INTERDEPENDENT RISK AND CYBER SECURITY: AN ANALYSIS OF SECURITY INVESTMENT AND CYBER INSURANCE

By

Woohyun Shim

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Communication Arts and Sciences – Media and Information Studies

2010

ABSTRACT

INTERDEPENDENT RISK AND CYBER SECURITY: AN ANALYSIS OF SECURITY INVESTMENT AND CYBER INSURANCE

By

Woohyun Shim

An increasing number of firms rely on highly interconnected information networks. In such environments, defense against cyber attacks is complicated by residual risks caused by the interdependence of information security decisions of firms. IT security is affected not only by a firm's own management strategies but also by those of others. This dissertation investigates the effects of interdependent IT security risks on two widely used security risk management tools – investment in self-protection and cyber insurance. An economic perspective is utilized that permits a systematic exploration of managerial and policy implications of interdependent risk and of possible responses that can help improve information security.

This dissertation first demonstrates that the presence of interdependent risks gives rise to different externality problems: investments to defend against targeted attacks such as hacking and distributed denial of service (DDoS) attacks cause negative externalities, whereas protections against untargeted attacks such as viruses, worms, Trojan horses and spyware generate positive externalities.

Chapter 3 of the dissertation theoretically explores the effects of interdependent risks on information security risk management strategies – information security investment and the purchase of cyber insurance products. It demonstrates that compared to a situation with

independent security risks, the level of the investment in the context of interdependent security risk is not socially efficient. In the presence of targeted attacks, firms overinvest in information security whereas in the presence of untargeted attacks firms underinvest in information security. We also found that, compared to the case of independent security risks, in the presence of positive externalities firms purchase less or equal insurance coverage while in the presence of negative externalities firms purchase equal insurance coverage. We concluded that the adoption of cyber insurance can at least partially solve the overinvestment problem whereas the underinvestment problem becomes more severe.

Chapter 4 uses data extracted from the 2007 and 2008 Korean Information Security Surveys to empirically test the hypotheses derived from the theoretical exploration. Although only some of the theoretical findings were tested empirically because of the limitation of the data, the dissertation found evidence that supports some of the findings: compared to firms experiencing untargeted attacks, firms experiencing targeted attacks invest less in information security and purchase less cyber insurance policies.

The dissertation is the first theoretical and empirical study linking different types of cyber attacks to information security management decisions. It contributes to the research on cyber security. Moreover, it might help organizations to improve security decisions and governments in formulating policies that lead to better social outcomes.

I dedicate this dissertation to

my wife, Boyoun Kim, and my daughter, Claire Shim,

for their unconditional love and support.

ACKNOWLDEGEMENTS

A number of people have provided invaluable support and help; I was able to complete this dissertation and my doctoral degree because of them. Since it may not be possible to name all of them, in this space, I would like to express my sincere appreciation to the most important ones.

First, I thank members of my dissertation committee for their insightful feedback and guidance. I am particularly grateful for the unconditional help I received from my dissertation director and committee chair, Dr. Johannes Bauer. He has always been there for me, giving me invaluable advice through my Ph.D. process. He introduced me to the area (of the economics of cyber security), and provided me with the indispensable intuition and instruction to design and draft my dissertation as well as several other studies. I believe he is one of the best advisers a Ph.D. student could ever have at Michigan State University. Drs. Steve Wildman and Kurt DeMaagd have been superb counselors to me. Particularly, their suggestions on the theoretical modeling have made it possible to enrich my dissertation. I would also like to thank Dr. Steve Lacy who have suggested numerous ideas and improvements which made my understanding on the empirical study deepen.

On a personal note, the completion of this dissertation and my degree would not have been possible without the support of many persons. Particularly, my parents, Daepyung Sim and Myungock Ahn, my parents in law, Mingon Kim and Younghee Ko, my brothers, Woojung Shim and Woochan Shim and their families, and my brother in law, Jongwoo Kim, deserve for

special thanks for their love and encouragement. My friends, Youngjoo Choi, Wooyoung Joo, Jeunga Lee and Hyuna Lee, also deserve sincere thanks for their support and help.

I offer special thanks to Kiyoun Beak and other staffs of the Korea Internet & Security Agency (KISA) for affording me access to data. This study was possible thanks to their cooperation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background

The rapid proliferation of information technologies has changed the environment in which firms operate and the ways they do business. Most firms now store proprietary information in their computer systems and transact with other firms via the Internet and dedicated network connections. The increased use of information and telecommunication technologies interconnects their information technology (IT) systems (Bandyopadhyay, 2006). While this rapid proliferation of information technologies has provided great benefits to organizations, for example in the form of increased productivity, it has also escalated their exposure to IT security breaches: there has been an explosion of malicious activities such as hacking, distributed denial of service (DDoS) attacks, phishing, pharming and a spread of viruses and worms, that endanger the soundness of organizations' security. For example, in South Korea, one of the world's most wired countries, in 2008, private information concerning roughly 10 million customers was leaked through hacking attacks on Internet Auction Co., Ltd, the national affiliate of eBay. Two years later, in 2010, it was discovered that private information on about 20 million customers of the major Korean retailer Sinsegae and 24 other companies had been obtained by Chinese hackers. In addition, in July of 2009, the websites of key government agencies and private companies suffered temporary paralyses or severe access disruptions due to a series of DDoS attacks. Similarly, in the U.S., hackers stole information on at least 200,000 credit card accounts and 40 million accounts with personal information from CardSystems Solution in June of 2005. HSBC Holdings and Data Processors International also had credit card account information stolen in 2003 and

2005. More recently, TJX Companies, Inc revealed that it had experienced a significant data breach caused by hackers breaking into its systems, and disclosed that an estimated 45.7 million credit and debit card records were stolen (Brodkin, 2007). These security breaches, understandably, draw tremendous attention, notwithstanding the difficulty in calculating the exact amount of damages or losses from them.

Although different motivations underlie various types of cyber attacks, the most commonly referenced ones are criminal, monetary and political motivations.[1] Hackers driven by criminal intent have, for example, used information technologies to disrupt police operations. In 1995, the Amsterdam police experienced a serious interruption of an investigation due to hackers who broke into its communication system (Kruyer, 1997). Politically motivated attacks are conducted by pressure groups and organized terrorist organizations. These groups use direct action tactics, opposition movements or terrorist attacks and employ communication technologies to pursue ideological goals and seek political change. For example, popular Indian websites have been attacked by pro-Pakistan hackers and U.S. websites, including those belonging to government agencies, have been attacked by pro-Chinese hackers for political reasons (Vatis, 2001). Cyber attackers who are primarily motivated by financial gain use their techniques to divert funds or extort money from businesses. They attack IT networks and seek security flaws for profit (Evers, 2005).[2] It is obvious that, no matter what the motivation involved, cyber attacks result in some

---

[1] Some researchers have used different models to classify the motivations of cyber perpetrators. Taylor (1999), for example, classified motivations into six categories: "feelings of addiction, urge of curiosity, boredom with the educational system, enjoyment of feelings of power, peer recognition, and political acts". Furnell and Warren (1999) argued that the motivations are "financial gain, revenge, ideology or just plain mischief making". Similarly, Turgeman-Goldschmidt (2005) discussed such other common motivations as curiosity, thrill-seeking, and lack of money.

[2] In addition, Rathmell (1999) divided cyber attackers into amateurs and professionals. The amateurs usually attack IT networks not for disrupting the information activities but for

level of adverse effect on the attacked party (Furnell & Warren, 1999). In some cases cyber attackers may have combined motivations (e.g., pursue both criminal and monetary goals).

There is increasing evidence, however, that cyber attacks today are motivated largely by monetary gain (Young, Zhang, & Prybutok, 2007). According to a Symantec Internet Security Threat Report (2007), the increased number of cyber attacks has primarily focused on data theft, data leakage and the spread of malware for stealing confidential information that can be used for monetary gain. Evers (2005) also found that financial profit was the key motivator of cyber attacks.[3] These financially motivated attacks, once realized, brought about considerable financial losses to victims.[4] For example, several Korean companies went offline after a series of DDoS attacks and were threatened by attackers that the attacks would be continued if the companies do not pay some money (Moon, 2008). Similarly, some online shopping companies in Korea had their websites hacked into and were warned that user information would be exposed unless the companies paid a ransom (Kang, 2010).

Increased interconnectivity, along with the explosion of cyber attacks noted above have therefore raised the concerns of public and private organizations. As a result, many organizations have begun to increase their investment in information security by continually adopting a range of more refined technical security solutions and hiring more employees who devote their effort to information security (Xia Zhao, 2007; X Zhao, Xue, & Whinston, 2009). Various detective and preventive mechanisms have become critical tools in dealing with IT security risks, thus enabling

---

exploring information systems for the sake of curiosity. The professionals, on the other hand, work individually or work for clients such as business intelligence firms engaged in industrial espionage and criminal organizations intent on outwitting policy surveillance or on perpetrating electronic frauds.

[3] Symantec said that a cyber perpetrator who controls 5,500 zombie PCs can earn $350 a week, according to an article in CNET News (Evers, 2005).

[4] According to the Internet Security Threat Report published by Symantec, a data breach of a U.S. firm costs average $6.75 million in 2009 (Symantec, 2010).

firms to identify IT security weaknesses and cope with IT security breaches (Ogut, 2006). However, as indicated by several surveys (L Gordon, Loeb, Lucyshyn, & Richardson, 2005, 2006; Richardson, 2007, 2008) and studies (Lawerence Gordon & Loeb, 2002), despite the high investment in information security, cyber threats and security breaches have steadily increased on a global scale.

It is therefore increasingly recognized that, to deal with security risk efficiently, IT security problems need to be considered from economic in addition to technical perspectives. The economics of information security has become a flourishing and dynamic research area. Economic views in combination with technology-based approaches to information security make it possible to address various security issues, such as interdependent risks and incentives of security investments, which cannot be solely addressed through a technical lens. Correspondingly, some researchers (e.g., R. Anderson & Moore, 2006; R. Anderson, Moore, Nagaraja, & Ozment, 2007; Kunreuther & Heal, 2003; Varian, 2000, 2004) have begun to employ economic concepts, such as externality, free riding, reliability, and moral hazard, to explore information security problems. These new research approaches have generated various interesting and innovative proposals and this dissertation adopts some of the approaches to investigate information security risk management strategies.

This dissertation therefore intends to investigate the effects of cyber attacks on two widely used security risk management strategies – information security investment and cyber insurance – and their relationship from the newly proposed economic perspectives, and to explore managerial and policy implications in order to improve information security. More explicitly, the primary objective of this study is to provide a detailed picture of IT security risk management strategies within the context of different externality problems caused by interdependent

information security risks in the intensely interconnected business world.

1.2 IT Security Risk and its Management

1.2.1 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 (Dzung, Naedele, Von Hoff, & Crevatin, 2005; Tally, 2009). Therefore, adversaries launching untargeted attacks intend to harm any vulnerable system which can be found on a network (Dzung, et al., 2005; Turk, 2005). Common examples of untargeted attacks include viruses, worms, trojan horses, and spyware. Figure 1-1 shows untargeted attacks schematically.

"Targeted" attacks are designed to damage a particular communication system or a firm's information assets, for such purposes as industrial espionage, terrorism or monetary gains (Dzung, et al., 2005; Tally, 2009). Attackers using such strategies typically collect information about the target, customize attacks for each particular victim, and thus know who will be attacked (Dzung, et al., 2005; Turk, 2005).[5] Examples of targeted attacks are malicious hacking and whaling. The scheme of targeted attacks is depicted in Figure 1-2.

[5] Several authors (e.g., Cavusoglu & Raghunathan, 2004; R. A. Martin, 2001; Radianti & Gonzalez, 2007) argued that there are typically two types of cyber attackers: 'white hats' and 'black hats'. The term white hats refers to persons who use their skills for "altruistic" and "legitimate" purposes, e.g., help organizations identify system vulnerabilities (Main & van Oorschot, 2003; R. A. Martin, 2001). On the other hand, black hats (known as crackers) are persons who break into organizations' systems or networks for "malicious" and "criminal" purposes, e.g., for personal gains (Main & van Oorschot, 2003; R. A. Martin, 2001; Young, et al., 2007). While white hats are mostly concerned about their reputation (L. Jean Camp, 2006), most black hats seem to seek monetary gains (Young, et al., 2007). Cyber attacks referred in this study are assumed to be conducted by black hats who attack organizations for profit since white hats are usually not threats to organizations.

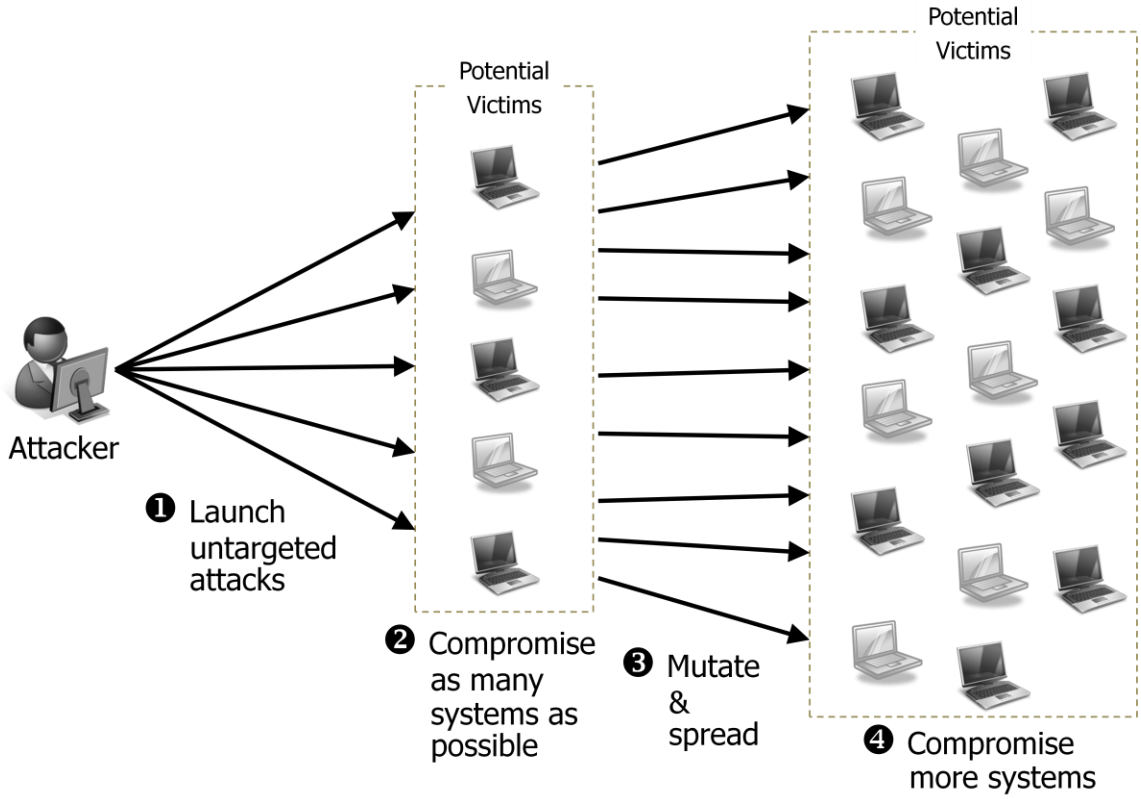


Figure 1-1. Typical Untargeted Attacks

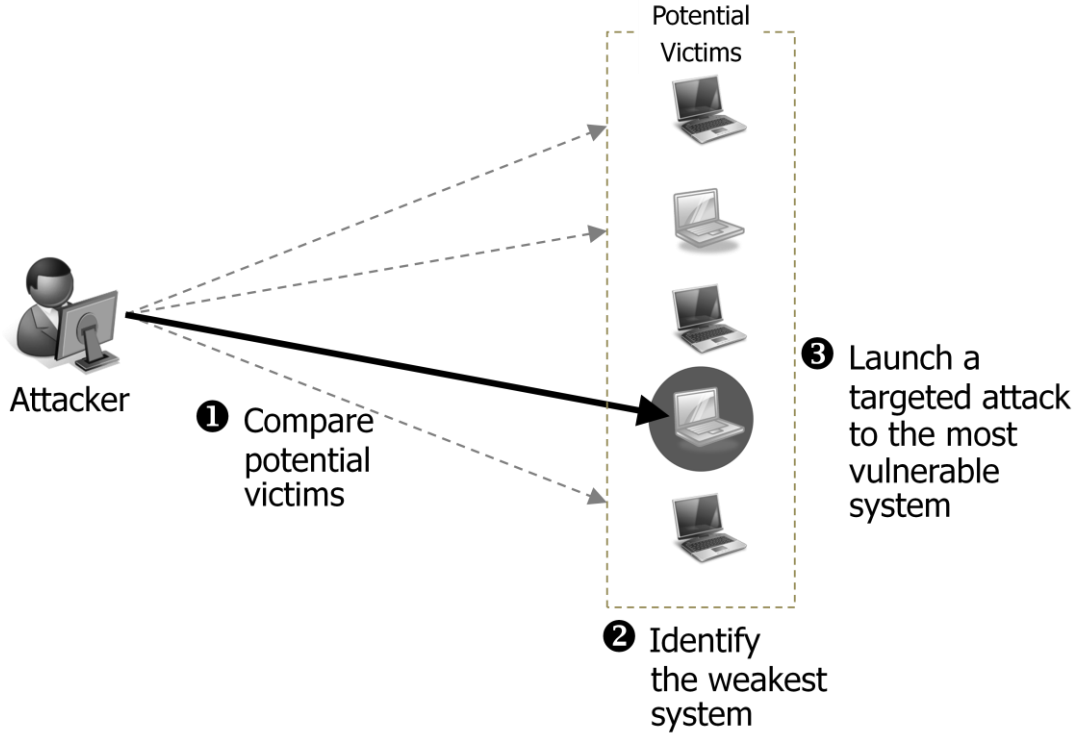


Figure 1-2. Typical Targeted Attacks

Although not considered in this study, there can be another type of attack: hybrid attacks. This type of attacks is the combination of 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 is infected in the first stage (see Figure 1-3). Since some malicious software can create backdoors on infected systems, the adversaries can easily gain access to the systems. Second, the adversaries may attack particularly vulnerable systems using infected machines in the first stage (see Figure 1-4). 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.

