited research primarily based on economic perspectives has been conducted in the field of information security (e.g., Anderson, 2001; Anderson and Moore, 2006; Anderson *et al.*, 2007; Camp and Wolfram, 2000; Gordon and Loeb, 2002; Varian, 2000]. Moreover, despite the importance of taking account of unique aspects of information security (e.g., misaligned incentives and interdependent security risks) in the research, these aspects have not been fully incorporated.

This study built on Gordon and Loeb's study and developed a conceptual framework to derive an optimal level of information security investment, when interdependent aspects of information security risks are taken into account, in the form of an economic model for information security investment decisions. More specifically, in the context of extending the G-L model, this study addressedthe unique phenomenon of information security by presenting a model of information security as a decision of a firm to invest in information in a world of interconnected firms. Two phenomena, termed externality problems, were considered: a positive externality exists when the investment in information security by a firm decreases the overall threat of a breach for other firms; a negative externality exists when the investment in information security by a firm increases attacks on other firms with lesser security. An economic model was developed and analyzed to show how positive and negative externalities caused by information security investments affect the behavior of the optimal security investment that should be devoted to securing information.

In addition to the support of the economic framework developed by Gordon and Loeb [2002], the analysis conducted in this study has shown that, for the case of negative externalities, the optimal investment in information security is higher than or equal to the optimal investment in the case of independent security risks, whereas the optimal spending on information security is lower than or equal to that of the independent security risk case. The analysis also demonstrated that, for the negative externality case, the area of no spending on information security is smaller than the area of zero investment in the case of the G-L model, while the area of zero investment in information security for the positive externality case has the same size with the case of the G-L model. This implies that, for the negative externality case, security investment in either extremely low or highly vulnerable information as-

sets might be justifiable while the investments in the other cases might be not.

Furthermore, the analysis shows that, compared to the optimal security investment in the G-L model which does not exceed 37% of the expected loss resulting from a security breach, the optimal amount to spend on information security does not exceed 73.58% of the expected loss for the negative externality case and $(1+\delta)^{-1} \cdot 36.97\%$ of the expected loss for the negative externality case. Therefore, the optimal spending on information security would be just little less than even the expected loss from a security breach for the negative externality case and far less than the than the expected loss for the positive externalities.

From the findings of the analysis, several interesting implications emerge. The primary implication of the analysis is that a collective effort is critical to reduce externality problems caused by interdependent security risks. Sharing security information by firms appears to be one of the most frequently mentioned options by authors (e.g., Gordon *et al.*, 2002, 2003; Gal-Or and Ghose, 2005; Hausken, 2007). They argued that, since information sharing can help firms avoid security incidents similar to those experienced by other firms, it can facilitate avoiding over- and underinvestment problems in information security and obtaining socially optimal information security investments. Due to unobservability of security related activities and potential costs of information sharing (e.g., damage to reputation and loss of consumer loyalty), however, firms tend to hesitate to share security related information with other firms. In setting mechanisms for sharing security information, therefore, appropriate incentives including financial rewards should be provided to firms for sharing security information.

The analysis also generates important implications for the policy makers regarding information security issues.As noted by authors such as Schneier [2002] and Varian [2000], liability and compliance rules can be very useful for mitigating security problems. Accordingly, there has been a growing number of cyber liability regulations enacted by a government. While the cyber liability regulations required firms to comply with a higher legal standard, these regulations do not seem to take interdependence of information security risks into account. For example, the Korean e-Financial Transaction Act (EFTA) adopted in 2006 prescribed only firms in the financial and insurance industry to exercise due care in electronic financial transactions and to comply with certain security standards in order to protect the customer information. However, due to interdependent security risks, the exclusion of firms not in the financial and insurance industry from EFTA might hinder firms in making socially optimal security investments: one possible scenario is that higher security requirements of EFTA for financial institutions and service providers lead those firms to overinvest in information security, while firms which are not targeted by EFTA underinvest in information security. Consequently, in order to obtain a better social outcome and a sound security environment, cyber liability regulations might be required to take interdependent security risks into account, and hence to target the wider range of firms in various industries.

