An Analysis of IT Security Management Strategies in the Presence of Interdependent Security Risk*

Woohyun Shim

Michigan State University, shimwoo@msu.edu

ABSTRACT

Recent widespread cyber attacks and security breaches have brought about a rapid increase in organizations' information security investments. A number of studies have explored the optimal level of security investment in situations of independent risk. Issues related to security investment within the context of interdependent risks, however, have not yet been sufficiently investigated. Although previous studies have addressed the security underinvestment problem caused by interdependent risks, for instance, relatively little attention has been paid to the security overinvestment problem. In addition, most of these studies have focused on self-protection mechanisms but not taken insurance mechanisms into account. This study therefore expands the current body of research by exploring multiple scenarios of insufficient and excessive security investments caused by interdependent risks and the interplay between IT security investment and cyber insurance. I discuss how interdependent risk affects firms' information security risk management with respect to the two different types of cyber attacks (i.e., targeted and untargeted attacks). Although the theoretical models upon which the analysis relies are based on expected utility theory, which is widely used in insurance research, this study derives unique propositions that have not been fully identified in other cyber insurance studies. A key finding is that organizations experiencing interdependent risks with different types of cyber attacks use different strategies in making IT security investment decisions and in purchasing cyber insurance policies for their information security risk management than firms that are facing independent risks. The study further provides an economic rationale for employing insurance mechanisms as a risk management solution for information security.

Keywords: H.1.1 [Models and Principles]: Systems and Information Theory—information theory
Index Terms: Interdependent security risks, security strategies, cyber insurance, security investment

1. Introduction

The rapid proliferation of information technologies (ITs) has changed the environment in which firms operate and the ways they do business. Most firms now store proprietary information in computer systems and transact with other firms via dedicated network connections as well as the Internet. While this rapid proliferation of information technologies has provided great benefits to organizations, it has also escalated their exposure to information security breaches. For example, in the U.S., TJX Companies, Inc. revealed that it had experienced a massive data breach caused by hackers breaking into its systems, and disclosed that an estimated 45.7 million credit and debit card records were stolen [2]. These security breaches, understandably, draw tremendous attention, notwithstanding the difficulty in calculating the exact amount of damages or losses from them.

While many organizations have begun to increase their investments in information security by continually adopting a range of more refined technical security solutions [3], these masive investments only part of the overall solutions, and a residual risk remains because there is no system that is foolproof against all types of threats [4, 5]. For example, computer viruses can be designed to mutate in response to technical solutions being employed, and hackers learn from new security technologies and identify ways to circumvent them. Another reason for the existence of residual risk is the interdependence of information security risks: a firm's security investment not only affects its own security risks but also those of other firms [3, 6]. This interdependence of IT security risks is the main focus of this study.

The interdependent feature of IT security risks generates externalities in various contexts. First, a firm's security investments often generate positive externalities for other firms.[1] 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. In contrast, a firm's security investment can also generate negative externalities such as the case where hacking attacks targeted at a highly secured server are diverted to other servers, and hence increase the risks of other firms. Therefore, a basic conclusion of the previous literature is that, without any mechanisms for internalizing externalities, self-interested firms' investment in IT security is likely to be below the socially optimal level (i.e., under-investment or under-provision) when security investments generate positive externalities, whereas the firms' investment in security tends to be above the socially optimal level (i.e., over-investment or over-provision) when security investments cause negative externalities [3, 7-9]. The question then is how to handle these externalities that result in inefficient security investments.

Researchers and practitioners in the field of information security have adopted an economic perspective to investigate how to

* This article is based in part on Chapter 3 of my dissertation, see [1].

[1] A typical example of a positive externality caused by an interdependent risk is Lojack, the auto theft response system. When Lojack is used by some cars, car owners who do not have Lojack benefit from a positive externality because theft against all autos is reduced by the fact that thieves cannot tell in advance which cars have Lojack protection [7].

internalize these externalities and overcome inefficiency [e.g., 10, 11]. Some have argued that the enforcement of liability for losses due to security breaches can internalize security externalities [12, 13]. Since it is difficult, if not impossible, to determine who is responsible for the losses, however, the imposition of liability might be an infeasible option for internalizing the externalities [3]. Other researchers [e.g., 3, 5, 10] have instead suggested using cyber insurance, which can transfer the risk to an insurer who is willing to accept the risks, as an approach to address the externality problems. With cyber insurance, like other insurance products, insured firms may be able to overcome investment inefficiency by balancing their expenditures between security investments and cyber insurance. To date, however, there is a relative paucity of literature on cyber insurance itself.

This study intends to answer two research questions that arise from the above discussion: (1) How do externalities caused by interdependent security risks influence two widely used security risk management strategies – information security investment and cyber insurance; and (2) How does cyber insurance affect a firm's decision regarding security investment. To answer these questions, the expected utility model is used with two firms to present the interplay between security investment and cyber insurance. More specifically, the impact of externalities on the security investments of the firms with and without insurance being available is analyzed.

Unlike the previous literature which mostly focused on illustrating socially inefficient security investments caused by interdependent risks, however, this study examines the effect of interdependent risks on decisions about both security investments and insurance coverage. In addition, this study illustrates how different types of cyber risks will cause different externality problems and give rise to different incentives to invest in information security. I conceptualize that there are two broad classes of risks, risks caused by targeted attacks and risks caused by untargeted attacks, and that these classes cause different types of investment inefficiency.

To the best of my knowledge, unlike other studies [e.g., 12, 14] which implicitly assume that interdependent security risks can result in either positive or negative externalities, this is the first study that links different types of cyber attacks (i.e., targeted and untargeted attacks) to a comprehensive mechanism of IT security risk management strategies that include both IT security investments and cyber insurance with interdependent risk.

Although the theoretical models are based on expected utility theory, which is widely used in insurance research, this study derives unique propositions that have not been fully identified in other cyber security studies. A key finding is that organizations experiencing interdependent risks with different types of cyber attacks use different strategies in making IT security investment decisions and in purchasing cyber insurance policies for their information security risk management compared to firms that are facing independent risks.

The remainder of the article is organized as follows; the next section presents several conceptual frameworks that address the characteristics of cyber attacks and security risks management strategies. I then present several theoretical models that tackle the issue of interdependent security risks and derive a number of new propositions that shows the effects of interdependent risks on security risk management strategies. Discussion and implications of the research are presented in the concluding segment.

2. IT Security Risk and its Management Strategies

2.1. Targeted vs. Untargeted Attacks

Cyber attacks can be categorized into targeted and untargeted attacks. "Untargeted" attacks aim at millions of potential victims, hoping to contaminate as many computer systems as possible [15, 16]. Therefore, adversaries launching untargeted attacks intend to harm any vulnerable system which can be found on a network [15, 17]. Common examples of untargeted attacks include viruses, worms, trojan horses, and spyware. Figure 2-1 shows untargeted attacks schematically. Since adversaries launching untargeted attacks do not target any specific system, an agent's increased investment for coping with untargeted attacks will decrease the risks faced by other agents connected to this agent's system. Therefore, investment in IT security against untargeted attacks is more likely to generate positive externalities.