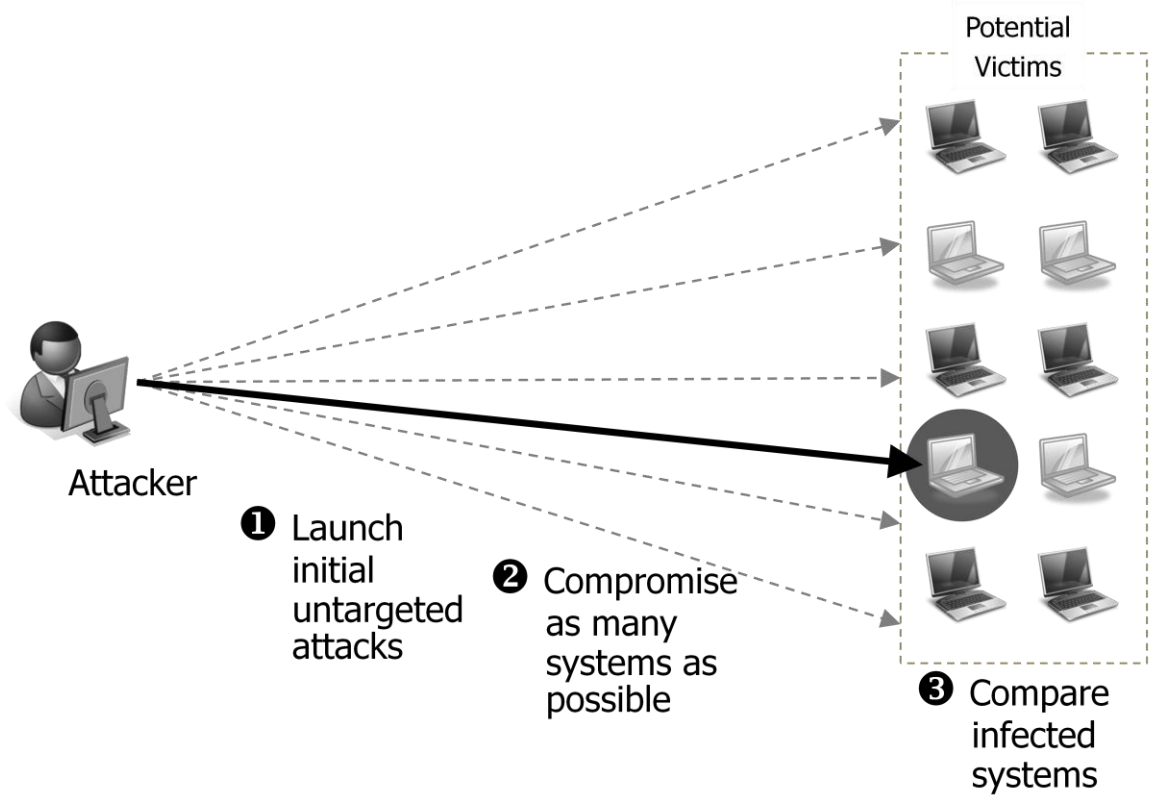


Figure 1-3. First Type of Hybrid Attacks

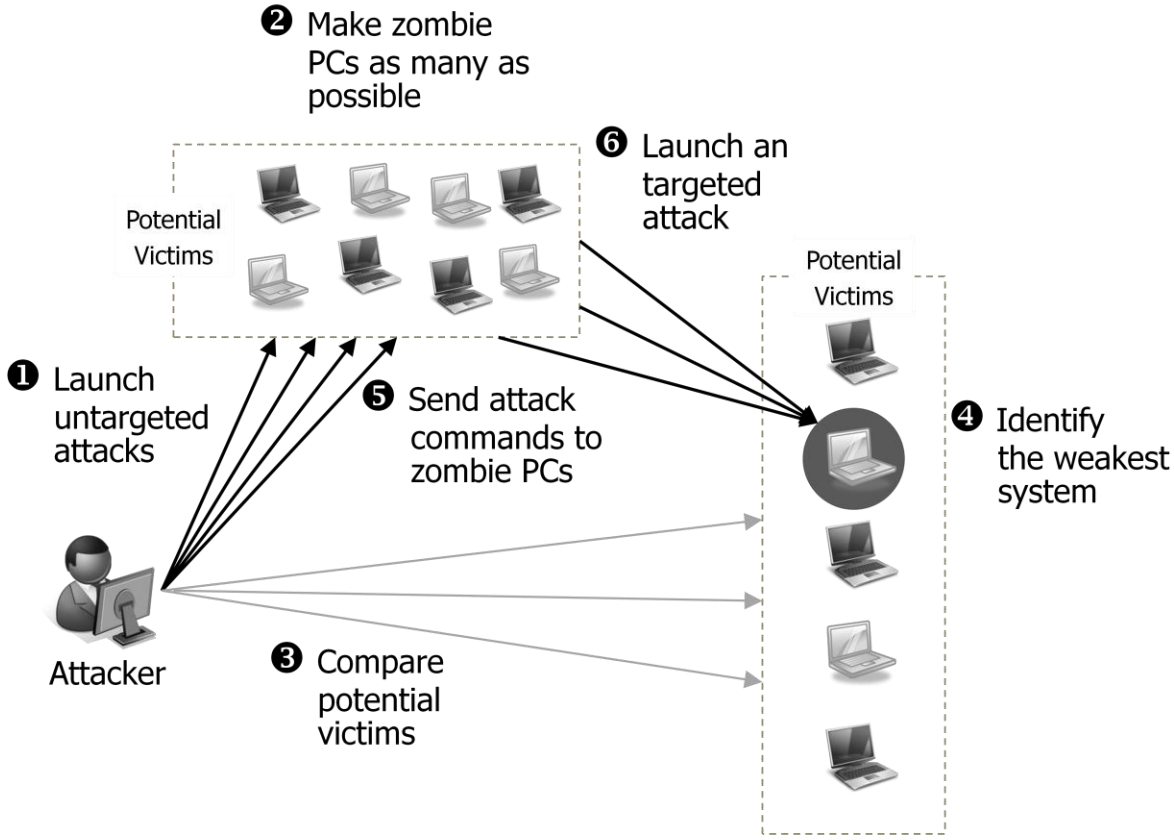


Figure 1-4. Second Type of Hybrid Attacks

The proposed categorization, which limits the types of cyber attacks to either targeted or untargeted attacks, has pros and cons. On the one hand, it simplifies the theoretical model and allows a crisper 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 affects a firm's security risk management strategies. For example, in the first type of hybrid attacks, the targeted attack following an initial infection by an untargeted attack can be avoided if servers can be protected from the initial attack wave.

1.2.2 Self-Protection, Self-Insurance and Cyber Insurance

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.[6] Self-protection (also known as 'loss prevention') attempts to reduce the probability of security breaches by employing such measures as firewalls, anti-virus software, authentication, and intrusion detection systems (IDSs). In contrast, self-insurance (also known as 'loss protection') attempts to minimize a loss caused by a security incident by deploying measures such as data backup systems and disaster recovery planning.

However, several studies (e.g., Doll, 2002; Ogut, 2006; Weiss, 2002) have questioned the effectiveness of sole dependence on this traditional security investment model, implemented by self-protection and self-insurance. This research claims that approaches such as detection and prevention of cyber attacks and protection of information systems against cyber attacks cannot solve IT security problems. This is primarily because of two key factors: imperfect detection and protection, and interdependency of IT security risks. In terms of the first factor, firms might not be able to fully protect their IT systems against cyber attacks or may even fail to detect the attacks since perpetrators continually use newer tactics which may not be detected by firms as most of the technical solutions are developed reactively in response to the detection of newer security flaws (Bandyopadhyay, 2006). Even if solution developers have great commitment and dedication to detect vulnerabilities or security problems, not all potential problems can be identified. Thus, solution developers release security patches for security problems often after the

[6] As Bolot and Lelarge (2008b) 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 dissertation, we do not distinguish them and refer them simply as self-protection.

problems are revealed (Majuca, 2006). As a result, while increased adoption of various technical solutions such as firewalls, IDSs and various encryption technologies may help organizations to reduce IT security vulnerabilities and to avoid potential losses from IT security breaches, organizations also have recognized that perfect defenses against cyber attacks may not be achievable or may even be undesirable if the cost is higher than the expected benefits.

In terms of the second factor, interdependent security risks, because of integrated and interconnected information systems, security breaches of one organization can readily spread to other organizations. Information sharing among organizations makes IT systems vulnerable not only at the level of the victimized organization but also for organizations sharing information assets with that organization (Bandyopadhyay, 2006; Ogut, Menon, & Raghunathan, 2005). Consequently, deficiencies in abilities for efficient 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 complement the weaknesses of traditional security management strategies.

Market insurance is a traditional instrument for shifting residual risks beyond due diligence (Bandyopadhyay, 2006). 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 were first introduced in the late 1970s (Majuca, Yurcik, & Kesan, 2006). These products merely extended traditional insurance policies to electronic banking in order to cover victims from losses caused by outsiders gaining physical access to computer systems (Majuca, 2006).

Early insurance policies for protecting policyholders against computer crime only covered physical damage from cyber crime. However, as the Internet era unfolded, new forms of cyber crime caused an increasing number of losses or damage of intangible assets. including lost data and information theft (Beh, 2001). Since the data and information managed by organizations do not, in many cases, exist in physical form, those insured by traditional insurance policies failed to get coverage for their loss of data and information from insurers (Majuca, 2006; Norman, 2001). The inability of early cyber insurance policies to deal with this problem resulted in costly litigation between insurers and cyber victims and insurers' attempts to avoid including intangible losses in insurance coverage (Majuca, 2006). Adopting traditional insurance policies in the field of information security therefore is not seen as an appropriate approach to hedge against IT security risks.

In addition, as Crane (2001) and Gold (2002) indicated, there is a significant risk that the insurance policies will not cover activities that occurred outside the specifically designated coverage area. As a result, given both increased IT security risks and the failure of insurance to manage the new characteristics of cyber risks, the demand for insurance products particularly designed to target cyberspace has increased.

Consequently, since the late 1990s, several insurance policies (known as 'early hacker insurance policies'), specifically designed to target cyber losses, were introduced.[7] These insurance produces were offered by several hardware/software companies teaming up with insurance companies (Majuca, 2006). As a result, these policies were not stand-alone insurance products, but part of risk management solutions offered by the companies to their customers.

[7] The examples are insurance policies introduced by ICSA TruScure, Cigna Corp/Cisco Systems/NetSolve, J.S. Wurzler Underwriting and IBM/Sedgwick in 1998, Counterpan/Lloyd's London and AIG in 2000, and Marsh McLennan/AT&T in 2001 (Majuca, 2006)

Further, these policies did not provide full insurance coverage.

Recent increased Internet risks due to more complex and organized cyber attacks, however, have resulted in a need for more advanced mechanisms to respond effectively to these increased risks. Accordingly, several cyber-liability laws which require a higher standard of compliance in certain IT-related activities were enacted (Majuca, 2006).[8] Increased Internet risks and stronger compliance obligation, brought about the emergence of more sophisticated cyber insurance products (Majuca, 2006).[9] These insurance policies covered not only losses, such as physical damages that were addressed by traditional insurance products, but they also provided coverage for intangible damages. According to Gralla (2001), the coverage of cyber insurance includes "DDoS attacks that bring down e-commerce sites, electronic theft of sensitive information, virus-related damage, losses associated with internal networks crippled by hackers or rogue employees, privacy-related suits, and legal issues associated with copyright and trademark violations".

1.2.3 Cyber insurance in Korea

Although self-protection and self-insurance strategies show similar trends worldwide and thus might be explained universally, cyber insurance has a relatively short history with widely varying levels of development in each country. Since our empirical data stem from Korean surveys, a brief discussion of the current conditions of cyber insurance in Korea is appropriate. Unlike physical damage to tangible properties which can be covered by insurance policies, damage

8 For example, in the U.S., the Gramm-Leach-Bliley (GLB) Act's security regulations issued in 2001 and the HIPAA security regulations passed in 2003 require certain types of firms to adopt appropriate security standards such as risk assessment and implementation of information security programs (Majuca, 2006).

9 These products include Marsh's NetSecure, AIG, Inc.'s NetAdvantage Security, NetAdvantage and NetAdvantage Pro, Lloyds of London's e-Comprehensive or Computer Information and Data Security Insurance; and Fidelity and Deposit's E-Risk Protection Program (Majuca, 2006)

caused by IT security breaches is frequently intangible, and, consequently, may not be covered by insurance policies (Beh, 2001). In addition, although traditional insurance policies have a designated coverage area and a place where an event must occur, cyber attacks can be launched anywhere in the world (Majuca, 2006). As a result, because of the inability of traditional insurance products to deal with the characteristics of cyber attacks, new insurance products which are specifically designed to cover cyber threats were introduced (Majuca, 2006).

In Korea, one of the leading countries in cyber security, the first cyber insurance product 'e-Biz Liability Insurance' was introduced in 1998. It was developed in the private sector by insurance companies such as Samsung Fire & Marine Insurance and LIG Insurance. The target clients of this product were Internet data centers and firms which provide Internet service (e.g., Internet service providers). Although this product covered destruction of data and information assets, the coverage was limited to physical damage such as network disruption and computer system malfunction. Moreover, the coverage did not include losses from hacking attacks, virus infection or theft of customer information. In 1999, several Korean insurance companies introduced a new insurance policy – 'Net Secure Comprehensive Insurance' – targeting all businesses that use network technologies. Unlike 'e-Biz Liability Insurance', this insurance policy had broader coverage for intangible damage caused by hacking, virus infection and the leaking of private information. This product covered not only the insured firm's own loss but also damage to third parties. However, the insurance companies offered the cyber insurance products with only $10,000 maximum coverage per an incident, as this was an uncertain and unknown field.

From 2000, there have been a series of cyber attacks in Korea. For example, in July 2000, around 250 major servers were broken into by a series of hacking attacks. Not only did the

attackers hack Korean government agencies, they also obstructed major businesses by secretly installing the 'Trinoo' DDoS program which causes an outage of services in compromised servers. Another example is the Slammer Internet worm, which appeared in January 2003. The Internet worm impaired network systems in Korean public and private sectors and caused a shut-down of most Internet services. The increased number of cyber attacks and the losses they caused highlighted the need for more detailed and sophisticated cyber insurance policies[10] and new strategies for governing IT security.

Consequently, there has been a growing effort to enact cyber liability regulations. Recently passed regulations attempted to update standards for highly networked environment and clarify liability rules given a series of extensive cyber incidents. Thus, these regulations required organizations to comply with a higher legal standard, particularly organizations with databases of financial and credit information as well as private information. For instance, in 2001 and 2003, the Electronic Signature Act, which was initially passed in 1999, was revised. Through these revisions, government expanded the definition of electronic signature to include more diverse digital environments and established higher standards for the security and reliability of electronic signatures. Another example is the e-Financial Transaction Act which was adopted in 2006. This act not only prescribed the shift of responsibility for losses caused by cyber financial accidents from customers to financial institutions, but also mandated that all financial institutions purchase cyber insurance in order to protect customers from hacking and theft of personal data.

Due to increased cyber threats and a higher standard of compliance, there was not only an expansion of coverage in existing insurance policies, but also the emergence of new cyber

[10] For example, after the spread of the Slammer Internet worm in 2003, the insurers, which provided 'e-Biz Liability Insurance', excluded Internet worm infections from the insurance coverage, as the reinsurance industry categorized Internet worm infections as natural calamity.

insurance products.[11] These insurance products were more complex than the early cyber insurance products in that these covered broader areas with higher maximum coverage. For example, the existing cyber insurance product, e-Biz Liability Insurance, expanded its coverage to include losses arising from intangible damages, such as DDoS and hacking attacks, theft of business information and data disruption causing monetary loss to customers, and broadened its target customers from Internet service providers to general businesses. Another example is the Electronic Transaction Liability Insurance, which was introduced in 2007. This product covers damage caused by various cyber attacks including hacking and DDoS, business interruption, theft or destruction of sensitive information, technology errors and judicial costs. Table 1-1 displays key features of the cyber insurance policies currently offered in Korea.

Table 1-1. Summary Table of Cyber Insurance Products[12]

Starting year	Product name	Maximum Coverage	Coverage
1998	e-Biz Liability Insurance	Max $10K per incident (before 2007) Max $2M per incident (Current)	Data disruption System destruction Network instability Hacking (from 2007) Theft of private information (from 2007)
1999	Net Secure Comprehensive Insurance	Max $5M per incident	Data disruption Business interruption Hacking Virus infection Leak of private information
2006	Private Information Liability Insurance	Max $5M per incident	Leak of private information
2007	Electronic Transaction Liability Insurance	Max $2M per incident	Hacking DDoS Business interruption Theft or destruction of sensitive information Technology errors and judicial costs

[11] In addition, class action lawsuits of victims in response to cyber accidents have recently sprouted. These led many companies to purchase cyber insurance policies which specifically offer third-party coverage.

[12] Note that there have been several cyber insurance products as Netizen Insurance and Private Information Leakage Compensation Insurance, which target individual customers specifically.

1.3 Organization of the Dissertation

The remainder of the dissertation is organized as follows.

The review of the existing literature on information security risk and its management is provided in Chapter 2. This chapter synthesizes important prior work on IT security and risk management, dividing the relevant studies into four areas: research on information security, research related to general insurance mechanisms, research on cyber insurance, and research related to other risk management tools. This chapter captures technical and economic perspectives in information security, and illustrates how market insurance mechanisms as well as other security-improving mechanisms have been adopted to the field of information security as risk management tools.

In Chapter 3, the study turns to a discussion of over- and underinvestment problems caused by interdependent security risks. Recent widespread cyber attacks and malicious activities have caused a rapid increase in organizations' information security investments. A number of studies have investigated the optimal level of security investment for situations of independent risk. However, issues related to security investment within the context of interdependent risks have not yet been sufficiently explored. For example, although previous studies have addressed the security underinvestment problem caused by interdependent risks, the security overinvestment problem has not been fully explored in academia (Powell, 2005; Xia Zhao, 2007). In addition, most of these studies have focused on self-protection mechanisms but not taken insurance mechanisms into account. This chapter therefore expands the current body of research by exploring multiple scenarios of security over- and underinvestment caused by interdependent risks and the interplay between IT security investment and cyber insurance. We 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, empirically testable, 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 chapter further provides an economic rationale for employing insurance mechanisms as a risk management solution for information security.

Despite the rapid growth of literature on information security investment, empirical studies are still sparse. Chapter 4 develops the details of the empirical study to test the theoretical findings of Chapter 3. Data for the empirical study was extracted from the 2007 and 2008 Korean Information Security Surveys published by the Korea Internet & Security Agency (KISA) (2007, 2008). The empirical results support propositions derived in Chapter 3. That is, in the presence of interdependent risk, protections against targeted attacks cause negative externalities, thereby resulting in higher information security investments and insurance policy purchase compared to defenses against untargeted attacks which cause positive externalities. This chapter further presents findings on the association between information security investments and cyber insurance purchase as well as the effects of firms' fundamental characteristics on IT security risk management strategies. Together with the theoretical analysis, the empirical results yield important insights about managerial and policy implications regarding IT security risk management and cyber insurance.

In Chapter 5, we conclude the dissertation with a discussion of our theoretical and empirical

findings and their implications. This final section also discusses directions for possible further research.

It should be noted that, to assist the reader, a certain level of redundancy was deliberately built into the dissertation. For that reason, the introductory sections to Chapters 3 and 4 reiterate key contextual information in order to make each chapter more self-contained.

To our best knowledge, this dissertation is the first study which connects targeted and untargeted cyber attacks to a comprehensive mechanism of information security risk management strategies that include both information security investments and cyber insurance with interdependent risk. It extends the existing literature of Ogut et al (2005) and Kunreuther & Heal (2003) on the economics of information security in the following manner. First, the dissertation considers both security investment and cyber insurance as risk management tools. Second, unlike Ogut et al. (2005) and Kunreuther & Heal (2003) who assume that security investments in the scenario of interdependent risks cause positive externalities, we consider an additional case where security investments can, to the contrary, generate negative externalities given certain types of security risks. This study is also unique in that we derive a number of new propositions that are not investigated in the existing literature, and derive empirically testable hypotheses on the effects of interdependent risk on the level of IT security investment and the purchase of a cyber insurance policy.

The dissertation expands and complements the current body of research by exploring the effects of the different types of security risks which cause interdependent risks on comprehensive risk management tools encompassing IT security investment and cyber insurance.

CHAPTER 2

LITERATURE REVIEW

This study is grounded in two distinct, but interconnected research areas: Economics of IT security and insurance economics, which can both inform an organization's IT risk management strategies. We first review the literature on information security and traditional insurance economics and then explore studies on cyber insurance and other risk management tools which have evolved as a new paradigm for managing IT security risk.

2.1 Information Security

Since Martin (1973) and Madnick (1978) discussed the links between information security risks and countermeasures, a vast literature has been published dealing with security management strategies for coping with information security risks. There are two major streams of research related to strategies for effective information security risk management.

The first stream is technology-oriented. The objective in this early era of research on information security was to increase our understanding of security risks and develop corresponding effective security countermeasures, primarily from a technical perspective. Researchers during this era investigated how to develop, improve and configure technical security measures in order to operate at optimum levels of detection and protection. Therefore, a large number of conceptual studies (e.g., J. Anderson, 1972; Axelsson, 1998; Friedman, 1988; Hsiao, Kerr, & Madnick, 1979; Wiseman, 1986) were conducted to develop effective technical security countermeasures that could reduce the probability of loss (self-protection) and the size of loss (self-insurance) (Ogut, Raghunathan, & Menon, 2005). These studies asserted that

technical security solutions, such as firewalls and IDSs, help decrease the probability of security risks.[13]

As information systems became more connected via the Internet, researchers began to be concerned about information security issues stemming from outside as well as inside threats although the focus remained on technical issues. Many studies in the field of computer science and telecommunications mirrored these concerns and discussed how the vulnerability of information systems could be overcome through technical measures (e.g., Cohen, 1995; Denning & Denning, 1997; Mukherjee, Heberlein, & Levitt, 1994). Contributors to this literature, therefore, have mostly focused on deploying technologies for detection, prevention and mitigation. While the literature on technical aspects of IT risk management grew, and a variety of technical security measures were widely adopted, information security breaches nevertheless became more pervasive and severe.

In response, some researcher such as Finne (1998), Buzzard (1999) and Meadows (2001) started to try to move beyond technology-oriented approaches to study information security risk management more broadly. This second stream of research was primarily based on economic perspectives on information security risk management, recognizing that information security is more than a technological issue. For example, Gordon and Loeb (2002) investigated the optimal level of information security investment in a risk neutral organization. Although their study did

[13] Although limited, some studies have emphasized the effectiveness of managerial and organizational security measures (e.g., Parker, 1981; Parker, 1983). Researchers in this field indicated that managerial and organizational security measures, such as security guidelines, policy statements and security staffs, are effective security measures for organizations trying to reduce security breaches. In addition, scholars such as Straub Jr. (1990), Straub Jr. & Nance (1990) and Straub Jr. & Welke (1998) conducted empirical analysis encompassing both technical controls, and managerial and organizational controls. They concluded that technical, managerial and organizational controls are all important and efficient security measures and should be taken into account for effective information security.

not take interdependent security risk into account, it provided a guide to understanding how vulnerability of information assets affects an organization's level of IT security investment. Using census data of Japanese local governments, Tanaka et al. (2005) found support for the results of Gordon and Loeb. In contrast, other researchers, such as Campbell et al. (2003) and Cavusoglu et al. (2004), explored the impact of a security breach on a firm. Campbell et al. (2003) investigated the relationship between a reported security breach and information assets influenced by the breach, and concluded that security breaches of confidential information generate higher negative economic effects than other types of information breaches.

Since the early 2000s, through pioneering contributions by authors such as Varian (2000), Camp & Wolfram (2000), Anderson (2001), and Gordon & Loeb (2002), studies in this stream have begun to incorporate unique aspects of information security risks. To this end, several microeconomic theories were used to study aspects such as misaligned incentives between stakeholders (including asymmetric information, moral hazard and adverse selection) and externalities (including network effects and interdependency).