While the findings shed significant light on the much unseen issue of information security investment in the case of interdependent security risks, this study has some limitations and has opportunities for expanding this study. First, sim-

ilarly with Gordon and Loeb [2002], the analysis is based on the specific functional form of the security breach functions. According to Willemson [2006], there is no reason to consider that two specific functional forms used in the G-L model correspond to any real vulnerability scenario. Therefore, it should be examined whether or not the propositions are generalizable, or other forms of probability functions of security breaches generate similar results with this study. Second, while the paper extends an aspect of Gordon and Loeb [2002] by takingpositive and negative externalities caused by interdependent security risks into account, it examines the externality problems in the separate models. Thus, a model in which the positive and negative externalities are combined should be analyzed in the future study. Lastly, empirical assessment that investigates whether or not firms' information security investments are consistent with the findings of this article should be conducted. In addition, while the single period model with identical firms provides useful insights regarding the relationships between information security investments and security vulnerability in the context of interdependent security risks, including dynamic aspects of firms' security investment strategies would enrich my economic model.

⟨References⟩

[1] Anderson, R., "Why Information Security is Hard An Economic Perspective," *Paper presented at the 17th Annual Conputer Security Applications Conference*, New Orleans, LA, 2001.

[2] Anderson, R. and Moore, T., "The Economics of Information Security," *Science*, Vol. 314, No. 5799, 2006, pp. 610-613.

[3] Anderson, R., Moore, T., Nagaraja, S., and Ozment, A., "Incentives and Information Security," In N. Nisan, T. Roughgarden, E. Tardos and V. Vazirani (Eds.), *Algorithmic Game Theory*, Cambridge University Press, 2007, pp. 631-647.

[4] Camp, L.J. and Wolfram, C., "Pricing Security," *Paper presented at the The CERT Information Survivability Workshop*, Boston, 2000.

[5] Gal-Or, E. and Ghose, A., "The Economic Incentives for Sharing Security Information," *Information Systems Research*, Vol. 16, No. 2, 2005, pp. 186-208.

[6] Gordon, L. and Loeb, M., "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, Vol. 5, No. 4, 2002, pp. 438-457.

[7] Gordon, L., Loeb, M., and Lucyshyn, M., "An Economics Perspective on the Sharing of Information Related to Security Breaches: Concepts and Empirical Evidence," *Paper presented at the First Workshop on the Economics of Information Security*, Berkeley, CA, 2002.

[8] Gordon, L., Loeb, M., and Lucyshyn, M., "Sharing Information on Computer Systems Security: An Economic Analysis," *Journal of Accounting and Public Policy*, Vol. 22, No. 6, 2003, pp. 461-486.

[9] Grance, T., Hash, J., Peck, S., and Smith, J., "Security Guide for Interconnecting Information Technology Systems," *NIST Special Publication*, 2002, pp. 800-847.

[10] Hausken, K., "Information Sharing Among Firms and Cyber Attacks," *Journal of Account-*

ing and Public Policy, Vol. 26, No. 6, 2007, pp. 639-688.

[11] Kunreuther, H. and Heal, G., "Interdependent Security," *Journal of Risk and Uncertainty*, Vol. 26, No. 2, 2003, pp. 231-249.

[12] Majuca, R.P., Yurcik, W., and Kesan, J., "The Evolution of Cyberinsurance," *In ACM Computing Research Repository (CoRR), Technical Report cs.CR/0601020*, 2006.

[13] Ogut, H., Menon, N., and Raghunathan, S., "Cyber Insurance and IT Security Investment: Impact of Interdependent Risk," *Paper presented at the Fourth Workshop on the Economics of Information Security*, Cambridge, MA, 2005.

[14] Ogut, H., Raghunathan, S., and Menon, N. M., "Information Security Risk Management through Self-Protection and Insurance," *Unpublished Manuscript*, The University of Texas at Dallas, 2005.

[15] Schneier, B., "Computer Security: It's the Economics, Stupid," *Paper presented at the First Workshop on the Economics of Information Security*, Berkeley, CA, 2002.

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

[17] Varian, H., "System reliability and free riding," In L.J. Camp and S. Lewis (Eds.), *Economics of Information Security (Advances in Information Security, Volume 12)*, Dordrecht, The Netherlands: Springer, 2004, pp. 1-15.

[18] Willemson, J., "On the Gordon and Loeb Model for Information Security Investment," *Paper presented at the Fifth Workshop on the Economics of Information Security*, Cambridge, UK, 2006.