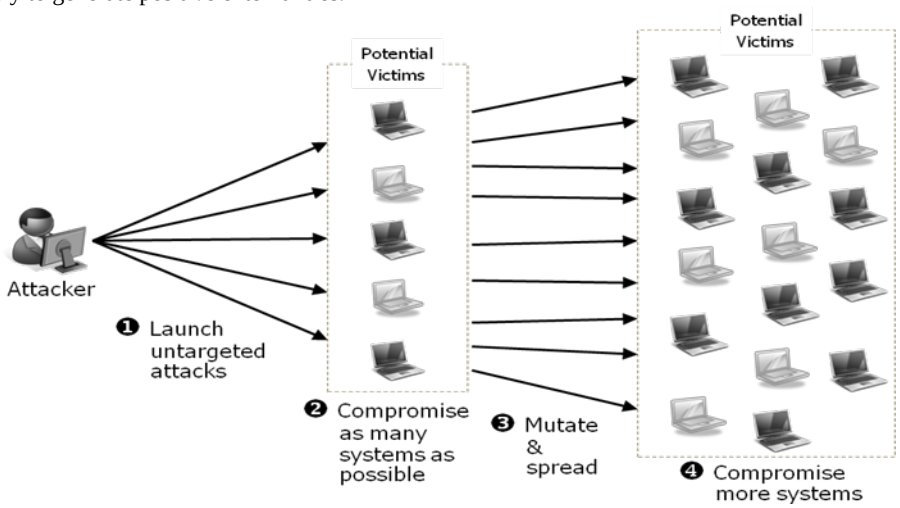

Figure 2-1. Typical untargeted attack

"Targeted" attacks are designed to damage a particular communication system or a firm's information assets [15, 16]. Attackers using such strategies typically collect information about the target, customize attacks for each particular victim, and thus know

who will be attacked [15, 17]. Examples of targeted attacks are malicious hacking and whaling. The scheme of targeted attacks is depicted in Figure 2-2. Since targeted attacks are customized for an intended communication network of systems [15, 16], an agent's increased investment in security against targeted attacks will increase the risks faced by other agents: adversaries launching targeted attacks will substitute less protected targets in place of their original targets, and thus the investment will generate negative externalities.[2] As a result, the relationship between the types of attack and the externality problem can be depicted, as shown in Figure 2-3.[3]

The proposed categorization, which limits the types of cyber attacks to either targeted or untargeted attacks, has advantages and disadvantages. On the one hand, it simplifies the theoretical model and thereby enables a clearer understanding of the direct effects of each type of attack on firms' security risk management strategies. On the other hand, it only allows a partial exploration of cases where the interaction between targeted and untargeted attacks (i.e., hybrid attacks) affects a firm's security risk management strategies.

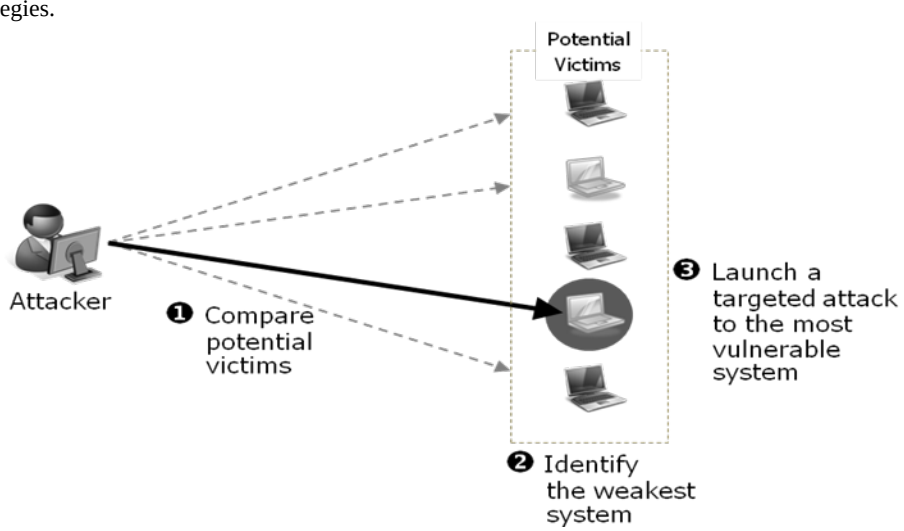

Figure 2-2. Typical targeted attack

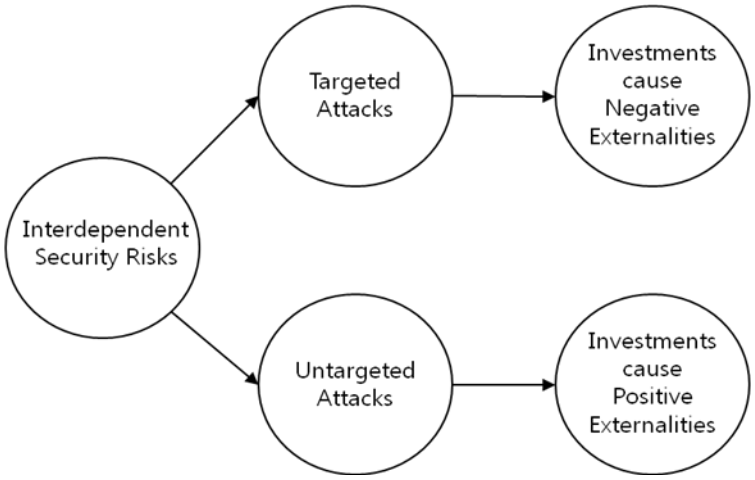

Figure 2-3. Types of attack and externalities

2.2. Self-Protection, Self-Insurance, and Cyber Insurance

[2] There might be hackers who are motivated by reputation in the hacking community. For example, some hackers try to break into computer networks of big companies such as Microsoft and Google because they will improve their own reputation if they succeed in breaking into networks which are extremely difficult to hack. In such cases, IT security investment of the firm will create a positive externality. This type of motivation, however, is only noted here and is not considered in this study.

[3] Although not analyzed in this study, there is another type of attack: hybrid attacks. This type of attack involves the combination of a targeted and untargeted attack and has two stages. In the first stage, adversaries initiate untargeted attacks by spreading malicious software. In the second stage, the adversaries launch targeted attacks using two different types of schemes. First, the adversaries may launch targeted attacks by breaking into the computer system, which was infected in the first stage. Since some malicious software can create backdoors in infected systems, the adversaries can easily gain access to the systems. Second, the adversaries may attack particularly vulnerable systems using machines that were infected in the first stage. Some worms and viruses turn infected systems into remote-controlled zombie computers. These zombies are used by the adversaries to carry out DDoS attacks, sending out spam e-mails, etc.

Traditional security management strategies to hedge against losses from IT security breaches involve three different instruments: self-protection (to reduce the probability of a loss), self-insurance (to reduce the size of a loss) and insurance bought in the market.[4] Recently, several studies [e.g., 19, 20, 21] have questioned the effectiveness of sole dependence on the traditional security investment model, implemented by self-protection and self-insurance. This body of research claims that deficiencies in abilities for perfect detection and protection, together with the existence of interdependent security risks result in a considerable residual risk for organizations. Firms therefore have started to demand alternative risk management mechanisms, most specifically market insurance that can make up for the weaknesses of traditional security management strategies.