Misaligned incentives, in particular, have been extensively studied in information security. Varian (2000) and Anderson (2001) were among the first contributors who demonstrated that misaligned incentives hinder successful deployment of security measures. They argued that asymmetric information and moral hazard caused by perverse incentives should be taken into account in effective analyses of information security problems. Subsequently, several researchers used game-theoretic approaches to illustrate economic incentive problems related to information security. Anderson et al (2007) argued that even if there is more spending on information security, security breaches cannot be avoided when moral hazard and adverse selection caused by misaligned incentives exist, as may be the case if the entities (i.e., individuals and organizations)

who are responsible for system security do not directly suffer losses resulting from security breaches. They therefore concluded that, without proper liability regimes, these problems might distort entities' incentives to invest in information security, and thus jeopardize entire security systems.

Though a relatively new focus in research on information security, externalities caused by interdependent risks have been analyzed in other security related areas. For instance, in an empirical study of Lojack – a hidden automobile security device used for locating stolen cars – Ayres and Levitt (Ayres & Levitt, 1998) found that, after the introduction of the product in a market, auto theft rates declined because of "positive externality-generating unobservable self-protection". Similarly, Lakdawalla and Zanjani (2005) found that a strong defense of a primary target country against terrorists' attacks causes negative externalities since the terrorists tend to attack allied nations rather than the well-protected primary target country.

In the field of IT security, researchers have also started to address the issues of interdependent risk. Although a substantial portion of this empirical work combines theories from both misaligned incentives and externalities in research, the literature on information security focusing on externalities emphasizes ascertaining the optimal level of security investment and public policy tools. Anderson (2001) first recognized the "externality" inherent in information security. He argued that IT security investments generate positive externalities since, if an organization makes it harder for perpetrators to break into its system, perpetrators may shift their efforts to other organizations' systems. He concluded that this makes implementing effective information security difficult. Kunreuther & Heal (2003) studied the effect of externalities caused by interdependent security risks. They considered a situation where the security risk of a firm can be transferred to other firms. Moreover, firms face two different types

of externalities (i.e., negative and positive externalities).[14] More specifically, they argued that a firm's investment in computer protection will convey positive externalities since the investment will reduce the other firms' possibility of computer virus infections from the firm; and a firm with no investment in computer protection will result in negative externalities because the firm's unprotected computer might raise the risk of other firms contaminated via this unprotected computer. In their model, when the lack of IT security in one system can damage not only that system, but also other systems interconnected with it, either all agents or none will invest in security. The authors concluded that mechanisms such as regulation or insurance might help overcome the externality problems.

Gordon et al. (2003) showed that, in the presences of interdependent security risks, if information assets are shared by organizations, it may enable certain firms to free ride on other firms' security investments which causes an underinvestment problem in IT security. Ogut et al. (2004) found that there is a negative externality in IT security investment among the interconnected organizations since security breach in one organization can transfer to other firms in the network. Varian (2004) analyzed the security investment of a multi-firm information system. He argued that, since system reliability depends on the involved parties' cooperative actions much in the same way that a wall is built to defend a city; system reliability may rely on the sum of players' efforts, or their minimum or maximum effort. Similarly, Powell (2005) addressed how externalities caused by the public good nature of information security can bring

[14] Note that, although Kunreuther & Heal (2003) used negative and positive externalities of security investments in their study, the definitions are somewhat different from our study. While they argued that positive externalities are generated by security investments and negative externalities are caused by not investing in information security, this study only considers externalities caused by IT security investments: that is, security investments can generate either positive or negative externalities.

about both over- and underinvestment problems. He argued that, although firms tend to underinvest in information security due to misaligned incentive, if the government decides the level of information security, firms are likely to overinvest in information security.

2.2 Insurance Economics

Whereas many issues related to cyber insurance will be discussed in the next section, it may be helpful to provide a snapshot of the discussion in the broader field of insurance economics. Since Borch (1960) and Arrow (1963) first discussed the rationale of insurance mechanisms, research on insurance as a risk management tool has flourished. Borch (1960) is one of the pioneers who formulated an optimal insurance contract. In his seminal paper, he derived Pareto optimal insurance policies using the endogenous insurance framework. In another seminal paper, Arrow (1963) investigated the moral hazard problem that arises when insurers cannot observe insureds' efforts for avoiding losses.

Roughly a decade later, the most widely cited studies in this area, written by Ehrlich & Becker (1972) and Rothschild & Stiglitz (1976), were published. Ehrlich & Becker (1972) showed that if potential insureds have a homogenous probability of loss and if information is symmetric between insurers and policyholders, then self-protection and insurance complement each other. On the other hand, Rothschild & Stiglitz (1976) illustrated that adverse selection and moral hazard phenomena arise when there is information asymmetry (perhaps due to the inability of monitoring) and potential insureds have different loss probabilities. They concluded that there might be no equilibrium, or even when equilibria exist, low-risk and/or high-risk individuals may be worse off than they would be otherwise. These studies have been generalized and extended by several researchers, including Schlesinger (1981, 1997), Doherty and Schlesinger (1983), Gollier

(1996), and Breuer (2006). There also have been a number of empirical studies that support the findings from the theoretical literature.

However, as mentioned previously, both the failure of traditional insurance mechanisms to manage the new types of cyber risks and unique aspects of information security risks (e.g., interdependency and information sharing) make it more difficult to use traditional insurance policies to deal with information security risks. This resulted in the development of a new area of research on insurance policies for information security risk management specifically targeting cyberspace.

2.3 Cyber Insurance as a Risk Management Tool

One of the common ways of transferring residual risks beyond due care is to use market insurance mechanisms. Cyber insurance was developed to mitigate IT security risks, particularly in cyberspace. It is designed to cover physical losses such as computer theft and hardware breakdowns well as intangible losses caused by data loss and leaks of confidential information.

Since the introduction of early hacker insurance policies in late 1990s, there has been a growing body of research investigating the role of cyber insurance as a risk management tool. The concept of handling security risks using insurance was first proposed by Lai et al. (1994) and further developed by Geer (1998, 2003) and Schneier (2001, 2002). These authors essentially argued that technical measures are not effective to reduce information security risks as a whole and additional approaches are needed to either mitigate the problems (through procedural means) or transfer them (through insurance). Gordon et al. (2003) discussed the benefits of using cyber insurance as a risk management tool. Gordon and his colleagues designed a framework of employing cyber insurance mechanisms for mitigating IT security risk that

cannot be managed by technology-based solutions. They then argued that organizations need to thoroughly assess their own IT security risks to fill the gap of technology-based solutions (i.e., residual risk) using cyber insurance products. In addition, Yurcik & Doss (2002) and Kesan et al. (2005b) demonstrated that cyber insurance is an attractive market solution for resolving information security problems since organizations have an incentive to reduce insurance premiums by increasing self-protection.

Consideration of the interplay between self-protection and insurance, and interdependent risks inherent in information security, however, has received relatively little, and only very recent, academic attention (Böhme, 2005; Böhme & Kataria, 2006, 2007; Bolot & Lelarge, 2008b; Hofmann, 2007; JP Kesan, RP Majuca, & WJ Yurcik, 2005a; Lelarge & Bolot, 2009; Majuca, et al., 2006; Ogut, Menon, et al., 2005; X Zhao, et al., 2009). Böhme (2005) argued that strong interdependencies among agents may obstruct the deployment of cyber insurance. In subsequent work (Böhme & Kataria, 2006, 2007), researchers distinguished local risk correlations (i.e., correlated risks within a firm) from global risk correlations (i.e., correlated risks across independent firms) and showed that global risk correlations influence an agent to seek cyber insurance while local risk correlations influence the insurance premium. Ogut et al. (2005) found that, although firms might be able to mitigate their security risks by purchasing insurance products, a high level of interdependent risks makes firms buy less insurance coverage, which hinders the development of the cyber insurance market, and also reduces firms' incentives to invest in information security protection. Hofmann (2007) extended the model proposed by Kunreuther & Heal (2003). He argued that in the presences of interdependent risks agents under-invest in self-protection and concluded that compulsory insurance offered by a monopolistic

insurer may resolve the under-investment problem by premium discrimination.[15] Bolot & Lelarge (2008a, 2008b) analyzed the conditions under which cyber insurance could encourage agents to invest more in self-protection. Their key finding was that employing cyber insurance could serve as a strong incentive for agents' increased investment in self-protection. Zhao et al (2009) presented economic models of under- and over-investment in security protection under correlated security risks. They argued that commercial insurance alone cannot address the problem of inefficiency in security investments, which problem could be overcome when commercial insurance was combined with managed security services and risk pooling arrangements.

2.4 Other Risk Management Tools

Although they are not a main focus of this study, it should be noted that there have been numerous economic-based studies that address other types of IT security risk management tools. Sharing security information by organizations is one of the risk mitigation mechanisms which has received great attention in recent years (e.g., Gal-Or & Ghose, 2005; L. A. Gordon, Loeb, & Lucyshyn, 2002; L. A. Gordon, et al., 2003; Hausken, 2007; Ogut, 2006).

Information sharing is considered by many as one of the most desirable ways of complementing security related activities since it can help organizations avoid suffering incidents similar to those experienced by other organizations. As a result of this potential benefit, many

[15] He explained why only compulsory insurance monopolies can internalize externalities (i.e., resolve the underinvestment problem due to interdependent risks) by the following rationale: in the case where security risks are interdependent, while agents tend to underinvest in security, insurers in a competitive insurance market cannot charge higher premium from those agents since other insurers may attract agents by making their premium lower than the insurers. Therefore, he concluded that externalities cannot be internalized in the case of a competitive insurance market.

governments and industry trade associations have made an effort to establish and develop information sharing organizations such as Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs) and Chief Security Officers Round Tables (CSORTs) (L. A. Gordon, et al., 2003).

Gordon et al. (2002, 2003) noted in their studies that information sharing can complement information security investments. They, however, showed that while information sharing can facilitate obtaining the optimal level of information security with a lower cost compared to what is possible in the absence of information sharing, without appropriate incentive mechanisms, it can also cause firms to free ride on the security spending of other firms. Therefore, they concluded that information sharing may result in underinvestment in information security.

Using game theory, Gal-Or and Ghose (2005) addressed the economic incentives for firms sharing security information, and proposed a theoretical framework which can explore the relationship between information sharing and information security investments. They showed that there are strong economic incentives for organizations to share security information if such sharing of information results in sufficiently large positive demand spillovers. They further demonstrated that there exists a complementarity effect between information sharing and security investment.

Ogut (2006) argued that information sharing by one organization reduces the probability of a security breach for the other organization, which, in turn, mitigates its own probability of a security breach caused by an attack via the other organization. He concluded that, since information sharing among members of the alliance reduces the negative effects of interdependent risks, it can increase firms' incentives to increase information security investments and to buy insurance policies.

It has also been suggested that the development of a market for trading security information could serve as a risk mitigation tool. For example, Schechter (2002) and Ozment (2004) argued that, as is also the case with trading commodities, by developing a market for transacting information about software vulnerabilities, software users have incentives to report the problems, and thus software vendors can improve the security of their software.

However, some researchers have argued that unregulated market-based risk mitigation mechanisms such as information sharing may not necessarily result in a better social outcome. Accordingly, some authors, primarily Schneier (2002) and Varian (2000), proposed that liability rules and commitment rules enacted by a government can be very useful for facilitating the mitigation of security problems. In addition, other researchers such as Kannan & Telang (2005) argued that the current type of voluntary information sharing organizations does not provide incentives to members since they do not offer financial rewards to members for identifying security risks. Government-funded information sharing organizations which reward members but do not charge a membership fee are therefore seen by the authors as more effective in identifying security risks.

2.5 Concluding Comments

Information security has been studied in diverse research areas. Many of the studies have shown that technological security measures alone cannot mitigate security risks effectively, and thus various additional risk management mechanisms have been suggested.

This review indicated, however, that there are several areas in the current literature that deserve further study: first, the existing literature on security investment has focusing mainly on the underinvestment problem, but has not dealt with the overinvestment problem; second,

although researchers have explored positive and negative externalities caused by interdependent risks, from both theoretical and, less frequently, empirical perspectives, they have not provided a rationale that accounts for when either positive or negative externalities might be generated; lastly, compared to the number of rapidly increasing theoretical studies, there have been only a few empirical studies on information security.

In order to effectively address the above problems, this study expands the current body of research by employing both theoretical and empirical approaches. Specifically, this study complements the current studies by first investigating, from a theoretical perspective, the effects of targeted and untargeted attacks on comprehensive risk management strategies in the case where interdependent risks exist. It then tests the conclusions derived from the theoretical exploration empirically.

CHAPTER 3

IT SECURITY MANAGEMENT THROUGH SELF-PROTECTION AND CYBER INSURANCE: THEORETICAL APPROACHES

3.1 Introduction

As increased connectivity raises the frequency of attacks and the size of losses, many companies have increased their spending on information security (X Zhao, et al., 2009) and have adopted a range of security measures to protect information systems. While protection measures have been continuously improving, intrusions into networked systems have also continued to increase (Majuca, et al., 2006). According to the 2008 Computer Crime and Security Survey by the Computer Security Institute (2008), for example, most of the organizations either had a security policy (68 percent) or were developing a formal information security policy (18 percent), and 31 percent of the organizations spent more than 5 percent of their overall IT budget to information security. Despite this great investment and effort, the survey indicated that 43 percent of respondents experienced security breaches and 27 percent of those had more than 5 security incidents. It also revealed that the average loss of organizations from security incidents was around $300,000 per organizations. Therefore, as Gordon & Loeb (2002) have pointed out, these findings imply that, although many firms have invested more in security measures for information security, the investments are not adequately allocated to prevent security breaches efficiently.

The importance of information security in the networked economy has, therefore, received a great deal of academic attention. Scholars have been conducting research that focuses on technical aspects (e.g., J. Anderson, 1972; Axelsson, 1998; Cohen, 1995; Denning & Denning, 1997; Friedman, 1988; Hsiao, et al., 1979; Mukherjee, et al., 1994; Wiseman, 1986) and

organizational aspects (e.g., Claflin, 2001; Karofsky, 2001; Parker, 1981, 1983; Vaughn, Henning, & Siraj, 2003) to reduce information security breaches. More recently, several studies, specifically focusing on economic perspectives, have tried to develop effective and efficient ways of hedging against security breaches (R. Anderson, 2001; R. Anderson & Moore, 2006; R. Anderson, et al., 2007; L. J. Camp & Wolfram, 2000; Lawerence Gordon & Loeb, 2002; Varian, 2000). However, as indicated by Bolot & Lelarge (2008a), the majority of these studies have focused mainly on issues of self-protection,[16] and have attempted to identify threats and to develop efficient countermeasures. Correspondingly, most firms also tend to invest in a vast array of security measures without ascertaining the effectiveness of the measures.

According to Böhme (2005) and Bolot & Lelarge (2008a), however, these massive investments in self-protection represent only part of the overall solutions required, and a residual risk remains because there is no system that is foolproof against all types of threats. 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: with interconnected IT, the information security risks of one agent are correlated with those of others (X Zhao, et al., 2009). In other words, a firm's security investment not only affect its own security risks but also those of other firms (Grance, Hash, Peck, & Smith, 2002; X Zhao, et al., 2009). This interdependence of information security risks is the main interest of this study.

---

[16] According to Bolot & Lelarge (2008a), Kesan et al (2005b) and Ehrlich & Becker (1972), firms can hedge security risks using three different approaches: self-protection, self-insurance and market insurance. Self-protection is an approach to reduce the probability of a loss. For example, intrusion detection and prevention systems are mechanisms of self-protection. Self-insurance is a mechanism to reduce the size of a loss, and includes such examples as DDoS mitigation systems, traffic engineering solutions, over-provisioning, and public relations companies. Market insurance can be defined as a mechanism to decrease the size of a loss through a third party.

The interdependent feature of information security risks generates externalities in various contexts. First, a firm's security investments often generate positive externalities onto other firms.[17] For example, if a firm raises its level of information security by investing more in technical solutions such as anti-virus and anti-spyware software, it may lower the chances of virus/spyware infection 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 DDoS attacks targeted at a highly secured server are diverted to other servers, and hence increase the risks of other firms.

A basic conclusion of the previous literature is that, without any mechanisms for internalizing externalities, self-interested firms' investment in information 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 (L. J. Camp & Wolfram, 2000; Lakdawalla & Zanjani, 2005; Muermann & Kunreuther, 2008; X Zhao, et al., 2009). The question then is how to handle these externalities that cause an inefficient investment in self-protection.

Researcher and practitioners in the field of information security have been investigating how to internalize these externalities and overcome inefficiency since the early 2000s (e.g., L. Gordon, et al., 2003; Kesan, et al., 2005b; Ogut, Menon, et al., 2005; Varian, 2000). Some have argued that the enforcement of liability for losses due to security breaches can internalize security externalities (Ogut, Raghunathan, et al., 2005; Varian, 2000). Since it is difficult, if not

[17] 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 buy Lojack exploit positive externalities since auto thieves cannot distinguish which car has Lojack (L. J. Camp & Wolfram, 2000).

impossible, to determine who is responsible for the losses, however, the imposition of liability might be an infeasible option for internalizing the externalities (X Zhao, et al., 2009). Other researchers (Bolot & Lelarge, 2008; LA Gordon, et al., 2003; Kesan, et al., 2005; Ogut, Menon, et al., 2005; Zhao, et al., 2009) 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 (Bolot & Lelarge, 2008a). With cyber insurance, like other insurance products, insured firms might 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.

The goal of this chapter is mainly to answer two questions that arise from the above discussion: (1) How do externalities caused by interdependent security risks influence firms' security investment decisions; and (2) How does cyber insurance affect a firm's decision regarding security investment. To answer these questions, the classical expected utility model is used with two firms to present the interplay between self-protection and cyber insurance. More specifically, the impact of externalities on the security investments of the firms with and without insurance being available is analyzed. The focus is on risks such as those caused by different types of cyber attacks (e.g., viruses, spyware, hacking and DDoS), where one's damages are affected by other members in a network. In the first part of this chapter, we explain security investment decision in terms of how positive and negative externalities affect firms' investments in IT security compared to the situation where IT security risks are independent, respectively.

We then investigate the impact of the utilization of the cyber insurance market on information security investments. More specifically, we consider the situation where IT security risks are independent and use this situation as the baseline model of our analysis. Next, we

assume firms are interconnected with other firms via network connections. The main goal at this stage is to estimate the pure effects of interdependency on an organization's optimal level of IT security investment. The next goal of our investigation is to explore the combined effect of interdependent security risk and the utilization of cyber insurance market on IT security risk management, and also to compare the levels of IT security investment in each scenario.

Unlike the previous literature which illustrated socially inefficient security investments caused by interdependent risks, the effect of interdependent risks on decisions about self-protection and insurance coverage are examined. Although many researchers have studied positive and negative externalities in information security, they did not explicitly correlate specific types of cyber attacks with each externality. In contrast, 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. We hypothesize 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.[18]

As defined in Section 1.1, targeted attacks are customized for an intended communication network of system (Dzung, et al., 2005; Tally, 2009). As a result, an agent's increased investment in security against targeted attacks will increase the risks faced by other agents, since adversaries launching targeted attacks will substitute less protected targets in place of their original targets, and thus the investment will generate negative externalities.[19]

---

[18] As explained in Section 1.1., we do not consider hybrid attacks in this study. However, key results derived for specific targeted and untargeted attacks can be applied to the stages that make up hybrid attack.

[19] 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 this case, IT security investment of the firm

In contrast, untargeted attacks aim at large numbers of potential victims hoping for overall success (Dzung, et al., 2005; Tally, 2009).[20] 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 self-protection against untargeted attacks is more likely to generate positive externalities.[21] Figure 3.1 shows the relationship between the types of attack and the externality problem.

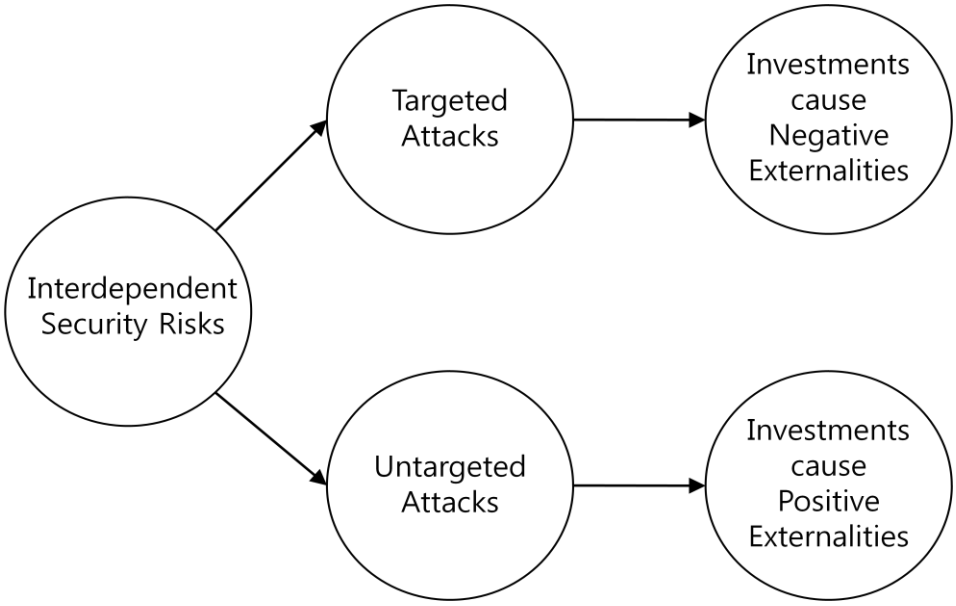


Figure 3-1. Types of Attack and Externalities

To the best of our knowledge, this is the first study that links these different types of cyber

---

will create a positive externality. Again, these types of motivations are not considered in this study.