[19] Zhao, X., "Economic Analysis on Information Security and Risk Management," *Unpublished doctoral dissertation*, The University of Texas at Austin, Texas, 2007.

[20] Zhao, X., Xue, L., and Whinston, A., "Managing Interdependent Information Security Risks: An Investigation of Commercial Cyber-insurance and Risk Pooling Arrangement," *Paper presented at the Thirtieth International Conference on Information Systems*, 2009.

⟨Appendix⟩

Proof of Proposition 2: Suppose the security breach probability function belongs to class I or class II. For class I, usingthe optimal security investment levels from Equations (5), (10) and (13), we have:

$$\frac{(\alpha\beta v_1 L_1)^{\frac{1}{\beta+1}}-1}{\alpha(1+\delta)} \le \frac{(v\alpha\beta L)^{\frac{1}{(\beta_1)}}}{\alpha} \le \frac{(2\alpha\beta v_1 L_1)^{\frac{1}{\beta+1}}-1}{\alpha} \quad \text{(A.1)}$$

For class II, using the optimal levels of security investments from Equations (7), (15) and (17), we have:

$$\frac{\ln\left(\frac{1}{-\alpha v_1 L_1(\ln v_1)}\right)}{\alpha(1+\delta)\ln v_1} \le \frac{\ln\left(\frac{1}{-\alpha v L(\ln v)}\right)}{\alpha \ln v} \le \frac{\ln\left(\frac{1}{-2\alpha v_1 L_1(\ln v_1)}\right)}{\alpha \ln v_1} \quad \text{(A.2)}$$

Note that the optimal levels of information security investments of each case are same only if they are in the range of zero investment.

Proof of Proposition 3: Suppose the security breach probability function belongs to class I. Using Equation (10) for the negative externality case, we have:

$$\frac{z_1^{I^*}(v_1)}{v_1 L_1} = \frac{(2\alpha\beta v_1 L_1)^{\frac{1}{\beta+1}}-1}{\alpha v_1 L_1} \quad \text{(A.3)}$$

Letting $x = \alpha v_1 L_1$, Equation (A.3) can be reorganized into:

$$\frac{z_1^{I^*}(v_1)}{v_1 L_1} = \frac{(2\beta x)^{\frac{1}{\beta+1}}-1}{x} \quad \text{(A.4)}$$

The right hand side of (A.4) reaches its maximum at:

$$x = 2^{-1}(\beta+1)^{\beta+1}\beta^{-\beta-2} \quad \text{(A.5)}$$

And substituting this (A.5) into (A.4) we get:

$$\frac{z_1^{I^*}(v_1)}{v_1 L_1} = 2\left(\frac{\beta}{\beta+1}\right)^{\beta+1} \quad \text{(A.6)}$$

The right hand side of (A.6) is increasing β. Applying L'Hospital's rule, we have:

$$\lim_{\beta\to\infty} 2\left(\frac{\beta}{\beta+1}\right)^{\beta+1} = 2e^{-1} \quad \text{(A.7)}$$

Hence, the right hand side of (A.6) is less than $2e^{-1}$ and $z_1^{I^*}(v_1) < 2e^{-1}v_1 L_1$ for the first class of security breach probability functions when negative externalities of security investments exist.

Now consider the positive externality case. Using Equation (13), we have:

$$\frac{z_1^{I^*}(v_1)}{v_1 L_1} = \frac{(\alpha\beta v_1 L_1)^{\frac{1}{\beta+1}}-1}{(1+\delta)\alpha v_1 L_1} \quad \text{(A.8)}$$

Letting $x = \alpha v_1 L_1$, Equation (A.8) can be written as:

$$\frac{z_1^{I^*}(v_1)}{v_1 L_1} = \frac{(\beta x)^{\frac{1}{\beta+1}}-1}{(1+\delta)x} \quad \text{(A.9)}$$

The right hand side of (A.9) reaches its maximum at:

$$x=(\beta+1)^{\beta+1}\,\beta^{-\beta-2} \tag{A.10}$$

And substituting this (A.10) into (A.9) we get:

$$\frac{z_1^{II^*}(v_1)}{v_1L_1}=(1+\delta)^{-1}\left(\frac{\beta}{\beta+1}\right)^{\beta+1} \tag{A.11}$$

The right hand side of (A.11) is increasing β. Applying L'Hospital's rule, we have:

$$\lim_{\beta\to\infty}(1+\delta)^{-1}\left(\frac{\beta}{\beta+1}\right)^{\beta+1}=(1+\delta)^{-1}e^{-1} \tag{A.12}$$

Hence, the right hand side of (A.11) is less than $(1+\delta)^{-1}e^{-1}$ and $z_1^{I^*}(v_1)<(1+\delta)^{-1}e^{-1}v_1L_1$ for the first class of security breach probability functions when positive externalities of security investments exist.