Market insurance is a traditional instrument for shifting residual risks beyond due diligence [22]. In spite of its similarity to self-insurance in that both mechanisms intend to reduce the size of a loss, market insurance is offered by third party insurance companies. In the field of information security, insurance products (known as cyber insurance), which specifically dealt with losses from computer crimes, cover not only losses, such as physical damages that are addressed by traditional insurance products, but also provide coverage for intangible damages.

3. Theoretical Analysis

This section presents theoretical models that show how interdependence in cyber security affects firms' decisions regarding security investments and cyber insurance purchases. In the models, I consider identical firms with an initial wealth *W* and a utility function $U(\cdot)$. I assume that firms are rational and risk averse, implying that the utility function is concave (i.e., $U'(\cdot) > 0$ and $U''(\cdot) < 0$), and constant absolute risk aversion (CARA) is given by $r = -U''/U'$. To simplify the illustration, this study assumes single-period probabilistic models for the risk, in which all firms' decisions and corresponding consequences occur in a simultaneous manner, such that firms invest in self-protection and/or purchase an insurance product in a single period.[5] There are only two possible states for the firm: a good state, in which the firm does not experience any security breach, and a bad state in which the firm experiences such a breach. Firm *i*'s breach probability (i.e., probability of loss or damage) is denoted by $B_i(\cdot)$ and can be decreased by the firm's investment in security (i.e., $B_i'(\cdot) < 0$). I assume that the breach probability has declining returns (i.e., $B_i''(\cdot) > 0$). In the case of independent IT security risks, $B_i(\cdot)$ is only determined by firm *i*'s level of security investment z_i, that is, $B_i(z_i)$. In contrast, the breach probability of a firm in the case of interdependent IT security risks is determined not only by the firm's own security investment, but also by those of other firms.[6] Similarly, a firm's investment in self-protection affects the breach probability at all firms. z_{-i} represents investment in self-protection of all firms except firm *i*. Consequently, in the interdependent case, firm *i*'s breach probability is $B_i(z_i, z_{-i})$. If a security breach occurs at firm *i*, the firm incurs a loss of L_i.

3.1 Investment in Self-Protection without a Cyber Insurance Market

The effect of a firm's investment in IT security generally depends on whether security risks are independent or interdependent. I first examine the baseline model in which security risks are independent and no cyber insurance product is available. I then consider cases in which breaches caused by untargeted and targeted attacks are interdependent, and thus generate positive and negative externalities, respectively.

3.1.1 Baseline Model of Independent Risks without a Cyber Insurance Market

I assume that, when there is no insurance product available, all firms manage cyber risks by investing only in self-protection. The condition that maximizes the expected utility of firm *i* can be expressed as

$$\max_{z_i} B_i(\cdot)U(W_i - L_i - z_i) + [1 - B_i(\cdot)]U(W_i - z_i) \tag{3.1}$$

where $U(W_i - z_i)$ is firm *i*'s utility without a security breach and $U(W_i - L_i - z_i)$ is its utility with a security breach. The first-order condition for IT security investment is

$$B_i'(\cdot) = \frac{B_i(\cdot)U_L' + [1 - B_i(\cdot)]U_N'}{[U_L - U_N]} \tag{3.2}$$

where $U_L = U(W_i - L_i - z_i)$ and $U_N = U(W_i - z_i)$. In order to assess this expression in a useful way, I use a Taylor series approximation which has been commonly used in the literature on uncertainty and insurance [e.g., 23, 24, 25].[7] Using the first-order Taylor series approximation,[8] $U_N \approx U_L + U_L'L_i$ and $U_N' \approx U_L' + U_L''L_i$, equation (3.2) can be rewritten as:

$$B_i'(z_i^o) = -\frac{1}{L_i} + r[1 - B_i(z_i^o)] \tag{3.3}$$

where $r = -U_L''/U_L'$. The superscript o on z_i indicates the case in which security risks are independent and no cyber insurance product is available.

---

[4] As reference [18] indicated, it is somewhat artificial to distinguish self-protection and self-insurance mechanisms since many IT security measures do both at the same time. Thus, in this study, I do not distinguish them and refer to them simply as self-protection.

[5] Therefore, this study does not take into account dynamic aspects which use game theoretic approaches.

[6] It can be argued that, ceteris paribus, a higher level of investment by a firm may increase the probability of a breach of other firms because hackers may focus their efforts on firms that are easier to attack. On the other hand, it can also be argued that a higher level of investment by a firm may reduce the breach probability of other firms since computers across firms are interconnected.

7 According to references [26] and [27], any well-behaved utility function can be expanded by a Taylor series approximation.

8 Hereinafter, I assume that a firm's initial wealth, W, is large enough to satisfy a condition for Taylor series approximation. In addition, I ignore the third and higher-order terms since, while they may exist, these derivatives will be multiplied by very small terms.

3.1.2 General Model of Interdependent Risks without a Cyber Insurance Market in the Context of Untargeted Attacks

Analyzed here are cases in which security risks are interdependent and IT security investments generate positive externalities due to untargeted cyber attacks. These attacks, which intend to harm large numbers of potential victims, generate positive externalities since the increased security investment of one firm will reduce the risks faced by other firms connected to this firm's computer system. Therefore, as shown in Figure 3-1, firms have incentives to invest less in information security than they do in this case.

Figure 3-1. Link between untargeted attacks and the level of investments

Following [12] and [3], I model positive externalities of security investments in the following manner. To simplify the model, I assume that there are only two symmetric firms with interdependent risks (i=1, 2). Security investments have direct effects as well as indirect effects. Direct effects refer to the effects of security investment on a firm's security that change the breach probability caused by a direct attack made on the firm's information system. Indirect effects refer to the effects of other firms' security investment on the firm's security which affects the breach probability caused by an attack through other firms' systems.[9]

I model the breach probability under direct effects as $p(z_1)$ where z_1 is the security investment by firm 1 ($p'(\cdot) < 0$ and $p''(\cdot) > 0$). The breach probability caused by indirect effects is given by $q \cdot p(z_2)$, $0 \le q \le 1$ where the parameter q is the degree of interdependency. A higher q indicates a higher degree of interdependence. $q \cdot p(z_2)$ represents the probability of malicious attacks breaking into firm 1's system through firm 2's system. Taken together, firm 1's security breach probability can be expressed as:

$$B_1(z_1, z_2) = p(z_1) + [1 - p(z_1)]qp(z_2) = 1 - [1 - p(z_1)][1 - qp(z_2)] \tag{3.4}$$

Figure 3-2 illustrates the breach probability of firm 1 in the case of positive externalities. If there are no externalities, the probability of breach is the dotted rectangle on the left. As positive externalities are considered, the oblique-lined rectangle in the center is added. The solid shaded rectangle represents the change of the breach probability resulted from the change of the degree of interdependence and firm 2's level of security investment.