[20] Common examples of targeted attacks are malicious hacking and DDoS, whereas examples of untargeted attacks include viruses, worms, trojan horses and spyware.

[21] One might argue that there can be a compound attack which first is an untargeted attack, then changes to a targeted attack. For example, perpetrators can spread malware to identify any vulnerable systems (that is, an untargeted attack), then attack most vulnerable system which is found during the untargeted attack. For the sake of simplicity, this study does not consider the possibility of situations of compound attacks.

attacks to information security risk management decisions, including both self-protection and cyber insurance. Unlike other studies (e.g., Kunreuther & Heal, 2003; Ogut, Menon, et al., 2005) which implicitly assume that interdependent security risks can result in either positive or negative externalities, this study demonstrates how different types of cyber attacks cause positive and negative externalities.

The rest of this chapter is organized as follows; the next section present several theoretical models that address the characteristics of interdependent cyber risks on security investments and the effect of cyber insurance. We then derive a number of new propositions that form the basis for the formulation of empirically testable hypotheses in Chapter 4.

3.2 Theoretical Models

It is widely recognized that, unlike most self-protection strategies against natural perils, self-protection against cyber attacks can have public effects not taken into account by the agent (Lakdawalla & Zanjani, 2005). Therefore, even if economists sometimes compare cyber attacks with natural disasters, because of the correlated characteristic of the risks,[22] an analysis of self-protection against cyber attacks should take the interdependencies into account explicitly.

This section presents theoretical models that show how interdependence in cyber security affects firms' decisions regarding self-protection investments and cyber insurance purchases. We start by building theoretical models in which firms' cyber security risks are either independent or interdependent but there is no cyber insurance product available. We show that, in the presence of interdependent cyber security risks, firms' private decisions to invest in self-protection are inefficient; they will invest more or less in security than the expected utility maximizing

[22] For example, the impact of a DDoS attack on economic infrastructure is similar to the impact from natural disasters such as a tsunami.

investments in the case of independent security risks. We then illustrate how the introduction of cyber insurance changes firms' self-protection strategies and explore whether this can eliminate or reduce the inefficiency caused by externalities.

In the models, we consider identical firms with an initial wealth *W* and a utility function $U(\cdot)$. We 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 $r = -\frac{U''}{U'}$. To simplify our 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.[23] 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 a security 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., $B_i'(\cdot) < 0$). We 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.[24] Similarly, a firm's investment in self-protection affects the breach probability at all

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

[24] 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

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.

3.2.1 Models for Security 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. According to Bolot & Lelarge (Bolot & Lelarge, 2008a), this creates a feedback loop as shown in Figure 3-2.

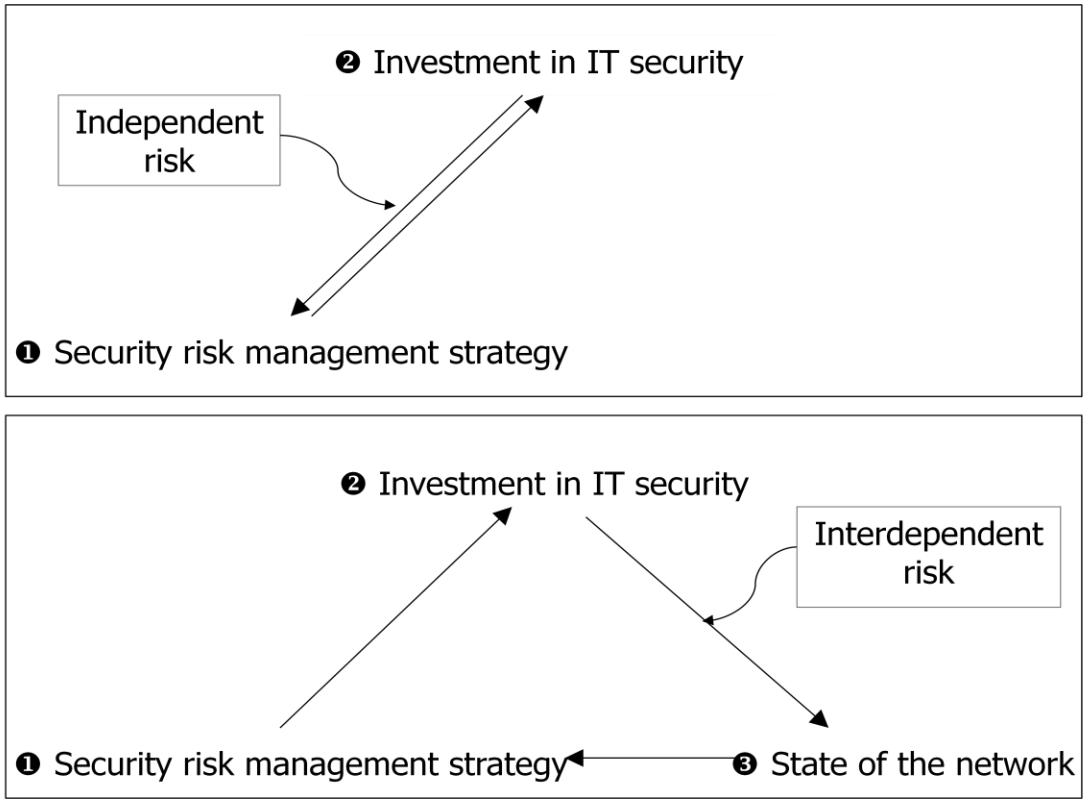


Figure 3-2. Feedback loop of IT security investment without cyber insurance
(figure based on Bolot & Lelarge (2008a))

---

firm may reduce the breach probability of other firms since computers across firms are inter-connected.

This section first examines the baseline model in which security risks are independent and no cyber insurance product is available. We then consider cases in which breaches caused by untargeted and targeted attacks are interdependent, and thus generate positive and negative externalities, respectively.

3.2.1.1 Baseline Model of Independent Risks without a Cyber Insurance Market

We assume that, when there is no insurance product available, all firms manage cyber risks by investing only in self-protection. There are two possible final outcomes for a firm: a desirable outcome where there is no security breach and firm *i*'s utility is $U(W_i - z_i)$ and a non-desirable outcome where firm *i* experiences a security breach and its utility is $U(W_i - L_i - z_i)$. Therefore, the condition that maximizes the expected utility of firm *i* can be expressed as

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

The first-order condition for IT security investment is

$$B_i'(\cdot)[U_L - U_N] - \{B_i(\cdot)U_L' + [1 - B_i(\cdot)]U_N'\} = 0 \tag{3.2}$$

where $U_L = U(W_i - L_i - z_i)$ and $U_N = U(W_i - z_i)$. Note that the first term is positive and reflects self-protection's mitigating impact on the breach probability. The second term reflects the net marginal pecuniary cost of self-protection. A firm balances the first term and the second term. Therefore, firm *i*'s equilibrium security investment satisfies

$$B_i'(\cdot) = \frac{B_i(\cdot)U_L' + [1 - B_i(\cdot)]U_N'}{[U_L - U_N]}. \tag{3.3}$$

As shown in the first-order condition, even if taking the partial derivative of $B_i(\cdot)$ with

respect to z_i and setting equal to zero can generate an equation that shows the characteristics of the equilibrium investment, it does not present a simple closed form solution. Consequently, in order to assess this expression in a useful way, appropriate manipulation of the equation is required. The basic technique for such manipulation that has been commonly used in the literature on uncertainty and insurance is a Taylor series approximation (e.g., Baily, 1977; Bhattacharya & Sood, 2006; Brookshire, Thayer, Tschirhart, & Schulze, 1985; Hau, 1999; Quaas & Baumgartner, 2008; Schoemaker, 1982).[25] This technique expands the representative firm's utility to be a Taylor series. Using the first-order Taylor series approximation,[26] $U_N \approx U_L + U'_L L_i$ and $U'_N \approx U'_L + U''_L L_i$, and substituting the above equation with these approximations, we derive a simple new expression that illuminates the balancing issue associated with selecting the optimal level of security investment:

$$B'_i(z_i^o) = -\frac{1}{L_i} + r[1 - B_i(z_i^o)] \tag{3.4}$$

where $r = -\frac{U''_L}{U'_L}$. The superscript o on z_i indicates the case in which security risks are independent and no cyber insurance product is available.

Next, we investigate the optimal security investment from the perspective of a social planner. Since a social planner will maximize the joint utility function, the condition that maximizes the joint expected utility of all firms in the system can be expressed as

[25] According to Schoemaker (1982) and Hirshleifer (1970), any well-behaved utility function can be expanded by a Taylor series approximation.

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

$$\max_{z_1, z_2, \cdots, z_n} \sum_{i=1,\cdots,n} \{B_i(\cdot)U(W_i - L_i - z_i) + [1 - B_i(\cdot)]U(W_i - z_i)\}. \quad (3.5)$$

It can be identified that the first-order condition with respect to z_i is same as equation (3.2), and hence the social optimal level of security investment is identical to equation (3.4).

3.2.1.2 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. With inter-connected networks, security breaches that occur in one firm can affect other firms which are connected to that firm through a network; that is, inaction of victims of security breaches causes further security intrusions into other systems. In particular, IT security investment for coping with untargeted attacks (e.g., viruses and malware intrusion), which intend to harm large numbers of potential victims, generates 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. For example, if a virus or a malware breaks into an unprotected system, it may be able to gain access to other systems in the network because many viruses and malware spread and proliferate among systems via trusted connections. Therefore, as shown in Figure 3-3, a firm's security investment reduces its probability of breach as well as that of others, and thus firms have incentives to underinvest in information security.

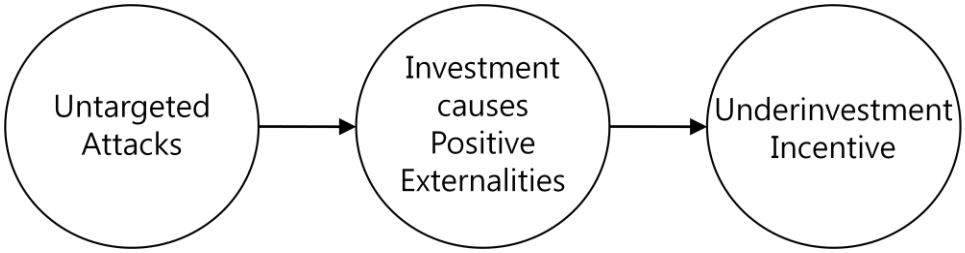


Figure 3-3. Link between Untargeted Attacks and the Level of Investments

Following Ogut et al. (2005) and Zhao et al. (2009), we model positive externalities of security investments in the following manner. To simplify the model, we assume that there are only two symmetric firms with interdependent risks (i=1, 2). The breach probability of each firm is affected by its security investments as well as those of others: that is, the effects of security investment can be classified into direct effects and 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. Therefore, an indirect effect is conditional on a direct effect of a security breach in a partnering firm.[27]

The breach probability caused by direct effects depends on the level of investment in self-protection whereas the breach probability caused by indirect effects is determined by other firms' security investment. We model the breach probability under direct effects as $p(z_1)$ where z_1

[27] Note that, according to Bandyopadhyay (2006), security breach which occurs at a firm's own site incurs a higher loss to the firm (direct loss) than 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 now superadditive and potentially higher than the case when these firms experience separate security breaches.

is the security investment by firm 1: that is, $p(z_1)$ represents the probability that malicious attacks break into firm 1's systems directly. $p(\cdot)$ is decreasing convex function, i.e., $p'(\cdot) < 0$ 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 measures the probability that a firm has a security breach given that another firm has a security breach and vice versa. q models the degree of interdependency or externality between the two firms' IT security. 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, a firm 1's breach probability can be expressed as:

$$B_1(z_1, z_2) = p(z_1) + [1 - p(z_1)]qp(z_2) = 1 - [1 - p(z_1)][1 - qp(z_2)] \qquad (3.6)$$

The probability that a breach does not occur at firm 1 is $[1 - p(z_1)][1 - qp(z_2)]$. It can be identified that $\frac{\partial B_1(z_1, z_2)}{\partial z_1} = p'(z_1)[1 - qp(z_2)] < 0$ and $\frac{\partial B_1(z_1, z_2)}{\partial z_2} = [1 - p(z_1)]qp'(z_2) < 0$ which implies that firm 1's breach probability is decreasing in its security investment and other firms' security investments. Figure 3-4 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 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.

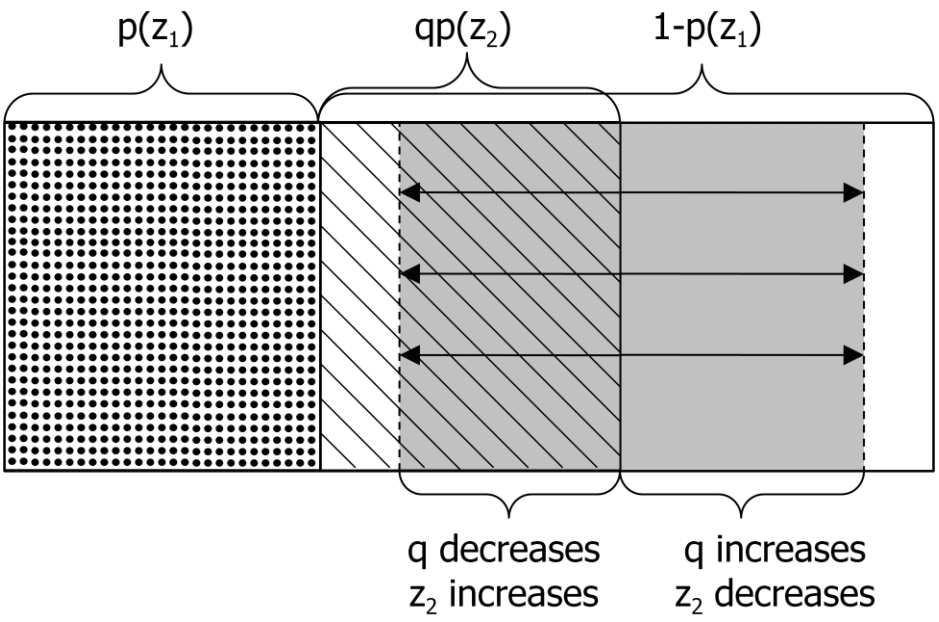


Figure 3-4. Illustration of Breach Probability with Positive Externalities

From equation (3.4), the first order condition with respect to z_1 can be expressed as

$$B_1'(z_1, z_2) = p'(z_1)[1-qp(z_2)] = -\frac{1}{L_1} + r[1-p(z_1)][1-qp(z_2)] \qquad (3.7)$$

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

$$p'(z_1^p) = -\frac{1}{L_1[1-qp(z_2^p)]} + r[1-p(z_1^p)] \qquad (3.8)$$

The superscript p on z_1 indicates the case where security investments generate positive externalities and there is no cyber insurance product available. Compare (3.8) with (3.4), if the cost of a breach is assumed to be equal to 1,

$$B_1'(z_1^o) = -\frac{1}{L_1} + r[1-B_1(z_1^o)] > p'(z_1^p) = -\frac{1}{L_1[1-qp(z_2^p)]} + r[1-p(z_1^p)] \quad \text{and} \quad z_1^o > z_1^p$$

since $B_1(z_1^o) = p(z_1^o)$ and $p'(\cdot) < 0$.

Next, we examine the social optimal security investment. From the perspective of a social planner, the maximization problem of the joint expected utility function in the case of two firms can be expressed as

$$\max_{z_1, z_2} \sum_{i=1,2} \{B_i(\cdot)U(W_i - L_i - z_i) + [1 - B_i(\cdot)]U(W_i - z_i)\}. \quad (3.9)$$

The first-order condition of (3.9) with respect to z_1 can be represented as

$$B_1'(U_{L1} - U_{N1}) - B_1 U_{L1}' - (1 - B_1)U_{N1}' + \frac{\partial B_2}{\partial z_1} U_{L2} - \frac{\partial B_2}{\partial z_1} U_{N2} = 0 \quad (3.10)$$

where $U_{Li} = U(W_i - L_i - z_i)$ and $U_{Ni} = U(W_i - z_i)$. Taylor approximation yields as before

$$B_1'(-U_{L1}'L) - (U_{L1}' + U_{L1}''L) - B_1(-U_{L1}''L) + \frac{\partial B_2}{\partial z_1}(-U_{L2}'L) = 0. \quad (3.11)$$

From $\frac{\partial B_1(z_1, z_2)}{\partial z_1} = p'(z_1)[1 - qp(z_2)]$, $\frac{\partial B_2(z_1, z_2)}{\partial z_1} = [1 - p(z_2)]qp'(z_1)$ and using the assumption of identical firms, the social optimal investment level of firm 1 can be written as

$$p'(z_1^{p*}) = -\frac{1}{L[1 - 2qp(z_1^{p*}) + q]} + r[1 - p(z_1^{p*})]\frac{[1 - qp(z_1^{p*})]}{[1 - 2qp(z_1^{p*}) + q]} \quad (3.12)$$

where z_i^{p*} is the firm i's social optimal investment level when security investments generate positive externalities and no cyber insurance market exists.

Comparing (3.12) with (3.8), it can be identified that firms underinvest in information security if security investments generate positive externalities (i.e., $z_i^{p*} > z_i^{p}$).

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

The model presented above implies that adversaries spread attacks across all possible targets. It can also be argued, however, that an adversary focuses all of his or her resources on a single target. Regardless of the underlying reasons for the attack, the focus on a single target may create instability in the network since it will cause something akin to an arms race among targets (Lakdawalla & Zanjani, 2005). 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 a Nash equilibrium by increasing investment in security protection by an infinitesimal amount. In would seem to follow then that a firm's security investment for coping with this type of targeted attacks (e.g., hacking and DDoS attacks), while reducing its own breach probability, increases the breach probabilities of other firms, and thus is likely to generate negative externalities.

Following Zhao et al. (2009), we model the negative externality of IT security investment in the following manner. A firm's breach probability is influenced not only by its own security investment but also by other firms' investments. If a firm's security investment is higher than the investment of other firms, its investment is more likely to drive away attacks targeted on the firm. In contrast, if a firm invests less than other firms, the firm is more likely to attract targeted attacks than are other firms. Therefore, to make security investment effective, a firm should invest more in security compared to other firms. Since this phenomenon gives firms overinvestment incentives, it may cause "destructive competition" which implies situations when firms invest an excessive amount of resources on information security to avoid targeted attacks

and may undermine their profits (Xia Zhao, 2007). The following figure illustrates the link between targeted attacks and an overinvestment incentive.

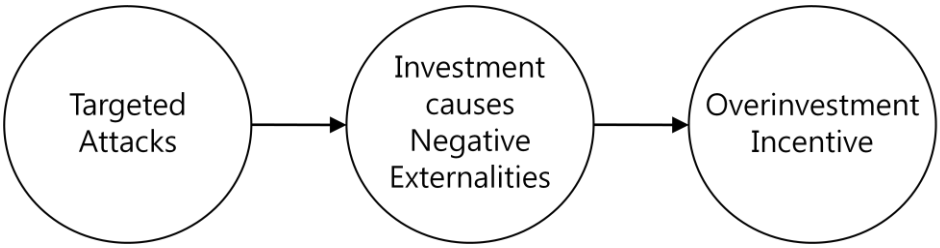


Figure 3-5 Link between Untargeted Attacks and the Level of Investments

We use the term $\frac{z_1}{z_2}$ to characterize the relative effectiveness of firm 1's security investment and model the breach probability as $B_1(z_1, z_2) = p(z_1 \cdot \frac{z_1}{z_2})$. It can be identified that $\frac{\partial B_1(z_1, z_2)}{\partial z_1} = \frac{2z_1}{z_2} p'(z_1 \frac{z_1}{z_2}) < 0$ and $\frac{\partial B_1(z_1, z_2)}{\partial z_2} = -\frac{z_1^2}{z_2^2} p'(z_1 \frac{z_1}{z_2}) > 0$ which implies that firm 1's breach probability decreases as its own security investment increases, but increases in relationship to increases in other firms' security investments. If firm 1 makes a higher security investment than firm 2 (i.e., $\frac{z_1}{z_2} > 1$), we have $z_1 \cdot \frac{z_1}{z_2} > z_1$ and $p(z_1 \cdot \frac{z_1}{z_2}) < p(z_1)$. 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. In contrast, if a firm's security investment is lower than other firms, the firm's investment is not

effective in decreasing its security risks. Therefore, the breach probability of a firm increases corresponding to other firm's security investments, which captures the negative externality of security investment. Figure 3-6 displays the information security risk in the case of negative externalities. Since the breach probability is determined not only by a firm's security investment but also by those of other firms, the breach probability changes as other firms changes the level of their security investments.