Now suppose the security breach probability function belongs to class II. When security investments cause negative externalities, from Equation (15), we have:

$$\frac{z_1^{II^*}(v_1)}{v_1L_1}=\frac{\ln\left(\dfrac{1}{-2\alpha v_1L_1(\ln v_1)}\right)}{\alpha v_1L_1(\ln v_1)} \tag{A.13}$$

Letting $x=-\alpha v_1L_1(\ln v_1)$, Equation (A.13) can be rewritten as:

$$\frac{z_1^{II^*}(v_1)}{v_1L_1}=\frac{\ln\left(\dfrac{1}{2x}\right)}{-x} \tag{A.14}$$

The first-order condition for maximum of the right-hand side is:

$$\frac{1+\ln(1/2x)}{x^2}=0 \tag{A.15}$$

Condition (A.15) is satisfied at the point $x=e/2$, as is the second-order condition:

$$\frac{-3-2\ln\left(\dfrac{1}{2x}\right)}{x^3}<0 \tag{A.16}$$

Thus, the right-hand side of (A.14) is maximized at $x=e/2$, taking on a maximum value of $2/e$ at this point. Hence, $z_1^{II^*}(v_1)/v_1l_1<2e^{-1}$. Hence, $z_1^*(v_1)<2e^{-1}v_1L_1$ in the case of negative externalities also holds for the second class of security breach probability functions.

When security investments generate positive externalities, from Equation (17), we have:

$$\frac{z_1^{II^*}(v_1)}{v_1L_1}=\frac{\ln\left(\dfrac{1}{-\alpha v_1L_1(\ln v_1)}\right)}{(1+\delta)\alpha v_1L_1\ln v_1} \tag{A.17}$$

Letting $x=-\alpha v_1L_1(\ln v_1)$, Equation (A.17) can be rewritten as:

$$\frac{z_1^{II^*}(v_1)}{v_1L_1}=\frac{\ln\left(\dfrac{1}{x}\right)}{-(1+\delta)x} \tag{A.18}$$

The first-order condition for maximum of the right-hand side is:

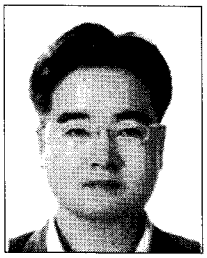
$$\frac{1+\ln(1/x)}{(1+\delta)x^2}=0 \tag{A.19}$$

Condition (A.15) is satisfied at the point $x=e$, as is the second-order condition:

$$\frac{-3-2\ln\left(\frac{1}{2x}\right)}{(1+\delta)x^3}<0 \qquad \text{(A.20)}$$

Therefore, the right-hand size of (A.17) is maximized at $x=e$, taking on a maximum value of $1/e$ at this point. Hence, $z_1^{II*}(v_1)/v_1L_1 < (1+\delta)^{-1}e^{-1}$. Hence, $z_1^*(v_1) < (1+\delta)^{-1}e^{-1}v_1L_1$ in the case of positive externalities also holds for the second class of security breach probability functions.

◆ About the Authors ◆



Woohyun Shim

Woohyun Shim is a senior researcher at Synthesys, Inc. in East Lansing, Michigan, USA. His current research interests include information security and privacy, intellectual property, innovation and regulation, digital ecosystems and IT convergence, and social networks. He has expertise in theoretical economic approaches using game theory, agency theory, transaction cost economics, and media economics. He also has experience in empirical econometric analyses including survival analysis, panel data analysis, and nonparametric analysis. Dr. Shim earned his Ph.D. in Media and Information Studies, with a concentration in Media Economics and Policy, from the College of Communication Arts and Sciences at Michigan State University.

Submitted : August 5, 2011 Accepted : September 22, 2011
1st revision : September 7, 2011