From equation (3.3), the first order condition with respect to z_1 can be expressed as

$$B_i'(z_1, z_2) = p'(z_1)[1 - qp(z_2)] = -\frac{1}{L_1} + r[1 - p(z_1)][1 - qp(z_2)]. \tag{3.5}$$

Therefore, if the cost of a breach is assumed to be equal to 1, the optimal level of security investment is the solution to the following equation:

$$p'(z_1^p) = -\frac{1}{L_1[1 - qp(z_2^p)]} + r[1 - p(z_1^p)]. \tag{3.6}$$

The superscript p on z_1 indicates the case where security investments generate positive externalities and there is no cyber insurance product available.

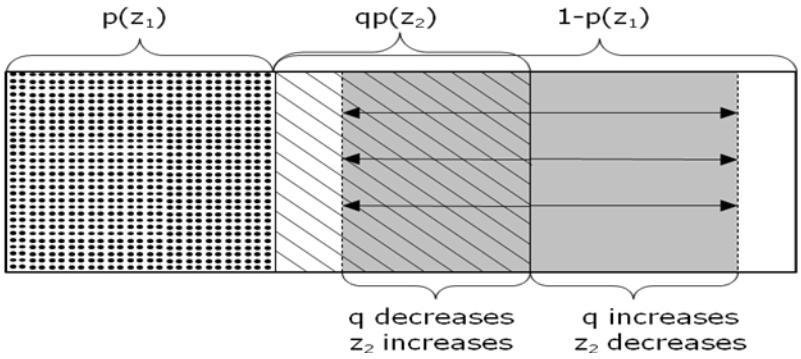

Figure 3-2. Illustration of breach probability with positive externalities

3.1.3 General Model of Interdependent Risks without a Cyber Insurance Market in the Context of Targeted Attacks

9 Note that, according to reference [22], a security breach which occurs at a firm's own site incurs a higher loss to the firm (direct loss) than is the case when the loss caused by a breach arises at the partnering firm (indirect loss). He further argued that if the shared asset is compromised at both the firms, the losses are then superadditive and potentially higher than is the case when these firms experience separate security breaches.

There are also cases in which an adversary focuses all of his or her resources on a single target. To see this outcome, consider a situation where a pool of malicious hackers chooses to attack the most vulnerable security system. Since firms know that the hackers will attack only one of them and will avoid firms with better protection than others, each firm has an incentive to deviate from Nash equilibrium by increasing investment in security protection by an infinitesimal amount. In other words, to make security investment effective, a firm should invest more in security compared to other firms. It would seem to follow then that a firm's security investment for coping with this type of targeted attacks, while reducing its own breach probability, increases the breach probabilities of other firms, and thus is likely to generate negative externalities. The following figure illustrates the link between targeted attacks and an incentive of excessive investment.

Figure 3-3. Link between targeted attacks and the level of investment

Following [3], I model negative externalities of security investments in the following manner: I use the term z_1/z_2 to characterize the relative effectiveness of firm 1's security investment and model the breach probability as $B_1(z_1, z_2) = p(z_1 \cdot (z_1/z_2))$. If firm 1 makes a higher security investment than firm 2 (i.e., $z_1/z_2 > 1$), we have $z_1 \cdot (z_1/z_2) > z_1$ and $p(z_1 \cdot (z_1/z_2)) < p(z_1)$. This implies that firm 1's security investment is more effective in decreasing its breach probability. For instance, if a firm invests more in security than do others, adversaries launching targeted attacks such as hacking and DDoS will substitute their initial target with a less protected target. Therefore, the breach probability of a firm increases corresponding to other firm's security investments, which captures the negative externality of security investment. Figure 3-4 displays the information security risk in the case of negative externalities.

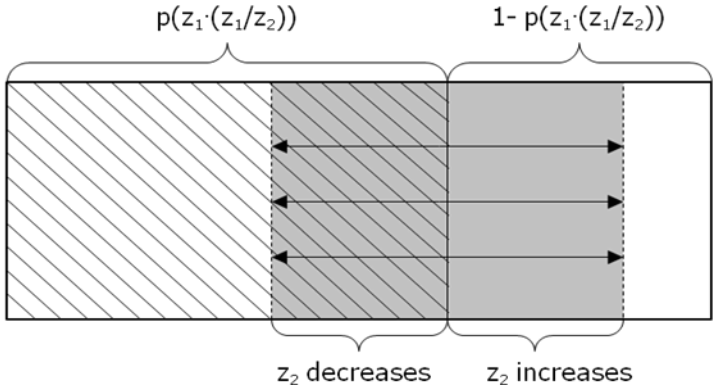

Figure 3-4. Illustration of breach probability with negative externalities

As was similarly the case in the previous section, I assume a case with two symmetric firms. Applying $B_1(z_1, z_2) = p(z_1 \cdot (z_1/z_2))$ and $\partial B_1(z_1, z_2)/\partial z_1 = (2z_1/z_2)\,p'(z_1 \cdot (z_1/z_2))$ to equation (3.3), and using symmetric assumption where $z_1 = z_2$, firm 1's equilibrium security investment is determined by

$$p'(z_1^n) = -\frac{1}{2L_1} + \frac{r[1 - p(z_1^n)]}{2}. \tag{3.7}$$

The superscript *n* on z_1 indicates the case where security investments generate negative externalities and there is no cyber insurance product available.

3.2 Interplay Between Self-Protection and Cyber Insurance

I now analyze the impact that cyber insurance has on the level of security investment in self-protection chosen by a firm. Based on [12], I model an insurance market, in this section, in the following manner. When a cyber insurance product is available, the insurance premium paid by firm *i* is $\pi_i I_i$ where π_i is the price of insurance coverage which shows the maximum willingness to pay to escape a loss from a security breach and I_i is indemnity paid by the insurer if a loss from a security breach is found. If firm *i* decides to purchase an insurance product, the firm pays the premium $\pi_i I_i$ at the beginning of the period and is paid an indemnity, I_i, at the end of the period if there is a security incident.[10]

To take insurance market maturity into account, I use the loading factor, λ, and thus the insurance price can be expressed as

[10] To simplify the analysis, I again use simple one-period expected utility models, in which all decisions and outcomes occur simultaneously.

$\pi_i = (1+\lambda)B_i$. That is, if competition in the insurance market is perfect (i.e., the insurance market is mature), the insurance price is actuarially fair, $\lambda = 0$, and the insurance companies make zero profit, $\pi_i = B_i$. In contrast, if competition in the insurance market is imperfect (i.e., the insurance market is immature), the insurance price is not actuarially fair, $\lambda > 0$, and the insurance companies make positive profits.[11]

3.2.1 Baseline Model of Independent Risks with a Cyber Insurance Market

Now assume that all firms can manage cyber security risks by investing in self-protection and/or purchasing a cyber insurance product. Using the indemnity payment I_i and insurance premium $\pi_i I_i$, firm *i*'s utility function is $U(W_i - L_i + [1-\pi_i(z_i)]I_i - z_i)$ with a security breach, whereas the utility function is $U(W_i - \pi_i(z_i)I_i - z_i)$ with no security breach. Therefore, the maximization problem of firm *i*'s expected utility can be presented as

$$\max_{z_i, I_i} B_i(z_i)U_i(W_i - L_i + [1-\pi_i(z_i)]I_i - z_i) + [1-B_i(z_i)]U_i(W_i - \pi_i(z_i)I_i - z_i). \quad (3.8)$$

By using, $\pi_i(z_i) = [1+\lambda]B_i(z_i)$, and the first order Taylor series approximation, the first order conditions for IT security investment and cyber insurance can be written as:

$$B_i'(z_i^{oI}) = -\frac{1}{(1+\lambda)L_i}, \quad (3.9)$$

and

$$I_i = L_i - \frac{\lambda}{r[1-B_i(z_i^{oI})](1+\lambda)} \quad (3.10)$$

where $r = -U_{LI}''/U_{LI}'$. The superscript *oI* on z_i means that security risks are independent and there is a cyber insurance product available. When an insurance market is mature, the loading factor λ equals zero, a firm purchases full insurance coverage ($I_i = L_i$) and the optimal level of investment is determined by $B_i'(z_i^{oI}) = -1/L_i$.