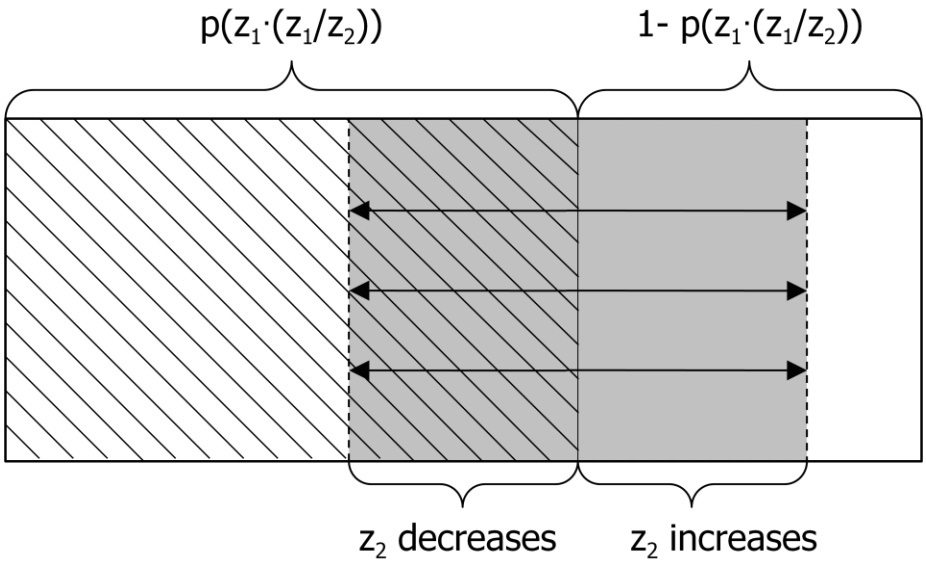


Figure 3-6. Illustration of Breach Probability with Negative Externalities

Similar to the previous section, I assume a case with two symmetric firms. Substituting equation (3.4) with $B_1(z_1, z_2) = p(z_1 \cdot \frac{z_1}{z_2})$ and $\frac{\partial B_1(z_1, z_2)}{\partial z_1} = \frac{2z_1}{z_2} p'(z_1 \cdot \frac{z_1}{z_2})$, and using symmetric assumption where $z_1 = z_2$, firm 1's equilibrium security investment is determined by

$$p'(z_1^n) = -\frac{1}{2L_1} + \frac{r[1 - p(z_1^n)]}{2} \tag{3.13}$$

The superscript n on z_1 indicates the case where security investments generate negative externalities and there is no cyber insurance product available. Compare (3.13) with (3.4),

$$B_1'(z_1^o) = -\frac{1}{L_1} + r[1 - B_1(z_1^o)] < p'(z_1^n) = -\frac{1}{2L_1} + \frac{r[1 - p(z_1^n)]}{2} \quad \text{and} \quad z_1^o < z_1^n \quad \text{since}$$

$B_1(z_1^o) = p(z_1^o)$ and $p'(\cdot) < 0$.

The social optimal investment level can be identified by solving the maximization problem of the joint expected utility function presented in equation (3.9). By using $\frac{\partial B_1(z_1, z_2)}{\partial z_1} = \frac{2z_1}{z_2} p'(z_1 \frac{z_1}{z_2})$, $\frac{\partial B_2(z_1, z_2)}{\partial z_1} = -\frac{z_2^2}{z_1^2} p'(z_2 \frac{z_2}{z_1})$ and the assumption of identical firms, eqation (3.11) can be written as

$$p'(z_1^{n*}) = -\frac{1}{L} + r[1 - p(z_1^{n*})]. \tag{3.14}$$

The superscript $n*$ on z_1 indicates the social optimal investment level where security investments generate negative externalities and there is no cyber insurance product available. Comparing (3.14) and (3.13), it can be identified that firms overinvest in information security in case where security investments generate negative externalities ($z_1^{n*} < z_1^n$) since

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

3.2.2 Interplay Between Self-Protection and Cyber Insurance

In the previous sections, we showed that externalities caused by interdependent IT security risks bring about the problems of inefficient investment. More specifically, when security investments

generate positive externalities, firms are likely to invest less in IT security ($z_1^o > z_1^p$) whereas firms tend to invest more when security investments cause negative externalities ($z_1^o < z_1^n$). We now analyze the impact that cyber insurance has on the level of security investment in self-protection chosen by a firm.

Researchers have proposed several measures for avoiding externality problems. However, as Lackdawalla & Zanjani (2005) and Zhao et al (2009) have noted, traditional approaches for internalizing externalities may be difficult to implement in the case of cyber security. Alternatively, some authors have proposed cyber insurance as an effective measure for internalizing externalities (Böhme, 2005; Bolot & Lelarge, 2008a; Lawerence Gordon & Loeb, 2002; Kesan, et al., 2005b; Lakdawalla & Zanjani, 2005; Muermann & Kunreuther, 2008; Ogut, Raghunathan, et al., 2005; X Zhao, et al., 2009). They argued that firms can employ cyber insurance to cope with the security risks which are not prevented by self-protection. If cyber insurance becomes available, Figure 3-2 illustrated above would be changed to the following feedback loop situation.

Based on Ogut et al. (2005), in this section, we model an insurance market 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 of a security breach is observed. 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.[28]

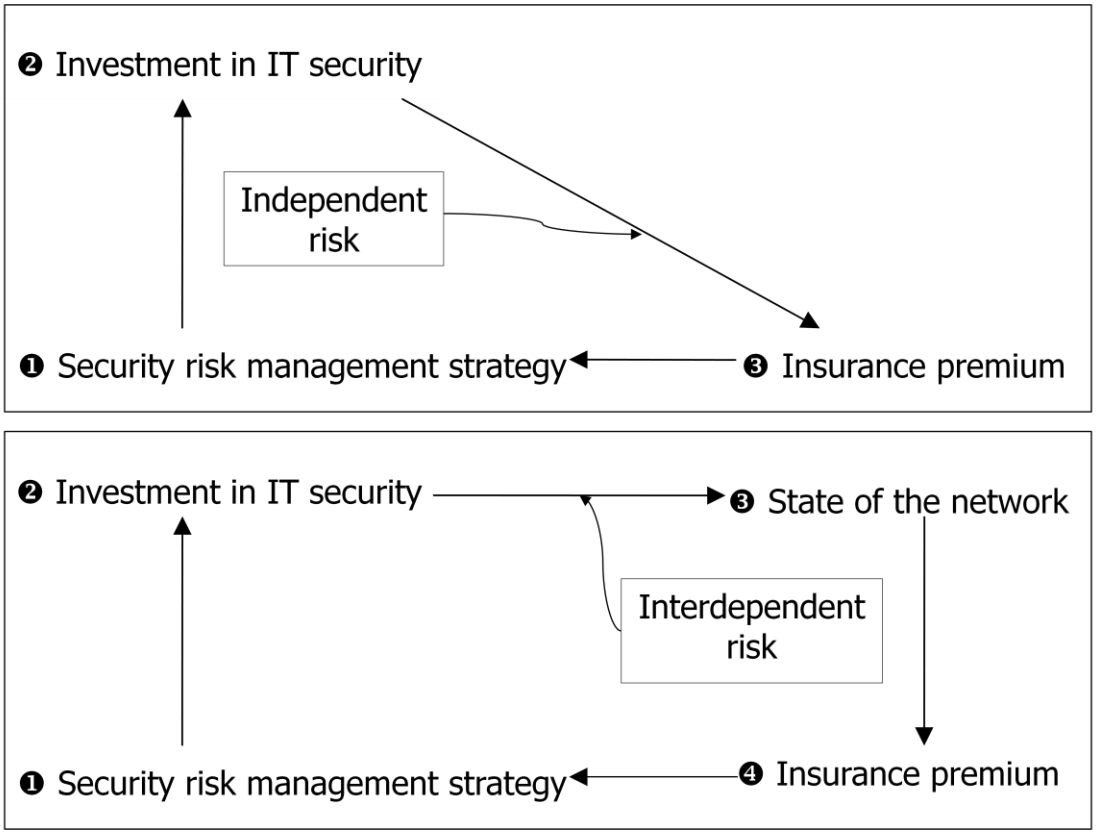


Figure 3-7. Feedback Loop of IT Security Investment with Cyber Insurance
(figure modified from Bolot & Lelarge (2008a))

To take insurance market maturity into account, we use the loading factor, λ, and thus the insurance price can be expressed as $\pi_i = (1+\lambda)B_i$. 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.[29]

---

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

[29] Currently, the cyber insurance market is not well developed (X Zhao, et al., 2009). There are

3.2.2.1 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

$$\max_{z_i, I_i} B_i(z_i)U_i(W_i - L_i + [1-\pi_i(z_i)]I_i - z_i) + [1-B_i(z_i)]U_i(W_i - \pi_i(z_i)I_i - z_i) \quad (3.15)$$

The first order condition for IT security investment is

$$\frac{\partial B_i(z_i)}{\partial z_i}(U_{LI} - U_{NI}) - \left[1 + \frac{\partial \pi_i(z_i)}{\partial z_i} I_i\right]\{B_i(z_i)U'_{LI} + [1-B_i(z_i)]U'_{NI}\} = 0 \quad (3.16)$$

where $U_{LI} = U(W_i - L_i + [1-\pi_i(z_i)]I_i - z_i)$ and $U_{NI} = U(W_i - \pi_i(z_i)I_i - z_i)$. The first order condition for insurance is

$$B_i(z_i)[1-\pi_i(z_i)]U'_{LI} - [1-B_i(z_i)]\pi_i(z_i)U'_{NI} = 0 \quad (3.17)$$

The equation (3.17) can be reorganized into

$$\frac{U'_{NI}}{U'_{LI}} = \frac{B_i(z_i)[1-(1+\lambda)B_i(z_i)]}{[1-B_i(z_i)](1+\lambda)B_i(z_i)} = \frac{[1-(1+\lambda)B_i(z_i)]}{[1-B_i(z_i)](1+\lambda)} \quad (3.18)$$

Dividing the equation (3. 16), the first order condition for IT security investment, by U'_{LI} gives

$$\frac{\partial B_i(z_i)}{\partial z_i}\frac{(U_{LI} - U_{NI})}{U'_{LI}} - \left[1 + \frac{\partial \pi_i(z_i)}{\partial z_i} I_i\right]\{B_i(z_i) + [1-B_i(z_i)]\frac{U'_{NI}}{U'_{LI}}\} = 0. \quad (3.19)$$

---

only a small number of insurance companies offering cyber insurance products, and thus they are likely to make positive profits.

By using $\pi_i(z_i)=[1+\lambda]B_i(z_i)$, $\frac{U'_{NI}}{U'_{LI}}=\frac{[1-(1+\lambda)B_i(z_i)]}{[1-B_i(z_i)](1+\lambda)}$ and the first order Taylor series approximation, $U_{NI}\approx U_{LI}+U'_{LI}(L_i-I_i)$, the first order condition for IT security investment can be changed to

$$-\frac{\partial B_i(z_i)}{\partial z_i}(L_i-I_i)-\left[1+(1+\lambda)\frac{\partial B_i(z_i)}{\partial z_i}I_i\right]\left[B_i(z_i)+\frac{(1-(1+\lambda)B_i(z_i))}{(1+\lambda)}\right]=0. \quad (3.20)$$

Therefore,

$$\frac{\partial B_i(z_i^{oI})}{\partial z_i^{oI}}=-\frac{1}{(1+\lambda)L_i}. \quad (3.21)$$

The superscript oI on z_i means that security risks are independent and there is a cyber insurance product available.

Similarly, by using the Taylor series approximation $U'_{NI}\approx U'_{LI}+U''_{LI}(L_i-I_i)$, we can substitute the first order condition for insurance into

$$\frac{U'_{NI}}{U'_{LI}}=\frac{U'_{LI}+U''_{LI}(L_i-I_i)}{U'_{LI}}=1+\frac{U''_{LI}(L_i-I_i)}{U'_{LI}}=\frac{[1-(1+\lambda)B_i(z_i)]}{[1-B_i(z_i)](1+\lambda)}. \quad (3.22)$$

Therefore,

$$I_i=L_i-\frac{\lambda}{r[1-B_i(z_i^{oI})](1+\lambda)} \quad (3.23)$$

where $r=-\frac{U''_{LI}}{U'_{LI}}$. 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 $B'_i(z_i^{oI})=-\frac{1}{L_i}$.

The above two equations (3.21) and (3.23) show how firm *i*'s two decision variables, z_i and I_i, are determined: the optimal security investment is determined by equation (3.21) and the optimal amount of insurance coverage demanded by firm i based on equation (3.23) is determined in anticipation of the residual risk.

Next, regarding the social optimal investment level, for simplicity, we assume that a cyber insurance market is mature, and hence $I_i = L_i$ and $\pi_i = B_i$. Consequently, the condition that maximizes the joint expected utility in case where a cyber insurance market exists can be expressed as

$$\max_{z_1, z_2, \cdots, z_n} \sum_i U(W_i - \pi_i(z_i) I_i - z_i). \tag{3.24}$$

The first order condition for IT security investment with respect to z_i is

$$\left(-\frac{\partial \pi_i(z_i)}{z_i} I_i - 1 \right) U_i' = 0. \tag{3.25}$$

It can be therefore identified that $B_i'(z_i^{oI*}) = -\frac{1}{L_i}$ where z_i^{oI*} indicates the social optimal investment level when security risks are independent and there is a cyber insurance product available. This implies that, if there are no externalities, the social optimal investment level is same as an individual firm's decision of a security investment level.

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

Now we consider the case in which a firm's security risk is interdependent and security investment has a positive externality. As in the previous section, I use λ as the loading factor

that shows the maturity of the insurance market and assume that there are two symmetric firms. Since we take security interdependence into account, a firm's investment strengthens its security as well as those of other firms. In the case of two symmetric firm (i.e., i=1, 2), therefore, firm 1 is maximizing its expected utility by solving

$$\max_{z_1, I_1} B_1(\cdot)U_1(W_1 - L_1 + [1-\pi_1(z_1, z_2)]I_1 - z_1) + [1-B_1(\cdot)]U_1(W_1 - \pi_1(z_1, z_2)I_1 - z_1) \quad (3.26)$$

where $B_1(\cdot) = B_1(z_1, z_2) = 1-[1-p(z_1)][1-qp(z_2)]$. The first order condition for IT security investment is

$$\frac{\partial B_1(\cdot)}{\partial z_1}(U_{LI} - U_{NI}) - \left[1 + \frac{\partial \pi_1(\cdot)}{\partial z_1} I_1\right]\{B_1(\cdot)U'_{LI} + [1-B_1(\cdot)]U'_{NI}\} = 0 \quad (3.27)$$

and the first order condition for insurance can be expressed as

$$\frac{U'_{NI}}{U'_{LI}} = \frac{B_1(\cdot)[1-(1+\lambda)B_1(\cdot)]}{[1-B_1(\cdot)](1+\lambda)B_1(\cdot)} = \frac{[1-(1+\lambda)B_1(\cdot)]}{[1-B_1(\cdot)](1+\lambda)} \quad (3.28)$$

Using $\pi_1(\cdot) = [1+\lambda]B_1(\cdot)$, the first order Taylor series approximation (i.e., $U_{NI} \approx U_{LI} + U'_{LI}(L_1 - I_1)$) and equation (3.28), the first order condition for IT security investment can be reorganized as

$$-\frac{\partial B_1(\cdot)}{\partial z_1}(L_1 - I_1) - \left[1 + (1+\lambda)\frac{\partial B_1(\cdot)}{\partial z_1} I_1\right]\left\{B_1(\cdot) + \frac{[1-(1+\lambda)B_1(\cdot)]}{(1+\lambda)}\right\} = 0 \quad (3.29)$$

Therefore,

$$\frac{\partial B_1(z_1^{pI}, z_2^{pI})}{\partial z_1^{pI}} = -\frac{1}{(1+\lambda)L_1} \quad (3.30)$$

Using symmetric assumption where $z_1 = z_2$ and $\frac{\partial B_1(z_1^{pI}, z_2^{pI})}{\partial z_1^{pI}} = p'(z_1^{pI})\{1 - qp(z_2^{pI})\}$,

the optimal IT security investment is determined by

$$p'(z_1^{pI}) = -\frac{1}{[1 - qp(z_1^{pI})](1+\lambda)L_1} \tag{3.31}$$

where superscript pI on z_1 indicates positive externality and the existence of a cyber insurance market.[30]

Also, employing another first order Taylor series approximation, $U'_{NI} \approx U'_{LI} + U''_{LI}(L_1 - I_1)$ and $B_1(z_1, z_2) = 1 - [1 - p(z_1)][1 - qp(z_2)]$, the first order condition for insurance (3.28) can be expressed as

$$I_1 = L_1 - \frac{\lambda}{r(1+\lambda)[1 - p(z_1^{pI})][1 - qp(z_1^{pI})]} \tag{3.32}$$

---

[30] To have unique equilibrium, the following condition should be satisfied. The slope of reaction function for each firm can be presented by:

$$R'_1(z_2) = \frac{p''(z_1^{pI})(1 - qp(z_2^{pI}))}{p'(z_1^{pI})qp'(z_2^{pI})}; R'_2(z_1) = \frac{p'(z_1^{pI})qp'(z_2^{pI})}{p''(z_1^{pI})(1 - qp(z_2^{pI}))}$$

In order for the reaction curves to intersect, R'_1 should be bigger than R'_2. Therefore,

$$R'_1(z_2^{pI}) = \frac{p''(z_1^{pI})(1 - qp(z_2^{pI}))}{p'(z_1^{pI})qp'(z_2^{pI})} > R'_2(z_1) = \frac{p'(z_1^{pI})qp'(z_2^{pI})}{p'(z_1^{pI})(1 - qp(z_2^{pI}))}$$

$$\rightarrow \{[p'(z_1^{pI})(1 - qp(z_2^{pI}))] - [p'(z_1^{pI})qp'(z_2^{pI})]\}$$

$$\times \{[p''(z_1^{pI})(1 - qp(z_2^{pI}))] + [p'(z_1^{pI})qp'(z_2^{pI})]\} > 0$$

Since the second brace in the LHS is positive, the unique equilibrium exists if $[p''(z_1^{pI})(1 - qp(z_2^{pI}))] - [p'(z_1^{pI})qp'(z_2^{pI})] > 0$.

where $z_1 = z_2$ and $r = -\frac{U''_{LI}}{U'_{LI}}$. 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 buy full insurance coverage.

We also investigate the social optimal level of IT security investment. By assuming a mature cyber insurance market as before, the maximization problem of the joint expected utility function of two firms can be represented as

$$\max_{z_1, z_2} \sum_{i=1,2} U_i(W_i - \pi_i(\cdot) I_i - z_i). \tag{3.33}$$

The first-order condition of (3.33) with respect to z_1 can be expressed as

$$\left(-\frac{\partial \pi_1(\cdot)}{\partial z_1} I_1 - 1 \right) U'_1 - \left(\frac{\partial \pi_2(\cdot)}{\partial z_1} I_2 \right) U'_2 = 0 \tag{3.34}$$

By replacing I_i and $\pi_i(\cdot)$ with L_i and $B_i(\cdot)$, respectively, and by using $\frac{\partial B_1(z_1, z_2)}{\partial z_1} = p'(z_1)[1 - qp(z_2)]$ and $\frac{\partial B_2(z_1, z_2)}{\partial z_1} = [1 - p(z_2)]qp'(z_1)$, equation (3.34) can be written as

$$-[p'(z_1)(1 - qp(z_2))L_1 + 1]U'_1 - [qp'(z_1)(1 - p(z_2)L_2]U'_2 = 0 \tag{3.35}$$

From the assumption of symmetric firms, therefore, the social optimal investment level of firm 1 is determined by

$$p'(z_1^{pI*}) = -\frac{1}{L_1[1 + q - 2qp(z_1^{pI*})]} \tag{3.36}$$

where z_i^{pI*} is the firm i's social optimal investment level when security investments generate positive externalities and there exists a cyber insurance market.

Comparing (3.36) with (3.31) in case of a mature cyber insurance market, it can be identified that, in spite of the adoption of a cyber insurance market, firms underinvest in information security if security investments generate positive externalities (i.e., $z_i^{pI*} > z_i^{pI}$).

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

In the previous section, we investigated the case in which investment in security measures causes negative externalities without considering the existence of a cyber insurance market. Here, we take cyber insurance into.

Using equation (3.30) and $\frac{\partial B_1(z_1, z_2)}{\partial z_1} = \frac{2z_1}{z_2} p'(z_1 \cdot \frac{z_1}{z_2})$, firm 1's equilibrium security investment is determined by

$$p'(z_1^{nI}) = -\frac{1}{2(1+\lambda)L_1} \tag{3.37}$$

when $z_1 = z_2$. In addition, applying $B_1(z_1, z_2) = p(z_1 \cdot \frac{z_1}{z_2})$, $U'_{NI} \approx U'_{LI} + U''_{LI}(L_1 - I_1)$ and $r = -\frac{U'_{LI}}{U''_{LI}}$ to equation (3.28), the optimal level of cyber insurance can be expressed as

$$I_1 = L_1 - \frac{\lambda}{r(1+\lambda)[1 - p(z_1^{nI})]} \tag{3.38}$$

when $z_1 = z_2$. The superscript *nI* used in both equations (3.37) and (3.38) is used to indicate that security investments generate negative externalities and there is a cyber insurance product available.