3.2.2 General Model of Interdependent Risks with a Cyber Insurance Market in the Context of Untargeted Attacks

I now consider the case in which a firm's security risk is interdependent and security investment has a positive externality. Using equations (3.9) and (3.10), the first order Taylor series approximation and a symmetric assumption (i.e., $z_1 = z_2$), the first order conditions for IT security investment and cyber insurance can be written as:

$$p'(z_1^{pI}) = -\frac{1}{[1-qp(z_1^{pI})](1+\lambda)L_1}, \quad (3.11)$$

and

$$I_1 = L_1 - \frac{\lambda}{r(1+\lambda)[1-p(z_1^{pI})][1-qp(z_1^{pI})]} \quad (3.12)$$

where superscript *pI* on z_1 and z_2 indicates positive externality and the existence of a cyber insurance market, and $r = -U_{LI}''/U_{LI}'$. Consequently, it can be seen that, as the insurance market becomes mature (i.e., as λ approaches to zero), firms are more likely to invest less in self-protection and, instead, buy full insurance coverage.

3.2.3 General Model of Interdependent Risks with a Cyber Insurance Market in the Context of Targeted Attacks

I now investigate the case in which investment in security measures causes negative externalities with considering the existence of a cyber insurance market. Using equation (3.9), firm 1's equilibrium security investment is determined by

$$p'(z_1^{nI}) = -\frac{1}{2(1+\lambda)L_1} \quad (3.13)$$

when $z_1 = z_2$. In addition, using equation (3.10), the optimal level of cyber insurance can be expressed as

$$I_1 = L_1 - \frac{\lambda}{r(1+\lambda)[1-p(z_1^{nI})]} \quad (3.14)$$

when $z_1 = z_2$. The superscript *nI* used in both equations (3.13) and (3.14) is used to indicate that security investments generate negative externalities and there is a cyber insurance product available.

3.3 Synthesis of the Theoretical Models: Impact of Externalities on Self-Protection and Cyber Insurance

To analyze the combined impact of interdependency and insurance market maturity on security investment and insurance coverage, I set forth security spending and insurance coverage in the cases of two identical firms in the following table.

[11] Currently, the cyber insurance market is not well developed [3]. There are only a small number of insurance companies offering cyber insurance products, and thus they are likely to make profits.

Table 3-1. Comparison of IT security investment and insurance coverage

	Insurance Market	No Insurance Market
Independence	$p'(z_1^{oI}) = -\frac{1}{(1+\lambda)L_1}$ $I_1^{oI} = L_1 - \frac{\lambda}{r[1-p_1(z_1^{oI})](1+\lambda)}$	$p'(z_1^{o}) = -\frac{1}{L_1} + r[1-p(z_1^{o})]$
Positive Externality	$p'(z_1^{pI}) = -\frac{1}{[1-qp(z_1^{pI})](1+\lambda)L_1}$ $I_1^{pI} = L_1 - \frac{\lambda}{r(1+\lambda)[1-p(z_1^{pI})][1-qp(z_1^{pI})]}$	$p'(z_1^{p}) = -\frac{1}{L_1[1-qp(z_1^{p})]} + r[1-p(z_1^{p})]$
Negative Externality	$p'(z_1^{nI}) = -\frac{1}{2(1+\lambda)L_1}$ $I_1^{nI} = L_1 - \frac{\lambda}{r(1+\lambda)[1-p(z_1^{nI})]}$	$p'(z_1^{n}) = -\frac{1}{2L_1} + \frac{r[1-p(z_1^{n})]}{2}$

Comparison of the solutions set forth above can provide valuable insight in understanding the issues of cyber security. I first compare the solutions for the baseline models with those for the general models of the cases of untargeted attacks (i.e., the existence of positive externality) and targeted attacks (i.e., the existence of negative externality).

From Table 3-1, it can be demonstrated that, when information security investment generates positive externalities, a firm's security investment reduces not only its breach probability but also those of others. For example, a firm which equips its computer systems with strong countermeasures against viruses and spyware will reduce the risks encountered by other firms connected to this firm's system. In the case of interdependent security risks with positive externalities, however, the risk controllable by firm 1's IT security investment is reduced from $p(z_1)$ to $p(z_1)[1-qp(z_2)]$ and the efficiency of its IT security investment, which is measured by the marginal reduction in breach probability resulting from the investment, is also reduced from $|p'(z_1)|$ to $|p'(z_1)[1-qp(z_2)]|$ [12]. As a result, taking together the reduced efficiency of IT security investment and the decreased controllability of security risk, firms may be discouraged from investing in IT security.

In contrast, in the case of negative externalities, we can observe that a negative externality caused by interdependency neither increases the breach probability nor reduces the risk controllability: that is, using two firms that are identical, it can be demonstrated that the overall security risk is unchanged since the probability of breach is the same whether firms' security risks cause a negative externality or no externality, i.e., $p(z_1) = p(z_1 \cdot (z_1 / z_2))$; the risk controllable by a firm's security investment also does not change for the same reason. On the other hand, the marginal decrease in security risk due to security investment, which is a measure of the efficiency of the investment, increases from $|p'(z_1)|$ to $|2p'(z_1)|$ in the case of identical firms. Therefore, from the firms' point of view, the increased efficiency of security investment along with the unchanged overall risk gives them incentives to increase investment in IT security. This implies that firms have an incentive to invest more in cases where IT security investment generates negative externalities (i.e., targeted attack cases) and to invest less in cases where IT security investment generates positive externalities (i.e. untargeted attack cases) compared to the interdependent security risk case. Since this explanation holds true whether a cyber insurance market exists or not, taking these statements together, this leads us to the following propositions (a formal proof appears in the appendix):

Proposition 1: *Without a cyber insurance market, firms experiencing untargeted attacks invest less in self-protection than do firms experiencing the same number of targeted attacks.*[12]

Proposition 2: *With a cyber insurance market, firms experiencing untargeted attacks invest less in self-protection than do firms experiencing the same number of targeted attacks.*

In spite of the higher breach probability in the case of positive externalities compared to probability in situations of independent risks (i.e., $p(z_1) + \{1-p(z_1)\}qp(z_2) > p(z_1)$), it can be demonstrated from Propositions 1 and 2 that positive externalities in IT security risks reduces a firm's incentive to invest in IT security. However, from the viewpoint of insurance companies, the higher breach probability in the case of positive externalities leads to a higher insurance premium charge for insureds, i.e., $(1+\lambda)[p(z_1) + \{1-p(z_1)\}qp(z_2)] > (1+\lambda)p(z_1)$, which, in turn causes firms to reduce their insurance coverage. On the other hand, unlike the case of positive externalities, the total risk of firms experiencing targeted attacks is lower than that of firms experiencing untargeted attacks since firms experiencing targeted attacks generally invest more in self-protection than firms suffering untargeted attacks. Therefore, an insurance company might charge a lower insurance premium for the firms experiencing targeted attacks and this causes the firms to increase their insurance coverage. This leads us to the following proposition (a formal proof appears in the appendix):

[12] Note that all propositions are stated under a '*ceteris paribus*' assumption.

Proposition 3: *With a cyber insurance market, firms experiencing targeted attacks spend more on cyber insurance coverage than do firms experiencing the same number of untargeted attacks.*

I now discuss the impact of loss on firms' strategies through a comparative static analysis. For firms experiencing untargeted attacks, since $p'(z_1^{pt})\{1-qp(z_2^{pt})\} = -1/(1+\lambda)L_1$, it can be seen that the efficiency of security investment increases as the amount of security loss increases (i.e., $\partial p'(z_1^{pt})[1-qp(z_1^{pt})]/\partial L_1 = 1/(1+\lambda)L_1^2 > 0$). This increased efficiency, in turn, causes firms to invest more in their IT security. Similarly, in the case where firms experiencing targeted attacks, since the efficiency of security investment increases as the level of loss increases (i.e., $\partial 2p'(z_1^{pt})/\partial L = 1/(1+\lambda)L^2 > 0$), the increased efficiency leads firms to increase the investment in IT security. Therefore, we get (a formal proof appears in the appendix):

Proposition 4: *With a cyber insurance market, firms increase security investments as the level of security risks rises,* $\partial z/\partial L > 0$.

Similarly, an increase in loss also brings about an increase in insurance coverage. This relationship exists because an increase in loss raises the expected loss, which increased expected loss causes an increase in insurance coverage [12]. Therefore,

Proposition 5: *With a cyber insurance market, firms purchase more insurance coverage as loss from a security breach rises,* $\partial I/\partial L > 0$ *(See Appendix for proof).*

In addition, as mentioned earlier, cyber insurance is regarded as a remedy for the residual risk, and hence increases as security investments rise. As [28] and [20] have indicated, this implies that, for a given breach probability, cyber insurance and information security investments are also complements in the equilibrium. That is, for a given probability of breach, an increase in security investments causes an increase in insurance coverage, and vice versa.[13] This leads us to the following proposition:

Proposition 6: *With a cyber insurance market, firms that make higher security investments in equilibrium will also cover more of the risk through cyber insurance,* $\partial I^*/\partial z^* > 0$ *(See Appendix for proof).*

Lastly, I investigate the effect of cyber insurance on the demand for self-protection. If market insurance were available at an actuarially fair price, $\pi(z) = B(z)$, the optimal investment in IT security would be smaller than the amount spent in the absence of market insurance. That is,

Proposition 7: *If a cyber insurance market is available and mature, firms invest less in cyber security when cyber insurance is available than when it is not (See Appendix for proof).*

As argued by [29], [8] and [3], Proposition 7 suggests that the employment of a cyber insurance market can only partially resolve the inefficient security investment problem in the case of targeted attacks by reducing the investment, whereas the insufficient security investment problem in the case of untargeted attacks becomes more severe. That is, even if the positive externality case is more problematic since it might cause higher security risks (due to less IT security investment and higher total risk), cyber insurance cannot solve this problem. The following figure illustrates how the adoption of a cyber insurance market affects firms' information security investments.

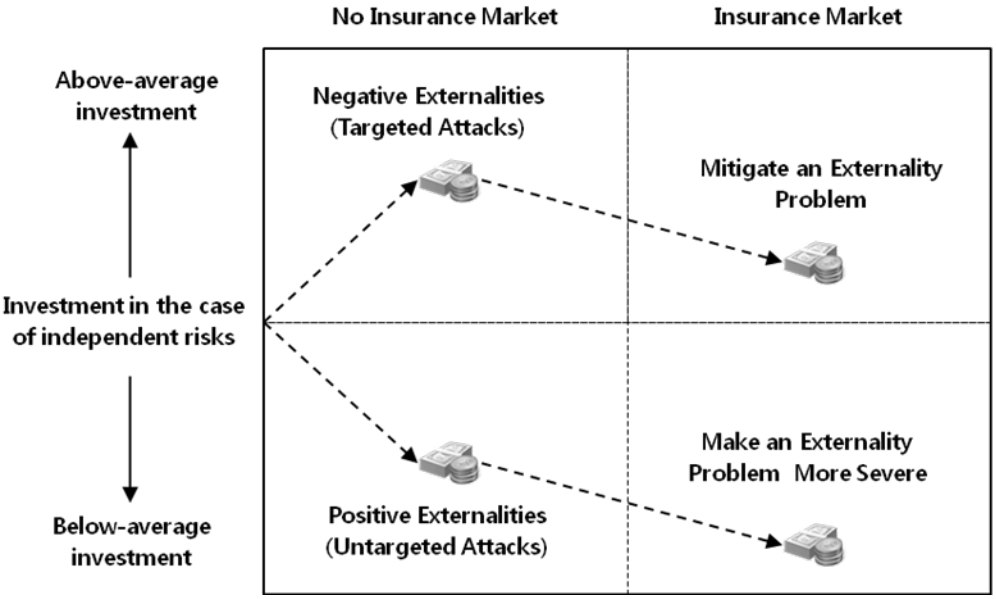

Figure 3-5. Effect of the Adoption of A Cyber Insurance Market on the Level of Information Security Investment

[13] Some researchers have argued that insurance coverage and security investments are substitutes. That is, IT security investments would be discouraged by cyber insurance. This effect is generally referred to as "moral hazard" since policyholders buy less than full insurance coverage as they increase the level of security investments [20].

4. Discussion and Implications

The current literature on IT security focuses generally on the effectiveness of the adoption of security solutions or products as security management tools. While this approach helps in understanding security risk management, it has paid relatively little attention to different incentives to invest in IT security. In this study, I considered firms' strategies for managing IT security risks when the risks are interdependent.

Specifically, this study brought together issues of information security investment and cyber insurance that jointly impact security risk management within a firm. I used a traditional insurance model which uses expected utility theory, and explored it under conditions of an interdependent security environment. In contrast to the current literature, this study not only took into account positive and negative externalities of IT security investments caused by interdependent security risks, but also explicitly illustrated how untargeted and targeted cyber attacks cause these externalities. I then analyzed the corresponding inefficiency in IT security investment using two security management mechanisms - self-protection and cyber insurance.

Several important implications emerged from the analysis. The first set of implications came from the perverse incentives to invest in IT security as the characteristics of interdependent information security risks distort firms' incentives for such investment. The analysis showed that when firms invest in IT security to protect their computer systems against untargeted attacks such as virus or spyware intrusion, the investments generate positive externalities and firms make insufficient investments in IT security. In contrast, when firms invest in IT security to protect their computer systems against targeted attacks such as hacking and DDoS attacks, the investment causes negative externalities and firms invest excessively in IT security. Hence, these misaligned incentives may cause inefficient IT security management practices.