We also identify the social optimal security investment using equation (3.34). By using $\frac{\partial B_1(z_1,z_2)}{\partial z_1} = \frac{2z_1}{z_2} p'(z_1 \frac{z_1}{z_2})$ and $\frac{\partial B_2(z_1,z_2)}{\partial z_1} = -\frac{z_2^2}{z_1^2} p'(z_2 \frac{z_2}{z_1})$, and by substituting I_i and $\pi_i(\cdot)$ with L_i and $B_i(\cdot)$, respectively, equation (3.34) can be rewritten as

$$\left(-\frac{2z_1}{z_2} p'(\frac{z_1^2}{z_2})L_1 - 1\right)U_1' + \left((\frac{z_2^2}{z_1}) p'(\frac{z_2^2}{z_1})L_2\right)U_2' = 0 \qquad (3.39)$$

Since we assume that firms are identical, the above equation become

$$p'(z_1^{nI*}) = -\frac{1}{L_1} \qquad (3.40)$$

where z_i^{nI*} indicates the social optimal investment when security investments bring about negative externalities and cyber insurance products are available. Comparing (3.40) and (3.37), it can be identified that $z_1^{nI*} < z_1^{nI}$ since $p'(z_1^{nI*}) = -\frac{1}{L_1} < p'(z_1^{nI}) = -\frac{1}{2L_1}$.

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

The impact of interdependency on IT security risk management strategy is not well understood. Furthermore, the nascent cyber insurance market is hampered by a lack of data about IT security risks and knowledge to assess them. Over time though, as more insurers enter the market, security risks are likely to be assessed more accurately, and the insurance market will mature. To analyze the combined impact of interdependency and insurance market maturity on security investment and insurance coverage, we set forth security spending and insurance coverage in the cases of two identical firms in the following table.

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 for understanding of the issues of cyber security. We first compare the solutions for the baseline models with those for the general model of the case of untargeted attacks (i.e., the existence of positive externality).[31]

Proposition 1-1: *In the scenario without a cyber insurance market, when IT security investment generates positive externalities, firms invest less than they do in the case of independent security risks.*

Proof:

[31] Before presenting the propositions, it should be noted that the propositions 1-2, 1-3, 1-4 and 1-5 are same as the propositions in the study of Ogut el al. (2005). The last of the propositions were derived by the author.

$$p'(z_1^o) = -\frac{1}{L_1} + r[1 - p(z_1^o)] > p'(z_1^p) = -\frac{1}{L_1[1 - qp(z_1^p)]} + r[1 - p(z_1^p)] \Rightarrow z_1^o > z_1^p.$$

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 risk 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 $\left|p'(z_1)\right|$ to $\left|p'(z_1)[1-qp(z_2)]\right|$ (Ogut, Menon, et al., 2005). 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. This is also true for the case where a cyber insurance market exists.

Proposition 1-2: *With a cyber insurance market, when IT security investment generates positive externalities, firms invest less than they do in the case of independent security risks.*

Proof:

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

As a result, in spite of the higher breach probability in the case of positive externalities than the probability in the case of independent risk case (i.e., $p(z_1) + \{1 - p(z_1)\}qp(z_2) > p(z_1)$), it can

be identified from Propositions 1-1 and 1-2 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., $(1+\lambda)[\,p(z_1)+\{1-p(z_1)\}qp(z_2)] > (1+\lambda)\,p(z_1)$. This causes firms to reduce their insurance coverage. Therefore,

Proposition 1-3: *With a cyber insurance market, when IT security investment generates positive externalities, insurance coverage is less or equal compared to the case of independent security risks.*

Proof:

$$I_1^{oI} = L_1 - \frac{\lambda}{r[1-p_1(z_1^{oI})](1+\lambda)} \geq I_1^{pI} = L_1 - \frac{\lambda}{r(1+\lambda)[1-p(z_1^{pI})][1-qp(z_1^{pI})]}$$

Consequently, from Propositions 1-1, 1-2 and 1-3, one can infer that positive externalities in cyber security lead firms to decrease their level of IT security investment and insurance coverage.

We now discuss the impact of loss on firms' strategies through a comparative static analysis. Since $p'(z_1^{pI})\{1-qp(z_2^{pI})\} = -\frac{1}{(1+\lambda)L_1}$, it can be seen that the efficiency of security investment increases as the amount of security loss increases (i.e., $\frac{\partial p'(z_1^{pI})[1-qp(z_1^{pI})]}{\partial L_1} = \frac{1}{(1+\lambda)L_1^2} > 0$). This increased efficiency, in turn, causes firms to invest more in their IT security. Therefore,

Proposition 1-4: *With a cyber insurance market, when IT security investment generates positive externalities, the investment increases as the level of security risk rises, that is,* $\frac{\partial z}{\partial L} > 0$.

Proof:

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

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

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

Similarly, an increase in loss also brings about an increase in insurance coverage. This relationship exists because an increase in loss raises the expected loss, and then the increased expected loss causes increment of insurance coverage (Ogut, Menon, et al., 2005). Therefore,

Proposition 1-5: *With a cyber insurance market, when IT security investment generates positive externalities, insurance coverage increases as loss from a security breach rises, that is,* $\frac{\partial I}{\partial L} > 0$.

Proof:

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

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

In addition, as mentioned earlier, cyber insurance is regarded as a remedy for the residual risk, and hence increases as security investments raises. This implies that, as Ehrlich & Becker (1972) and Ogut (2006) indicated, for a given breach probability, cyber insurance complements security investments.[32] This leads us to the following proposition:

Proposition 1-6: *With a cyber insurance market, when IT security investment generates positive externalities, firms that have higher security investments in equilibrium, will also be observed to have higher level of cyber insurance coverage in equilibrium,* $\frac{\partial I^*}{\partial z^*} > 0$.

Proof:

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

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

$$\rightarrow \frac{\partial I_1^{pI*}}{\partial z_1^{pI*}} = \frac{\partial I_1^{pI*}}{\partial p(z_1^{pI*})}\frac{\partial p(z_1^{pI*})}{\partial z_1^{pI*}} > 0$$

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 identical two firms, it can be identified that the overall security risk is unchanged since the probability of breach is the same whether firms' security risks causes a negative externality or

[32] Some researchers argued that insurance coverage and security investments are substitutes. That is IT security investments would be discouraged by cyber insurance. This effect ahs generally referred as "moral hazard" since policyholders buy less than full insurance coverage as they increase the level of security investments (Ogut, 2006).

no externality, i.e., $p(z_1) = p(z_1 \cdot \frac{z_1}{z_2})$; 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 $\left|p'(z_1)\right|$ to $\left|2p'(z_1)\right|$ 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. Hence,

Proposition 2-1: *In the scenario without a cyber insurance market, when IT security investment generates negative externalities, firms invest more than they do in the case of independent security risks.*

Proof:

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

Since the increase in security investment generates higher efficiency in reducing the breach probability when there is a negative externality in IT security, firms will make above average security investments regardless of the existence of a cyber insurance market. As a result,

Proposition 2-2: *With a cyber insurance market, when IT security investment generates negative externalities, firms invest more than they do in the case of independent security risks.*

Proof:

$$p'(z_1^{nI}) = -\frac{1}{2(1+\lambda)L_1} > p'(z_1^{oI}) = -\frac{1}{(1+\lambda)L_1} \Rightarrow z_1^{nI} > z_1^{oI}$$

In addition, unlike the case of positive externalities, we can observe that firms will buy the more insurance coverage that they purchase in the case of independent security risks. This leads us to the following proposition:

Proposition 2-3: *With a cyber insurance market, when IT security investment generates negative externalities, insurance coverage is more compared to the case of independent security risks.*

Proof:

$$I_1^{oI} = L_1 - \frac{\lambda}{r[1-p_1(z_1^{oI})](1+\lambda)} < I_1^{nI} = L_1 - \frac{\lambda}{r(1+\lambda)[1-p(z_1^{nI})]}$$

A comparative static analysis for the impact of loss on firm's IT security strategies is given below. Since the efficiency of security investment increases as the level of loss increases (i.e., $\frac{\partial 2\,p'(z_1^{nI})}{\partial L} = \frac{1}{(1+\lambda)L^2} > 0$), we know that the increased efficiency causes the increased investment in IT security. Therefore,

Proposition 2-4: *With a cyber insurance market, when IT security investment generates negative externalities, the investment increases as the level of security risk rises, that is,* $\frac{\partial z}{\partial L} > 0$.

Proof:

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

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

An increased risk of loss causes an increase in insurance coverage as well. An increased expected loss makes firms purchase a higher level of insurance coverage. That is,

Proposition 2-5: *With a cyber insurance market, when IT security investment generates negative externalities, insurance coverage increases as loss from a security breach rises, that is,* $\frac{\partial I}{\partial L} > 0$.

Proof:

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

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

As with Proposition 1-6, in the case of negative externalities, cyber insurance and information security investments are also complements in the equilibrium. That is, for a given probability of breach, increase in security investments causes increase in insurance coverage, vice versa.

Proposition 2-6: *With a cyber insurance market, when IT security investment generates negative externalities, firms that have higher security investments in equilibrium, will also be observed to*

have higher level of cyber insurance coverage in equilibrium, $\frac{\partial I^*}{\partial z^*} > 0$.

Proof:

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

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

$$\rightarrow \frac{\partial I_1^{nI}}{\partial z_1^{nI}} = \frac{\partial I_1^{nI}}{\partial p(z_1^{nI})}\frac{\partial p(z_1^{nI})}{\partial z_1^{nI}} > 0$$

In addition, we 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 3: *If a cyber insurance market is available and mature, firms' security investment is less than the investments without a cyber insurance market.*

Proof:

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

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

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

As argued by Powell (2005), Lakdawalla & Zanjani (2005) and Zhao et al (2009), Proposition 3 suggests that, if security investment is inefficient from the social planner's point of view (i.e., overinvestment in the case of negative externalities and underinvestment in the case of positive externalities), the employment of a cyber insurance market can at least partially resolve the overinvestment problem by reducing the investment whereas the underinvestment problem becomes more severe. That is, even if the positive externality case is more problematic since this 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.

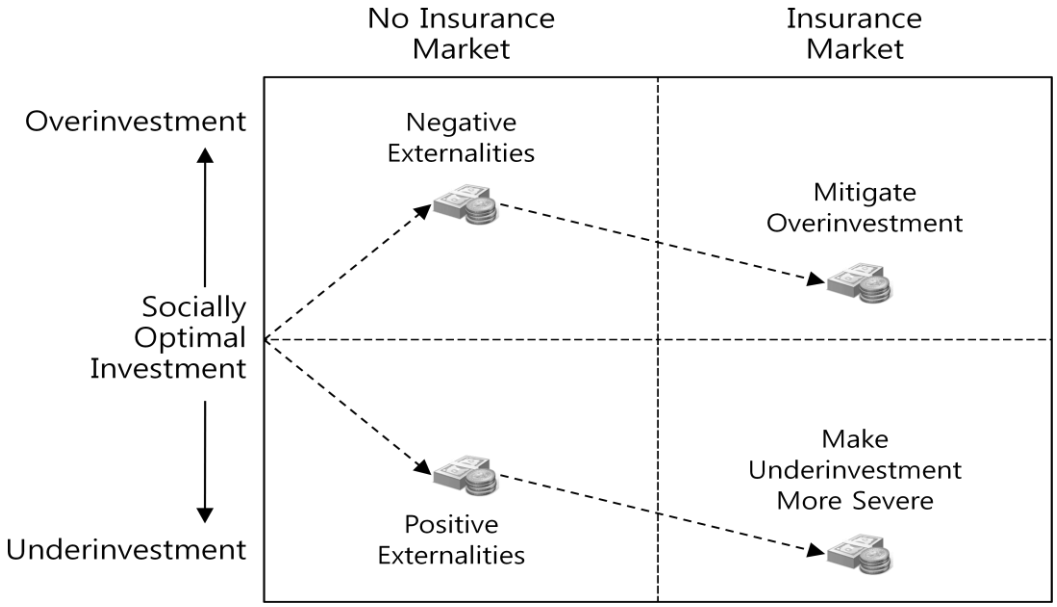


Figure 3-8. Effect of the Adoption of Cyber Insurance Market on the Level of Information Security Investment

3.3 Discussion and Conclusion

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 chapter, we considered firms' strategies for managing IT security risks when the risks are interdependent. As computer networks become increasingly interconnected and integrated in business processes, the IT risk exposure of one firm also makes other firms' networks vulnerable since shared information assets can spread malicious activities or software from one firm to another (Ogut, Menon, et al., 2005).

Specifically, this chapter brought together issues of information security investment and cyber insurance that jointly impact security risk management within a firm. We 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 account for 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. We 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 perverse incentives to invest in IT security. The characteristics of interdependent information security risks distort firms' incentives to invest in IT security. 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 underinvest 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 investments cause negative externalities and firms overinvest in IT security. Hence, these misaligned incentives may cause strategically inefficient IT security management practices.

The second set of implications addressed 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 overinvestment problem whereas it may decrease a social surplus because the underinvestment problem might become more severe. Consequently, the adoption of cyber insurance can only resolve the overinvestment problem but does not mitigate the underinvestment problem.

The complementarity between security investments and the purchase of cyber insurance coverage is another implication of the examination. Although the study found that the adoption of cyber insurance might aggravate the security underinvestment 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 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 mechanism take advantage of the

complementarity effect could solve the underinvestment problem from the adoption of cyber insurance and result in a better social outcome.

In the next chapter, we will expand this theoretical approach to with empirical analysis that tests main implications.

CHAPTER 4

IT SECURITY MANAGEMENT THROUGH SELF-PROTECTION AND CYBER INSURANCE: EMPIRICAL APPROACH

4.1 Introduction

Information technologies are important enablers of the development of telecommunication networks. Various business processes using information technologies such as Electronic Data Interchange (EDI) are widely deployed and have increased connectivity between businesses. The benefits of these networking technologies have been well studied (Clark & Hammond, 1997; Mukhopadhyay, Kekre, & Kalathur, 1995; Srinivasan, Kekre, & Mukhopadhyay, 1994)

It is also increasingly recognized that, as organizations become more reliant on networking technologies, they become more susceptible to IT security breaches and associated losses.

Given these circumstances, IT security risk management has drawn enormous attention from organizations. To mitigate IT security risks, technical security measures such as firewalls, IDSs and authentication systems have been largely adopted by business organizations (Majuca, 2006; Ogut, 2006). While these measures, in the forms of hardware and software, can be a part of overall solutions for IT security management, hedges against cyber attacks based solely on technical measures can never be perfect. Moreover, complete prevention of and protection against information security breaches might be undesirable due to cost inefficiency (Majuca, 2006).

Furthermore, a unique aspect of the IT security domain, interdependent security risk, makes IT security risks management challenging. For example, while dedicated connections among networked organizations can raise the overall efficiency of information exchange, they also increase the organizations' security risks. These connections make it easy for a hacker, who has

broken into one firm, to penetrate other firms via the dedicated connection (L. J. Camp & Wolfram, 2000; Grance, et al., 2002). This interdependency not only makes security decisions of one organization affect the risks other firms face, but also causes the risk management strategies adopted by that organization to influence the strategies of other organizations. Consequently, IT researchers have been increasingly concerned about this interconnected IT security environment (Bank & Richmond, 2005).

Interdependent security risk is problematic since it results in externalities. One way of internalizing the externalities is to purchase cyber insurance that can transfer the residual risk to third party insurers (Bandyopadhyay, 2006; L. Gordon, et al., 2003). Many researchers have studied the effects of cyber insurance on IT security investment and have provided useful insights (e.g., Majuca, 2006; Ogut, 2006). However, as several surveys have demonstrated (e.g., Hulme, 2002; Kovacs, Markham, & Sweeting; Richardson, 2008; Johh Ridd & Rand Europe, 2002), even though organizations have continued to increase their investments in self-protection, they have been reluctant to purchase cyber insurance coverage. These findings need to be examined through more systematic empirical study.

Data that would allow an empirical analysis of organizations' IT security management, including investments in self-protection and cyber insurance, is very limited. Only a few surveys have investigated both organizations' investments in self-protection and cyber insurance (Richardson, 2007, 2008). This study takes advantages of a rich data set, the 2007 and 2008 Korean Information Security Surveys published by the Korea Internet & Security Agency (2007, 2008), from which key information can be extracted to formulate an empirical model examining the theoretical questions raised in the previous chapter. These surveys include detailed information on organizations' IT security management practices, including self-protection

activities and the purchase of cyber insurance.

As far as we know, this is the first study that empirically investigates the effects of interdependent security risks on firms' IT security risk management practices (including both self-protection and cyber insurance) in the case of different types of cyber attacks. More specifically, the empirical analysis reported in this chapter was conducted to answer the following three questions:

(1) Do different types of cyber attacks in the case of interdependent security risks increase or decrease the incentives of firms to invest in self-protection and to purchase a cyber insurance product?

(2) Does the seriousness of cyber threats affect firms' decision related to self-protection and cyber insurance?

(3) How do firms' incentives regarding self-protection decisions change if cyber insurance is available?

We derive hypotheses using the propositions identified in the previous chapter and analyze our models under different scenarios with positive and negative externalities.

The rest of this chapter is organized as follows. In Section 4.2, we set up the research hypotheses derived from the theoretical propositions. Section 4.3 describes the data and research methods, and Section 4.4 analyzes different regression models and reports the research results. Lastly, in Section 4.5, we discuss insights from the analysis and managerial and policy implications.

4.2 Research Hypotheses

In the previous chapters, we illustrated the relationship between self-protection and cyber

insurance within strategic IT security management tools and derived a set of propositions which shows the effects of cyber insurance on investment in self-protection. By combining these propositions, we can develop a set of empirical hypotheses. Due to data constraints there are certain challenges, however, in using the propositions directly as our hypotheses: 1) it is impossible to divide the population into groups with and without a cyber insurance market; and 2) our dataset does not contain information regarding independent security risks. As a result, we do not derive hypotheses from Propositions 1-1, 2-1 and 3 since the propositions involve the case without cyber insurance market. With respect to the remainder of the propositions, this study combines each corresponding proposition into one hypothesis (e.g., Propositions 1-2 and 2-2 become one hypothesis). Therefore, building on the propositions, we derive five hypotheses that can be tested in our empirical analysis.

Our first hypothesis is derived from the combination of Propositions 1-2 and 2-2 which state that, when firms have access to a cyber insurance market, they have an incentive to overinvest in case where IT security investment generates negative externalities (i.e., targeted attack case) and to underinvest in cases where IT security investment generates positive externalities (i.e., untargeted attack case) compared to the independent security risk case. This is clear since a combination of $z_1^{oI} > z_1^{pI}$ from Proposition 1-2 and $z_1^{nI} > z_1^{oI}$ from Proposition 2-2 makes $z_1^{nI} > z_1^{oI} > z_1^{pI}$. This implies that individual firms investing in IT security to reduce security breaches caused by targeted attacks do not take the effect of their security investment on other firms into account and are likely to invest more to strengthen IT security than others. On the other hand, individual firms investing in IT security for coping with untargeted attacks tend to invest less since security risks are less controllable and security investments are less efficient

than in the case of independent security risks. As a result, other things being equal,[33]

Hypothesis 1: *Firms experiencing untargeted attacks invest less in self-protection than firms experiencing the same level of targeted attacks*

The second hypothesis combines Propositions 1-4 and 2-4 which indicate that, regardless of whether IT security investment generates positive or negative externalities, firms increase their security investment as the level of security risk rises, that is, $\frac{\partial z}{\partial L} > 0$. This means that an increase in loss raises the efficiency of security investments since an increase in losses raises the expected loss. This higher efficiency results in an increase in the firms' security spending. Consequently,

Hypothesis 2: *Firms experiencing higher losses invest more in self-protection.*

According to Propositions 1-3 and 2-3, compared to situations of independent security risk, firms purchase less or the same amount of cyber insurance in cases where IT security investments generate positive externalities (i.e., untargeted attacks) whereas firms purchase an higher amount of insurance in cases where IT security investments generate negative externalities (i.e., targeted attacks): that is, $I_1^{oI} \geq I_1^{pI}$ from Proposition 1-3 and $I_1^{nI} > I_1^{oI}$ from Proposition 2-3 becomes $I_1^{nI} > I_1^{oI} \geq I_1^{pI}$. From an insurance company's point of view, the total risk of firms experiencing untargeted attacks is higher than that of firms experiencing

[33] Note that all hypotheses are stated under a '*ceteris paribus'* assumption.

targeted attacks since firms experiencing untargeted attacks invest less in self-protection, in general, than firms suffering targeted attacks. Therefore, an insurance company might raise insurance prices for firms in the case of untargeted attacks, while firms subject to targeted attacks might be offered insurance at the same price as that of the independent risk case. Therefore,

Hypothesis 3: *Firms experiencing untargeted attacks spend less on cyber insurance products than firms experiencing the same level of targeted attacks*

Hypothesis 4 stems from Propositions 1-5 and 2-5 which state that firms always buy more insurance as the loss increases, that is, $\frac{\partial I}{\partial L} > 0$. This is because, as noted in Hypothesis 3, an increase in losses results in an increase in the expected loss, which will cause firms to increase their spending in cyber insurance. Therefore,

Hypothesis 4: *Firms experiencing higher losses purchase a cyber insurance product.*

Hypothesis 5 is derived from Propositions 1-6 and 2-6. Propositions 1-6 and 2-6 assert that if firms have access to a cyber insurance market, firms investing more in information security are more likely to purchase cyber insurance than firms investing less in information security. This implies that there is an association between security investment and the purchase of cyber insurance in which they complement each other; that is, cyber insurance encourages IT security investment and vice versa. From this phenomenon, therefore, the following hypothesis can be derived:

Hypothesis 5: *Firms purchasing a cyber insurance product invest more in IT security, vice versa.*

The set of empirical hypotheses derived here will help answering the research questions regarding the role of information security investment and cyber insurance as IT security risk management tools.