The second set of implications relate to whether the adoption of cyber insurance can mitigate the negative effects of interdependent IT security risks. The analysis showed that the adoption of cyber insurance lowers the overall level of IT security investment regardless of firms' purchase of cyber insurance policies. Therefore, from a social planner's perspective, the adoption of cyber insurance can potentially improve social welfare by mitigating the problem of excessive investment in the case of negative externalities (i.e., a targeted attack case) whereas it may decrease a social surplus because the insufficient investment problem in the case of positive externalities (i.e., an untargeted attack case) might become more severe. Consequently, the adoption of cyber insurance can only resolve the excessive investment problem but does not mitigate the insufficient investment problem.

The complementarity between investments in self-protection and the purchase of cyber insurance coverage is another implication of this examination. Although this study found that the adoption of cyber insurance might aggravate the insufficient security investment problem, the complementarity effect can potentially mitigate this problem and can improve social welfare. For example, due to the complementarity effect, subsidizing organizations to purchase cyber insurance policies, which cover damages caused by untargeted attacks, will increase organizations' purchase of the insurance policies as well as the level of IT security investments. Another example is price discrimination by insurance companies. From the insurance companies' point of view, the total risk caused by untargeted attacks is higher than that of targeted attacks due to IT security underinvestment and thus the insurance company would charge higher premiums for covering damages from untargeted attacks. However, because of the complementarity effects, price discrimination by insurance companies, which charges lower premiums for policies covering untargeted attacks than targeted attacks, would increase both firms' purchase of insurance products and the firms' security investments, and, in turn, reduce total risk and insurance claims caused by losses from untargeted attacks. In sum, additional mechanisms that take advantage of the complementarity effect could solve the insufficient investment problem resulting from the adoption of cyber insurance and lead to a better social outcome.

Appendix

Proof of Proposition 1. Compare (3.6) with (3.3), if the cost of a breach is assumed to be equal to 1, $B_1'(z_1^o) = -\frac{1}{L_1} + r[1 - B_1(z_1^o)] > p'(z_1^p) = -\frac{1}{L_1[1 - qp(z_2^p)]} + r[1 - p(z_1^p)]$ and $z_1^o > z_1^p$ since $B_1(z_1^o) = p(z_1^o)$ and $p'(\cdot) < 0$.

Similarly, compare (3.7) with (3.3), $B_1'(z_1^o) = -\frac{1}{L_1} + r[1 - B_1(z_1^o)] < p'(z_1^n) = -\frac{1}{2L_1} + \frac{r[1 - p(z_1^n)]}{2}$ and $z_1^o < z_1^n$. Therefore, it can be demonstrated that $z_1^n > z_1^o > z_1^p$

Proof of Proposition 2. Compare (3.11) with (3.9), if the cost of a breach is assumed to be equal to 1, $p'(z_1^{oI}) = -\frac{1}{(1+\lambda)L_1} > p'(z_1^{pI}) = -\frac{1}{[1 - qp(z_1^{pI})](1+\lambda)L_1}$ and $z_1^{oI} > z_1^{pI}$. In contrast, compare (3.13) with (3.9), $p'(z_1^{nI}) = -\frac{1}{2(1+\lambda)L_1} > p'(z_1^{oI}) = -\frac{1}{(1+\lambda)L_1}$ and $z_1^{nI} > z_1^{oI}$. As a result, $z_1^{nI} > z_1^{oI} > z_1^{pI}$

Proof of Proposition 3. Comparing equations (3.10), (3.12) and (3.14), it can be demonstrated that $L_1 - \frac{\lambda}{r(1+\lambda)[1 - p(z_1^{nI})]} > L_1 - \frac{\lambda}{r[1 - p_1(z_1^{oI})](1+\lambda)} \geq L_1 - \frac{\lambda}{r(1+\lambda)[1 - p(z_1^{pI})][1 - qp(z_1^{pI})]}$. As a result, $I_1^{nI} > I_1^{oI} \geq I_1^{pI}$.

Proof of Proposition 4. In the presence of positive externalities, the impact of loss on firm 1's security investment can be expressed as:

$$\frac{\partial p'(z_1^{pI})[1-qp(z_1^{pI})]}{\partial L_1} = \frac{1}{(1+\lambda)L_1^2}$$

$$\rightarrow \frac{\partial p'(z_1^{pI})[1-qp(z_1^{pI})]}{\partial z_1^{pI}} \frac{\partial z_1^{pI}}{\partial L_1} = \frac{1}{(1+\lambda)L_1^2}$$

$$\rightarrow \frac{\partial z_1^{pI}}{\partial L_1} = \frac{1}{(1+\lambda)L_1^2\{p''(z_1^{pI})[1-qp(z_1^{pI})] - p'(z_1^{pI})qp'(z_1^{pI})\}} > 0$$

Similarly, in the presence of negative externalities, the impact of loss on firm 1's security investment can be presented as:

$$\frac{\partial p'(z_1^{nI})}{\partial L_1} = \frac{1}{2(1+\lambda)L_1^2}$$

$$\rightarrow \frac{\partial z_1^{nI}}{\partial L_1} = \frac{1}{2(1+\lambda)L_1^2 p''(z_1^{nI})} > 0$$

Proof of Proposition 5. In the presence of positive externalities, the impact of loss on firm 1's purchase of cyber insurance coverage can be expressed as:

$$\frac{\partial I_1^{pI}}{\partial L_1} = 1 - \frac{\lambda}{r(1+\lambda)} \frac{\partial\{[1-p(z_1^{pI})][1-qp(z_1^{pI})]\}^{-1}}{\partial z_1^{pI}} \frac{\partial z_1^{pI}}{\partial L_1}$$

$$= 1 + \frac{\lambda}{r(1+\lambda)} \frac{[-p'(z_1^{pI})(1-qp(z_1^{pI})) - (1-p(z_1^{pI}))qp'(z_1^{pI})]}{[1-p(z_1^{pI})]^2[1-qp(z_1^{pI})]^2} \frac{\partial z_1^{pI}}{\partial L_1} > 0$$

On the other hand, in the presence of negative externalities, the impact of loss on firm 1's purchase of cyber insurance coverage can be determined by:

$$\frac{\partial I_1^{nI}}{\partial L_1} = 1 - \frac{\lambda}{r(1+\lambda)} \frac{\partial[1-p(z_1^{pI})]^{-1}}{\partial z_1^{nI}} \frac{\partial z_1^{nI}}{\partial L_1}$$

$$= 1 - \frac{\lambda}{r(1+\lambda)} \frac{p'(z_1^{nI})}{[1-p(z_1^{nI})]^2} \frac{\partial z_1^{nI}}{\partial L_1} > 0$$