4.3 Approaches and Methods

Survey data about firms' IT security investments are limited. Only a small number of countries, including the U.S., Australia and Korea have conducted annual surveys for cyber crime and IT security. Moreover, empirical data related to cyber insurance are even more difficult to find. In this section, we will discuss the details of a unique dataset that we had access to and how we will test the hypotheses empirically.

4.3.1 Data Source

The data used in this study was extracted from the 2007 and 2008 Korean Information Security Surveys[34] published by the Korea Internet & Security Agency (KISA) (2007, 2008).[35] The main goal of these surveys was to gather detailed information on current information security practices in Korean businesses. The survey covered 10 industries which based on OECD the industry classification. The population consisted of firms with a computer network and more than five employees. Using 2006 Information Society Statistics (National Information Society Agency,

[34] Although the yearly surveys have been conducted since 2001, we only use these two years of surveys since the previous surveys did not include in-depth information on self-protection and cyber insurance, and 2009 Korean Information Security Survey was not available at the time of the study.

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

2006) for the 2007 Korean Information Security Survey and 2006 Korean Census on Basic Characteristics of Establishments (Statistics Korea, 2006) for the 2008 survey, 272,702 and 290,069 firms were identified as the populations for each survey. In order to have a large enough sample of firms which can provide statistically reliable results for analysis of subgroups, KISA established target sample sizes of 2,500 firms for the 2007 survey and 2,800 firms for the 2008 survey. The surveys used a stratified two-stage sampling methodology, based on firm size and industry type. Within each stratum, survey respondents were randomly selected.

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

Over a period of two years, the surveys collected data on 5,336 organizations (2,508 in 2007 and 2,828 in 2008). In order to conduct an empirical analysis, we pooled the data from both years. This is equivalent to assuming that the factors influencing the dependent variable did not markedly change during these two years, which seems defensible.

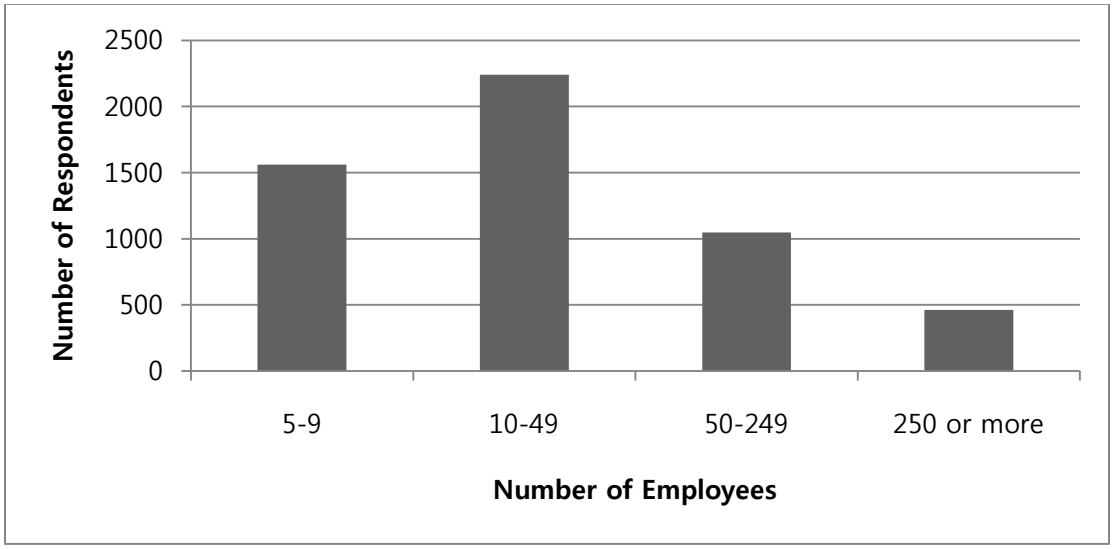
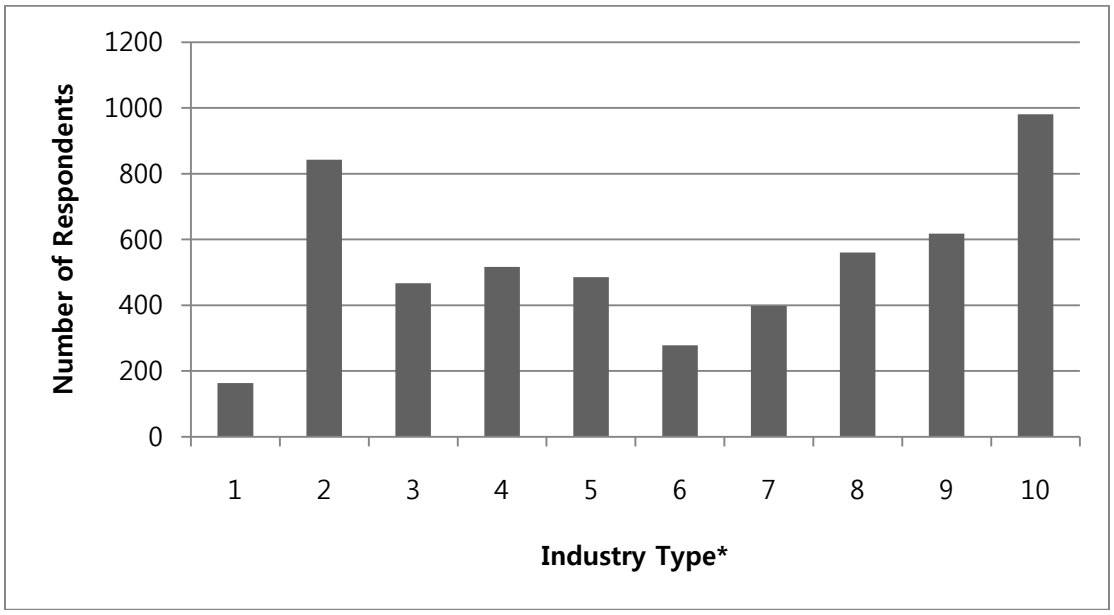


Figure 4-1. Size of Respondent Firms

Figures 4-1 and 4-2 show the characteristics of respondent firms by industry type and the number of employees.



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

Figure 4-2. Industry Type of Respondent Firms

The surveys address four areas: information security environment, information security measures, damages from security incidents and the firm's status. More specifically, the section collecting data on the information security environment addresses questions related to information security policies, security department & personnel management, security awareness training and the investment level, information security management system and safety inspection, and IT budget for information security. The second section, information security measures, addresses questions related to the use of certified security solutions, security outsourcing, measures for database, website & network security, actions for spam e-mails, physical access controls, actions taken after security breaches, purchase of cyber insurance, and actions for

private information protection. The section for damages from security incidents contains questions related to frequency and magnitude of security breaches, sources of security breaches, and the size of losses caused by security breaches. The last section, a firm's status, has questions related to the size and the sales of a firm.

4.3.2 Description of Variables

As outlined in the previous chapter, there are differences between the analytical model and the empirical analysis. For instance, in the theoretical model, we considered the situation where a cyber insurance market is not available at all, but it is impossible to obtain this data from the surveys since cyber insurance products are already widely available in Korea. Similarly, although we also took account of the case of independent security risks in the analytical model, this case is not part of the empirical analysis since the surveys do not contain any data related to independent security risks. Consequently, our hypotheses were formulated in a way that allows test the theoretical questions given the features of the dataset. This subsection describes the variables which will be used to test the hypotheses.

4.3.2.1 The Dependent Variables

Our dependent variables are a firm's information security investment and the purchase of a cyber insurance product. Investment in self-protection is used for testing H1 and H2 while the purchase of a cyber insurance product is used in examining H3 and H4. Note that, for H5, since we test an association between information security investments and the purchase of a cyber insurance product, both of them are used as response variables. More details will be provided in Section 4.4.3.3.

A firm's investment in self-protection can be measured in many ways. Tanaka et al. (2005), for example, used a binary choice variable (use or no use of the information security policy) as a proxy for a firm's security investment. The authors employed this measure since it is almost impossible to measure security investments directly, which are distributed among many different security controls, such as hardware, software and training. Therefore, they hypothesized that firms which have an elaborate security policy invest a substantial amount of money in information security to achieve effective solutions. Liu et al. (2008) used the number of security measures as a proxy variable of security investment. In their study, rather than using the real number of security measures employed, the authors categorized security investment levels into two groups: a group with a low security investment level (i.e., the number of security measures is four and below) and a group with a high security investment level (i.e., the number of security measures is seven and above).

In this study, we use the percentage of the total IT budgets allocated to information security as a proxy for a firm's information security investment (hereinafter referred to as "information security investment rate") (L Gordon, Loeb, Lucyshyn, & Richardson, 2004): this measure can be defined as the relative percentage of a firm's total IT budget which is given to the firm's activities on information security.[36] In spite of certain limitations,[37] this variable is widely used to measure the financial level of information security investment (e.g., J. Anderson, 2003; L Gordon, et al., 2004, 2005, 2006; Johnson & Goetz, 2007; Richardson, 2007, 2008). The KISA

[36] One might argue that it is not clear whether a firm spending a low proportion of its high IT budget on security is better than a firm spending a high share of its low IT budget on security. Even if firms' amounts of IT budgets differ based on their dependency on IT, it can at least be inferred that firms spending a high percentage of their IT budget on security make a greater effort to secure their information system than do firms spending a low share of their IT budget on security.

[37] For example, according to Richardson (2008), not all the funds in the security budget comes from IT budget – e.g., some funds can come from audit or other departments.

surveys categorize the information security investment rate into seven categories: 0%, 0~less than 1%, 1~less than 3%, 3~less than 5%, 5~less than 7%, 7~less than 10% and 10% or more. We assign 0 through 6 to each category, respectively.

The other dependent variable used in this study is the purchase of a cyber insurance product. This measure is a dichotomous choice variable which indicates whether a firm purchased a cyber insurance product or not. However, this measure is somewhat restrictive since it does not show the information about coverage levels or payment rates. It is operationalized as a dummy variable that takes on the value of 1 if an organization purchases a cyber insurance product.

4.3.2.2 The Independent Variables

The independent variables can be categorized into two groups: research variables and control variables. Research variables are necessary to empirically test the hypotheses. These variables include the degree of victimization from targeted attacks and untargeted attacks, losses caused by security breaches and the purchase of a cyber insurance product. Particularly, for H1 and H2, we employ the numbers of targeted and untargeted attacks as proxy variables for the degree of the victimization. As noted previously, we categorize viruses/worms/trojan horses and spyware into the category of untargeted attacks and malicious hacking and DDoS in the category of targeted attacks. Therefore, the number of untargeted attacks is the sum incidents caused by viruses/worms/trojan horses and spyware, whereas the number of targeted attacks is measured by the total number of security breaches caused by malicious hacking and DDoS. With respect to the construction of these two variables, some aspects need to be noted: the surveys we use counted incidents only when they caused actual damages or losses. Therefore, since security incidents which did not result in damages or losses are not included in the data, the actual

number of incidents can be higher than the reported number of incidents. Furthermore, the surveys categorized the number of the incidents into five categories using the following boundaries: 0, 1, 2~3, 4~5, 6~9 and over 10 incidents, and provided the actual number only when the number of incidents is over 10. We change these categories to numeric values by assigning the medium value to the categories of 2~3, 4~5 and 6~9. That is, 2~3 became 2.5, 4~5 became 4.5 and 6~9 were coded as 7.5. We then sum up the numbers of two types of incidents in targeted and untargeted attack categories, as explained above.

In order to test H3 and H4, we use losses caused by security incidents as the research variable. The effects of security incidents are multi-faceted, ranging from direct damages such as disruption of computer systems, loss of information assets, and declines in productivity, to indirect damages such as damage to reputation and loss of consumer loyalty. Selecting the proper variable is therefore not straightforward. The surveys reported several alternative measures for losses caused by security incidents, such as the number of incidents resulting in productivity reduction per year, the average hours causing productivity reduction per incident, the average number of employees experiencing productivity reduction per incident, the total cost caused by system/network/data losses, and the number of computers and servers suffered by data or hardware losses. This study uses a measure that multiplies the number of incidents resulting in productivity reduction per year and the average hours causing productivity reduction per incident. This measure therefore shows the firm's total hours experiencing productivity reduction due to security incidents per year. We use this measure because it, unlikely other measures, is not likely to be affected by the size of the firm.

As mentioned in the previous section, for H5, we only test an association between investment in self-protection and the purchase of cyber insurance. Therefore, no independent variable will be

used.

In addition to the research variables, we also employ several control variables which may influence the dependent variables. In particular, we use three control variables: firm size, industry type, and awareness of information security importance.

Firm size is measured by the number of employees. This variable is included because of empirical evidence on the positive relationship between the size of businesses and the level and quality of security control implementation, for example, as identified by Baker & Wallace (2007). The KISA surveys categorize firms into four categories: 5~9 employees, 10~49 employees, 50~249 employees, and 250 employees or more. This study assigned 1 through 4 to each category, respectively.

Industry type is included since some industries might be very different in some aspects from the rest of other industries. For example, firms in financial and insurance industries might regard information security more importantly than other industries. Therefore, we consider industry-specific differences by including industry type in the models. The surveys group organizations into 10 different industries: (1) agriculture, forestry, and fisheries, (2) manufacturing, (3) construction, (4) wholesaling, (5) retailing, (6) restaurant and lodging, (7) logistics and telecommunications, (8) financial and insurance, (9) real estate, renting and business activities, and (10) other services. We created nine dummy variables indicating the industry type of the organization using "other services" as the default category.[38]

[38] Note that this convention does not influence the outcome.

Table 4-1. Variables Used in the Study

Variable	Description	Type
SEC_INV_RATE	Information security investment rate. It is used as a proxy for information security investment. It is measured by the percentage of the total IT budgets allocated to information security. It is coded 0 if the rate is 0%; coded 1 if 0~less than 1%; coded 2 if 1~less than 3%; coded 3 if 3~less than 5%; coded 4 if 5~less than 7%, coded 5 if 7~less than 10%; and coded 6 if 10% or more.	Dependent
CYB_INS	Purchase of a cyber insurance product. It is coded 1 if a firm purchased a cyber insurance product.	Dependent /
N_TARGETED	The number of targeted attacks. It is measured by the number of cyber incidents caused by hacking and DDoS attacks.	Independent (research)
N_UNTARGETED	The number of untargeted attacks. It is measured by the number of cyber incidents resulted from viruses/worms/trojan horses and spyware.	Independent (research)
P_LOSS	Losses caused by cyber incidents. It is measured by a firm's total hours of productivity reduction per year due to cyber incidents.	Independent (research)
AG_FR_FI_DUM	Industry dummy variable. It is coded 1 if a firm is in the 'agriculture, forestry, and fisheries' industry and 0 otherwise.	Independent (control)
MANU_DUM	Industry dummy variable. It is coded 1 if a firm is in the 'manufacturing' industry and 0 otherwise.	Independent (control)
CONS_DUM	Industry dummy variable. It is coded 1 if a firm is in the 'construction' industry and 0 otherwise.	Independent (control)
WS_DUM	Industry dummy variable. It is coded 1 if a firm is in the 'wholesaling' industry and 0 otherwise.	Independent (control)
RET_DUM	Industry dummy variable. It is coded 1 if a firm is in the 'retailing' industry and 0 otherwise.	Independent (control)
RES_LODGE_DUM	Industry dummy variable. It is coded 1 if a firm is in the 'restaurant and lodging' industry and 0 otherwise.	Independent (control)
LOGI_TEL_DUM	Industry dummy variable. It is coded 1 if a firm is in the 'logistics and telecommunications' industry and 0 otherwise.	Independent (control)
FIN_INS_EDU	Industry dummy variable. It is coded 1 if a firm is in the 'financial and insurance' industry and 0 otherwise.	Independent (control)
RE_REN_BI_DUM	Industry dummy variable. It is coded 1 if a firm is in the 'real estate, renting and business activities' industry and 0 otherwise.	Independent (control)
OTHER_SER_DUM	Industry dummy variable. It is coded 1 if a firm is in the 'other services' industry and 0 otherwise. It is used as a default category.	Independent (control)

Table 4-1 (cont'd)

FIRM_SIZE	Firm size. It is measured by the number of employees. It is coded 1 if a firm has 5~9 employees; coded 2 if a firm has 10~49 employees; coded 3 if a firm has 50~259 employees; and coded 4 if a firm has 250 employees or more.	Independent (control)
AW_IS_EDU_DUM	Awareness of the necessity of security training. It used as a proxy for awareness of information security importance. It is coded 1 if a firm's managers answered the firm needs employees' security training and 0 otherwise.	Independent (control)

Note: All variables are from the 2007 and 2008 KISA surveys

4.3.3 Empirical Models

In the previous section, we developed our research hypotheses, which, when answered, will elucidate how interdependent security risks as well as the different types of cyber-torts affect firms' decisions about self-protection and the purchase of cyber insurance. We also illustrated the characteristics and the limitations of our dataset. Despite some limitations, the dataset allows shedding light on hypotheses H1-H5.

Table 4-2. List of Research Hypotheses

Number	Hypothesis	Test Model
1	Firms experiencing untargeted attacks invest less in cyber security than do firms experiencing the same level of targeted attacks	Negative binomial regression model
2	Firms experiencing higher losses invest more in self-protection	
3	Firms experiencing untargeted attacks spend less in cyber insurance products than do firms experiencing the same level of targeted attacks	Logistic regression model
4	Firms experiencing higher losses purchase a cyber insurance product.	
5	Firms purchasing a cyber insurance product invest more in IT security.	Linear trend test

To test the five hypotheses which are set forth again in Table 4-2, we employ a variety of statistical and econometric instruments, depending on the nature of the data and the hypothesis. The techniques used can be divided into two categories: those that test a causal relationship and those that test an interaction between variables. Of the hypotheses dealing with a causal relationship, one dependent variable is a non-negative count variable (i.e., H1 and H2), and the other dependent variable is dichotomous (i.e., H3 and H4). While we use a negative binomial regression model for testing H1 and H2, a logistic regression model is employed for examining H3 and H4. For testing an association between variables (i.e., H5), this study uses a linear trend test of an association. In the following, we expand upon each instrument and describe the appropriateness of its use.

4.3.3.1 Negative binomial regression models

For H1 and H2, since the dependent variable, security investment rate, has the discrete non-negative nature,[39] key assumptions of the ordinary least squares (OLS) model, such as the normality and homoskedasticity of the residuals cannot be guaranteed. As a result, coefficient estimates using OLS regression would be asymptotically biased, inefficient and inconsistent (Cameron & Trivedi, 1998; Greene, 2003; Long, 1997). To deal with a discrete non-negative dependent variable, two alternative approaches can be used: Poisson regression and negative binomial regression.

Since Poisson regression assumes that the variance is determined by a single parameter, the mean, when the observed variance is larger than the nominal variance, there may be

[39] Although, in reality, security investment in self-protection can be considered a continuous non-negative variable, the proxy variable, IT security investment rate, extracted from the surveys is reported as categorical data.

overdispersion (Greene, 2003). When overdispersion occurs, the estimates of standard errors will be biased downward and any inference from the estimates is therefore doubtful (Stokes, Davis, & Koch, 2000). In contrast, negative binomial regression uses a more flexible distribution and therefore does not suffer from the problem of overdispersion (Greene, 2003). This study therefore uses the negative binomial regression developed by Hausman, Hall and Griliches (1984).[40] The regression model can be specified as:

$$P\left(\frac{k_i}{\varepsilon}\right) = e^{-\mu_i \exp(\varepsilon)} \mu_i^{k_i} / k_i!$$

where k_i is firm i's IT security investment rate and $\mu_i = e^{(B'X_i + \varepsilon)}$ when X_i is the vector of independent variables for firm i's case. Also, $P\left(\frac{k_i}{\varepsilon}\right)$ indicates the probability that firm i will undertake information security investment in the *k*th category; μ_i is the mean of k_i or the average of IT security investment rate; $\exp(\varepsilon)$ is assumed to have a gamma distribution with a mean of 1.0 and a variance of α^2. The estimated model has the form of $k_i = B'X_i + \varepsilon$. For H1, other than the control variables, we use the number of targeted and untargeted attacks as the research variables. The magnitudes of the research variables indicate the effects of the variables on the information security investment rate. For instance, assume that the magnitude of the coefficient of the number of targeted attacks is bigger than the magnitude of the coefficient of the number of untargeted attacks and both coefficients are positive and statistically significant. This

[40] Two alternative approaches can be used to deal with a discrete non-negative dependent variable: Poisson and negative binomial regression. Here, we use the negative binomial regression since the negative binomial regression is less restrictive in that it does not require the assumption of equivalence between the conditional mean and the conditional variance of the dependent variable (Greene, 2003).

implies that, everything else being equal, a one unit increase in the number of targeted attacks generates a higher increase in the security investment rate than does a one unit increase in the number of untargeted attacks, which is consistent with H1. Similarly, for H2, which uses losses caused by security breaches as a research variable, the coefficient of the research variable also shows the impacts of the variable on the information security investment rate.