Proof of Proposition 6. In the case of positive externalities, the relationship between firm 1' security investment and cyber insurance purchase can be determined by:

$$\frac{\partial I_1^{pI*}}{\partial p(z_1^{pI*})} = -\frac{\lambda\{r(1+\lambda)[(1-qp(z_1^{pI*})) + q(1-p(z_1^{pI*}))]\}}{\{r(1+\lambda)[1-p(z_1^{pI*})][1-qp(z_1^{pI*})]\}^2} < 0$$

$$\frac{\partial p(z_1^{pI*})}{\partial z_1^{pI*}} = -\frac{1}{[1-qp(z_1^{pI*})](1+\lambda)L_1} < 0.$$

Therefore, $\frac{\partial I_1^{pI*}}{\partial z_1^{pI*}} = \frac{\partial I_1^{pI*}}{\partial p(z_1^{pI*})} \frac{\partial p(z_1^{pI*})}{\partial z_1^{pI*}} > 0$. Similarly, in the presence of negative externalities, the relationship can be demonstrated by:

$$\frac{\partial I_1^{nI*}}{\partial p(z_1^{nI*})} = -\frac{\lambda(1+\lambda)r}{\{r(1+\lambda)[1-p(z_1^{nI*})]\}^2} < 0$$

$$\frac{\partial p(z_1^{nI*})}{\partial z_1^{nI*}} = -\frac{1}{2(1+\lambda)L_1} < 0$$

As a result, $\frac{\partial I_1^{nI}}{\partial z_1^{nI}} = \frac{\partial I_1^{nI}}{\partial p(z_1^{nI})} \frac{\partial p(z_1^{nI})}{\partial z_1^{nI}} > 0$.

Proof of Proposition 7. From Table 3-1, the comparison of optimal security investment for each cell leads us to the following results.

$$p'(z_1^{oI}) = -\frac{1}{L_1} < p'(z_1^{o}) = -\frac{1}{L_1} + r[1 - p(z_1^{o})] \rightarrow z_1^{oI} < z_1^{o}$$

$$p'(z_1^{pI}) = -\frac{1}{[1 - qp(z_2^{pI})]L_1} < p'(z_1^{p}) = -\frac{1}{L_1[1 - qp(z_2^{p})]} + r[1 - p(z_1^{p})] \rightarrow z_1^{pI} < z_1^{p}$$

$$p'(z_1^{nI}) = -\frac{1}{2L_1} < p'(z_1^{n}) = -\frac{1}{2L_1} + \frac{r[1 - p(z_1^{n})]}{2} \rightarrow z_1^{nI} < z_1^{n}$$

REFERENCES

[1] W. Shim, "Interdependent risk and cyber security: An analysis of security investment and cyber insurance," Michigan State University Ph.D., 2010.

[2] J. Brodkin, "TJX breach may spur greater adoption of credit card security standards," in *Network World*, ed, 2007.

[3] X. Zhao, *et al.*, "Managing Interdependent Information Security Risks: An Investigation of Commercial Cyberinsurance and Risk Pooling Arrangement," presented at the Thirtieth International Conference on Information Systems, Phoenix, AR, 2009.

[4] R. Böhme, "Cyber-insurance Revisited," in *Workshop on the Economics of Information Security 2005*, Cambridge, MA, 2005.

[5] J. Bolot and M. Lelarge, "Cyber insurance as an incentive for Internet security," in *Workshop on the Economics of Information Security 2008*, Hanover, NH, 2008, pp. 25-28.

[6] T. Grance, *et al.*, "Security guide for interconnecting information technology systems," *NIST Special Publication*, pp. 800-47, 2002.

[7] L. J. Camp and C. Wolfram, "Pricing security," in *The CERT Information Survivability Workshop*, Boston, 2000, pp. 31–39.

[8] D. Lakdawalla and G. Zanjani, "Insurance, self-protection, and the economics of terrorism," *Journal of Public Economics*, vol. 89, pp. 1891-1905, 2005.

[9] A. Muermann and H. Kunreuther, "Self-protection and insurance with interdependencies," *Journal of Risk and Uncertainty*, vol. 36, pp. 103-123, 2008.

[10] L. Gordon, *et al.*, "A framework for using insurance for cyber-risk management," *Communications of the ACM*, vol. 46, pp. 81-85, 2003.

[11] J. Kesan, *et al.*, "The Economic Case for Cyberinsurance," presented at the Securing Privacy in the Internet Age Symposium, Stanford, CA, 2005.

[12] H. Ogut, *et al.*, "Cyber Insurance and IT Security Investment: Impact of Interdependent Risk," in *The Workshop on the Economics of Information Security*, Cambridge, MA 2005.

[13] H. Varian, "Managing Online Security Risks," in *The New York Times*, ed, 2000.

[14] H. Kunreuther and G. Heal, "Interdependent security," *Journal of Risk and Uncertainty*, vol. 26, pp. 231-249, 2003.

[15] D. Dzung, *et al.*, "Security for industrial communication systems," *Proceedings of the IEEE*, vol. 93, pp. 1152-1177, 2005.

[16] G. Tally, "Phisherman: A Phishing Data Repository," in *Conference For Homeland Security, 2009. CATCH '09. Cybersecurity Applications & Technology*, 2009, pp. 155-160.

[17] R. J. Turk, *Cyber incidents involving control systems*: Idaho National Engineering and Environmental Laboratory, 2005.

[18] J. Bolot and M. Lelarge, "A new perspective on internet security using insurance," in *the 27th Conference on Computer Communications (INFOCOM '08)*, Phoenix, AZ, 2008.

[19] M. Doll, "Security & Technology Solutions: The 2002 Ernst & Young Digital Security Overview: An Executive Guide and Diagnostic," *Ernst & Young LLP*, 2002.

[20] H. Ogut, "Information technology security risk management," Ph.D. 3210675, The University of Texas at Dallas, Dallas, Texas, 2006.

[21] T. R. Weiss, "Security holes closed in New York Times intranet after hacker intrusion," in *Computerworld*, ed. Framingham, MA IDG Enterprise, 2002.

[22] T. Bandyopadhyay, "Mitigation and transfer of information security risk: Investment in financial instruments and technology," Ph.D. Dissertation, The University of Texas at Dallas, 2006.

[23] J. Bhattacharya and N. Sood, "Health Insurance and the Obesity Externality," *Advances in Health Economics and Health Services Research*, vol. 17, pp. 279-318, 2006.

[24] A. Hau, "A Note on Insurance Coverage in Incomplete Markets," *Southern Economic Journal*, vol. 66, pp. 433-442, 1999.

[25] M. Quaas and S. Baumgartner, "Natural vs. financial insurance in the management of public-good ecosystems," *Ecological Economics*, vol. 65, pp. 397-406, 2008.

[26] P. Schoemaker, "The expected utility model: its variants, purposes, evidence and limitations," *Journal of Economic Literature*, vol. 20, pp. 529-563, 1982.

[27] J. Hirshleifer, *Investment, interest, and capital*: Prentice-Hall Engel wood Cliffs, NJ, 1970.

[28] I. Ehrlich and G. S. Becker, "Market Insurance, Self-Insurance, and Self-Protection," *The Journal of Political Economy*, vol. 80, pp. 623-648, 1972.

[29] B. Powell, "Is cybersecurity a public good? Evidence from the financial services industry," *Journal of Law, Economics and Policy*, vol. 1, pp. 497-510, 2005.