4.3.3.2 Logistic regression models

The second model used is logistic regression. The main difference between this model and a negative binomial regression model is that the dependent variable is dichotomous.

If a model involves a binary dependent variable, using the OLS regression renders the result inappropriate: the effects of independent variables may be biased, inefficient and inconsistent (Greene, 2003; Long, 1997).[41] This is mainly because the OLS regression allows estimated probabilities to be outside the [0, 1] range. A logistic regression model assures that the estimated probability lies within the [0, 1] range.

In this study, both H3 and H4 use a binary choice variable, the purchase of a cyber insurance product. To test these hypotheses, therefore, we use a logistic regression model, in which the probability of a firm's purchase of a cyber insurance product is explained by the independent variables. Specifically, we use maximum likelihood logistic regression. This method yields parameter estimates that are unbiased and asymptotically efficient. The logistic regression model can be specified as:

$$P(y_i = 1) = \exp(\alpha + x_i\beta) / [1 + \exp(\alpha + x_i\beta)]$$

where y_i is the dependent variable (i.e., the purchase of a cyber insurance product), x_i is the

[41] As a result, using OLS regression is inappropriate for this type of dependent variable

vector of independent variables for the *i*th case, α is the intercept parameter, and β is the vector of regression parameters.

4.3.3.3 Linear Trend Test

H1-H4 postulate causal relationships that can be explored using econometric techniques. However, H5 establishes an association between two variables – security investment rate and the purchase of a cyber insurance product – rather than a causal relationship. Although simple contingency table analyses or loglinear models are commonly used methods for identifying an association between categorical variables, we cannot use these methods since the variable, security investment rate, is not nominal but ordinal.

If one or both of the variables in testing an association are ordinal, the common instrument for testing independence, the chi-square test, ignores the ordering information. Since neglecting ordinality results in a power loss, test statistics which take this information into account are more appropriate. In such cases, trend association is a commonly used method. The trend test examines the change of the level of one variable is associated with the change of the level of the other variable.

To detect an linear association, the trend test uses a test statistic, M^2, which can be denoted by:

$$M^2 = (n-1)r^2$$

where r is the correlation between two variables and n is the sample size. As n increases, M^2 approximates a chi-square distribution with one degree of freedom. Like loglinear models, the linear trend test does not distinguish between independent and dependent variables. In other words, this test regards all variables as response variables and reflects the pattern of association

between them.

4.4 Empirical Findings

4.4.1 Descriptive Statistics

The total number of observations was 5,336. Before conducting statistic analyses, we screened the data for missing values and found a few missing values in the dataset. For example, as noted earlier, the surveys assigned scores between 1 and 6 to the number of cyber incidents of each type experienced by a firm. In some instances, however, some of the observations were found to have the value 999, which indicates a missing value.

The data were also screened for outliers since outliers would affect the model fit. According to Wooldridge (2003), the presence of outliers can be attributed to two main causes: incorrect data entries or sampling from members of a population who have very different characteristics from the rest of the population. It is sometimes, however, not obvious whether outliers are generated by coding error or sampling error. For instance, we found that some firms experienced more than 100 virus/worm/trojan horse infections, spyware infections or DDoS attacks. Although the outliers here were more likely to the result of incorrect data entries, it is also possible that these outliers are actually correct values from surveyed firms with very different characteristics. Furthermore, determining whether to keep or discard outliers is a difficult question with no clear resolution; while there are many techniques for identifying outliers, there is no universal way of treating them. Moreover, since the variables used in this study are nonnegative and many values are zeros, typical outlier detection approaches such as Tukey's method (Tukey, 1977) or Grabb's test (Grubbs, 1969), which assume a normal distribution of a dataset, are not appropriate. To detect outliers, therefore, we visually inspected the data using an index plot in which the

standardized residuals are mapped with respect to the corresponding observation (Stokes, et al., 2000). Using this procedure, we identified only very few outliers and eliminated them from the dataset.

All observations with missing values or regarded as outliers were discarded from the data. Table 4-3 shows the numbers of removed outliers and missing values from each variable. Ultimately, after 57 observations were removed due to missing values and outliers, 5,279 observations remained that were used for estimation purposes.[42]

Table 4-3. Missing Values and Outliers*

	Security Investment Rate	Cyber Insurance	# of virus/worm /trojan horse infections	# of Spyware Infections	# of hacking attacks	# of DDoS attacks
Missing values	15	35	-	3	1	2
Outliers	-		3	5	-	1

* Some observations have both outliers and missing values

Means, standard deviations, as well as the minima and maxima of the dependent, independent and control variables employed in the models are presented in Table 4-4.

Relative frequency histograms of the two dependent variables – the security investment rate and the purchase of cyber insurance – are depicted in Figures 4-3 and 4-4. As clearly seen in these two figures, the counts of both variables are highly skewed towards zero, which reinforces the choice of econometric instruments for testing the hypotheses.

[42] Note that we also conducted regression analyses with outliers and found that the removal of outliers did not cause a change in the qualitative nature of the findings.

Table 4-4. Descriptive Statistics

Variable	N	mean	S.D.	min	max
SEC_INV_RATE	5,279	1.274	1.512	0	6
CYB_INS	5,279	0.054	0.226	0	1
N_TARGETED	5,279	0.387	1.554	0	24
N_UNTARGETED	5,279	2.296	4.455	0	60
P_LOSS	5,279	6.546	77.832	0	2,500
AG_FR_FI_DUM	5,279	0.031	0.173	0	1
MANU_DUM	5,279	0.159	0.366	0	1
CONS_DUM	5,279	0.088	0.284	0	1
WS_DUM	5,279	0.098	0.297	0	1
RET_DUM	5,279	0.091	0.288	0	1
RES_LODGE_DUM	5,279	0.052	0.223	0	1
LOGI_TEL_DUM	5,279	0.075	0.263	0	1
FIN_INS_EDU	5,279	0.105	0.306	0	1
RE_REN_BI_DUM	5,279	0.116	0.320	0	1
OTHER_SER_DUM	5,279	0.185	0.388	0	1
FIRM_SIZE	5,279	2.075	0.912	1	4
AW_IS_EDU_DUM	5,279	0.510	0.500	0	1

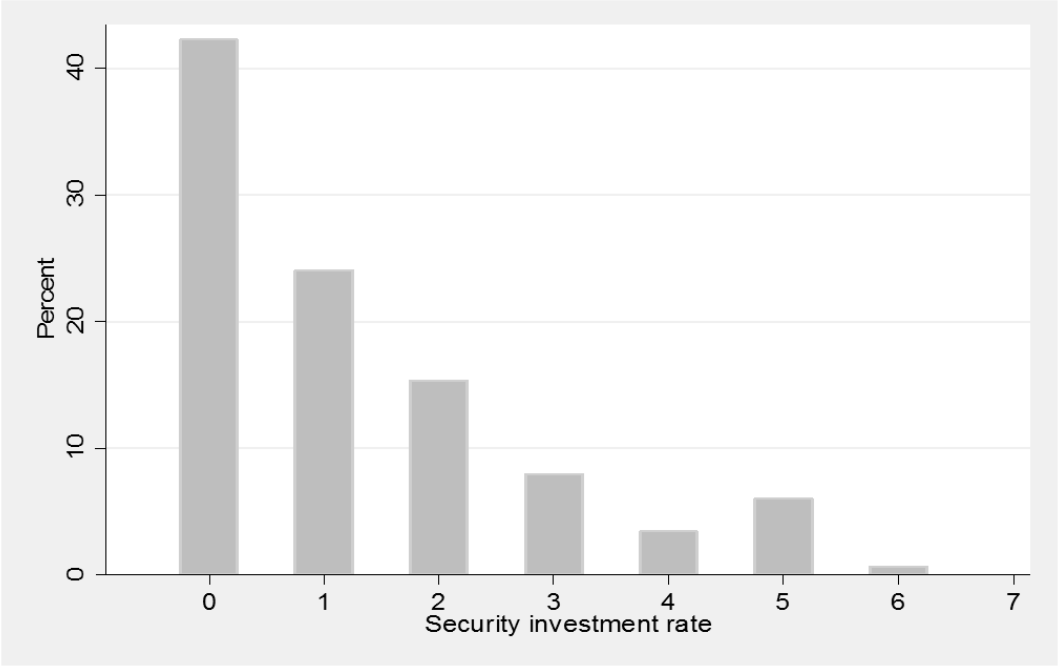


Figure 4-3. Relative Frequency Plot of Security Investment Rate

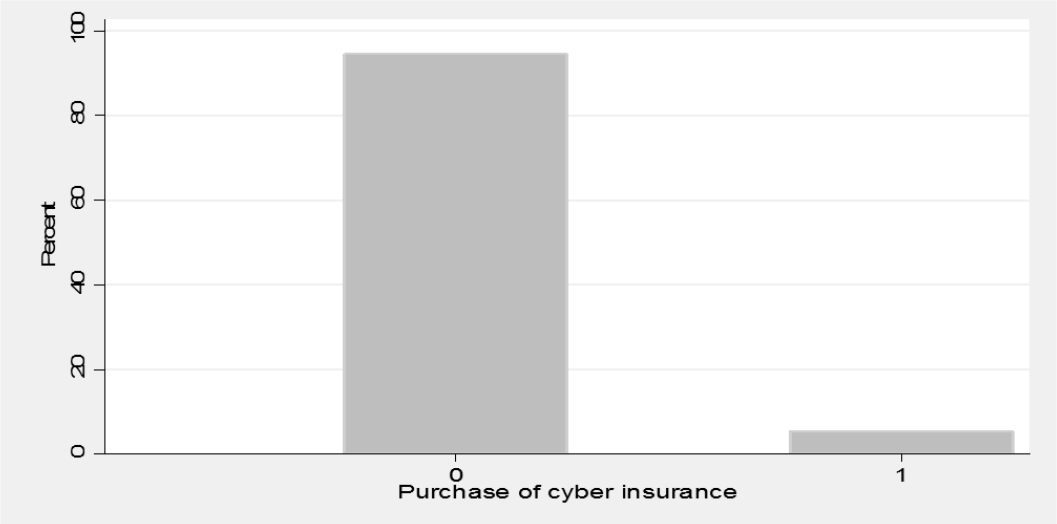


Figure 4-4. Relative Frequency Plot of the Purchase of Cyber Insurance

Figure 4-5 below shows the frequency of targeted attacks and untargeted attacks. As demonstrated in this figure, untargeted attacks occurred more frequently than did targeted attacks.

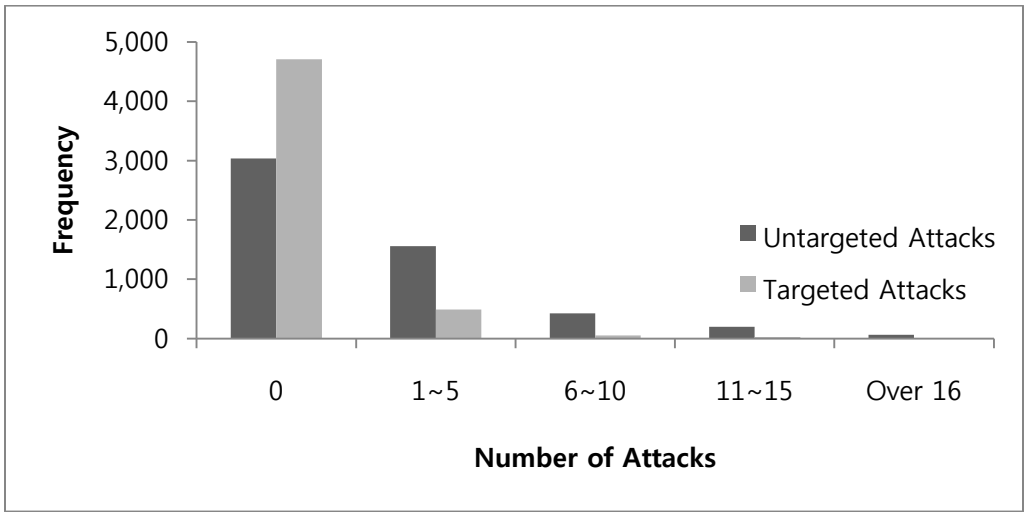


Figure 4-5. Frequency of the Number of Targeted Attacks

Table 4-5 displays Pearson correlations among the study variables. No correlation coefficient is so high (i.e., r>.70) as to suggest that there might be a multicollinearity problem in the estimation.[43]

[43] Similarly, variance inflation factors (VIF) also did not indicate multicollinearity at the levels specified by Belsley et al.(2004).

Table 4-5. Pearson Correlation Matrix

Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1. SEC_INV_RATE	1																
2. CYB_INS	0.16	1															
3. N_TARGETED	0.08	0.03	1														
4. N_UNTARGETED	0.09	-0.05	0.35	1													
5. P_LOSS	0.03	0.02	0.06	0.1	1												
6. AG_FR_FI_DUM	0.03	0.02	-0.01	-0.01	-0.01	1											
7. MANU_DUM	0.01	-0.07	0.00	0.05	0.02	-0.08	1										
8. CONS_DUM	-0.07	-0.07	0.00	0.01	0.00	-0.06	-0.14	1									
9. WS_DUM	-0.01	-0.04	-0.01	0.02	0.01	-0.06	-0.14	-0.1	1								
10. RET_DUM	-0.04	0.01	0.01	0.00	0.00	-0.06	-0.14	-0.1	-0.1	1							
11. RES_LODGE_DUM	-0.03	0.00	0.01	-0.01	-0.01	-0.04	-0.1	-0.07	-0.08	-0.07	1						
12. LOGI_TEL_DUM	0.02	0.02	0.01	-0.01	0.02	-0.05	-0.12	-0.09	-0.09	-0.09	-0.07	1					
13. FIN_INS_EDU	0.10	0.32	0.00	-0.06	-0.01	-0.06	-0.15	-0.11	-0.11	-0.11	-0.08	-0.1	1				
14. RE_REN_BI_DUM	0.01	-0.07	0.04	0.04	-0.01	-0.06	-0.16	-0.11	-0.12	-0.11	-0.09	-0.1	-0.12	1			
15. OTHER_SER_DUM	-0.02	-0.08	-0.05	-0.03	-0.01	-0.09	-0.21	-0.15	-0.16	-0.15	-0.11	-0.14	-0.16	-0.17	1		
16. FIRM_SIZE	0.24	0.04	0.05	0.07	0.00	-0.01	0.07	-0.02	-0.07	-0.05	0.04	0.00	-0.01	0.02	0.02	1	
17. AW_IS_EDU_DUM	0.26	0.11	0.09	0.12	0.02	0.03	-0.02	-0.08	-0.02	-0.04	-0.03	0.00	0.14	-0.03	0.03	0.25	1

4.4.2 Hypotheses Testing

4.4.2.1 Testing H1 and H2

As noted earlier, either Poisson or negative binomial regression could be used to test H1 and H2, which have the discrete non-negative dependent variable – the security investment rate. However, a Poisson regression approach should be employed with caution since a Poisson regression approach usually suffers from an overdispersion problem (i.e., an over-dispersed response variable).[44] When is such a problem exists, the estimated standard errors are incorrect and a statistical test for estimated parameters invalid.

Therefore, before proceeding with our analysis, we first investigated whether overdispersion actually occurs in the case of a Poisson regression model. Table 4-6 below contains the goodness-of-fit statistics of a model for testing H1 and H2, when a Poisson distribution is used. The last column, value/DF, displays the ratios of approximate chi-square values to their degrees of freedom, which indicate the statistics for the difference between the tested model and the full model (Stokes, et al., 2000). If these ratios are close to 1, a model is considered to fit the data well (Stokes, et al., 2000). In contrast, ratios higher than 1 are evidence of overdispersion (Stokes, et al., 2000). The values of 1.6550 for the Deviance/DF and 1.6184 for Pearson/DF, therefore, suggest that a Poisson regression analysis indeed suffers from overdispersion. Since overdispersion is known to result in biased estimates of standard errors, this study used a negative binomial regression model to test H1 and H2, which can overcome this problem.

[44] Overdispersion occurs when the variance is much greater than the mean for all independent variables (Wooldridge, 2003).

Table 4-6. Goodness-of-fit Statistics of Poisson Regression

Criteria For Assessing Goodness Of Fit			
Criterion	Degree of Freedom	Value	Value/DF
Deviance	5,264	8711.9606	1.6550
Scaled Deviance	5,264	8711.9606	1.6550
Pearson Chi-Square	5,264	8519.1696	1.6184
Scaled Pearson X2	5,264	8519.1696	1.6184
Log Likelihood		-4561.3467	

Table 4-7 displays the refitted goodness-of-fit statistics of the model when a negative binomial distribution is assumed. Here, the values of 1.0852 for the Deviance/DF and 0.9936 for Pearson/DF are close to 1, which indicates no evidence of overdispersion. These values also indicate that the model fits the data well.[45]

Table 4-7. Goodness-of-fit Statistics of Negative Binomial Regression

Criteria For Assessing Goodness Of Fit			
Criterion	Degree of Freedom	Value	Value/DF
Deviance	5,264	5712.2661	1.0852
Scaled Deviance	5,264	5712.2661	1.0852
Pearson Chi-Square	5,264	5230.4667	0.9936
Scaled Pearson X2	5,264	5230.4667	0.9936
Log Likelihood		-4235.0020	

[45] Alternatively, we can use -2 Log L value to test the goodness of fit of a model. That is, since the log likelihood for our model is -4235.00 and is -4530.89 for the intercept-only model, -2 Log L is $-2\times(-4530.89+4235.00)=591.78$. Using a chi-squared test, it can be seen that the value yields a p-value<.0001 with 17 degree of freedom.

Since the model has a good fit to our data, identifying the coefficient estimates using a negative binomial regression analysis was seen as appropriate. Table 4-8 presents the estimated parameters, standard errors, and p-values of the negative binomial regression.

Table 4-8. Analysis of Parameter Estimates

Negative binomial regression — Number of obs = 5279; LR chi2(14) = 591.78; Prob > chi2 = 0.0000; Pseudo R2 = 0.0360

Dispersion = mean

Log likelihood = -7921.2416

SEC_INV_RATE	Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
N_TARGETED	.0247254	.0105858	2.34	0.020	.0039777	.0454731
N_UNTARGETED	.0122969	.0037307	3.30	0.001	.0049849	.0196089
P_LOSS	.0001826	.0001745	1.05	0.295	-.0001594	.0005245
AG_FR_FI_DUM	.2763068	.0948445	2.91	0.004	.090415	.4621986
MANU_DUM	.0814516	.0555132	1.47	0.142	-.0273522	.1902554
CONS_DUM	-.1099951	.0708434	-1.55	0.121	-.2488457	.0288555
WS_DUM	.1582021	.0645867	2.45	0.014	.0316146	.2847897
RET_DUM	.0237394	.0675933	0.35	0.725	-.1087411	.1562198
RES_LODGE_~M	-.0514489	.0826769	-0.62	0.534	-.2134926	.1105948
LOGI_TEL_DUM	.2011521	.0694087	2.90	0.004	.0651135	.3371907
FIN_INS_DUM	.3713589	.059726	6.22	0.000	.2542982	.4884196
RE_REN_BI_~M	.1262668	.0605692	2.08	0.037	.0075533	.2449803
FIRM_SIZE	.2269573	.0177889	12.76	0.000	.1920916	.2618229
AW_IS_EDU_~M	.4801987	.0347226	13.83	0.000	.4121435	.5482538
_cons	-.6890386	.0570792	-12.07	0.000	-.8009118	-.5771654
/lnalpha	-.6299243	.0583147			-.7442189	-.5156296
alpha	.5326321	.0310603			.4751053	.5971245

Likelihood-ratio test of alpha=0: chibar2(01) = 652.69 Prob>=chibar2 = 0.000

Note: Statistically significant coefficients are highlighted

Several implications can immediately be drawn from the table: all variables with statistical significance at a level of 0.05 have positive relationships with the dependent variable, SEC_INV_RATE. More specifically, the coefficients of N_TARGETED and N_UNTARGETED reveal that a firm's likelihood of investing in information security is positively influenced by the numbers of the attacks. Of the dummy variables for industry types, the following five variables are statistically significant: AG_FR_FI_DUM, WS_DUM, LOGI_TEL_DUM, FIN_INS_DUM and RE_REN_BI_DUM. The positive signs of the parameter estimates of the variables indicate

that firms in such industries are likely to invest more in information security than firms in the default industry – 'other services' industry. We also found that FIRM_SIZE and AW_IS_EDU_DUM are statistically significant and positively related to SEC_INV_RATE.

In contrast, P_LOSS and the industry dummy variables, MANU_DUM, CONS_DUM, RET_DUM and RES_LODGE_DUM did not turn out to be statistically significant.

The R-square value for the model is 0.036. There are several possible reasons for this low R-square value, which is a common phenomenon in the type of model used here. First, the use of various discrete (i.e., dichotomous and polytomous) variables with limited variability also causes a low R-square value. While the low R-square value might indicate the model is incomplete and there are some missing variables in the system, its explanatory power needs to be evaluated by the statistical significance of each independent variable, rather than the R-square value, as explained by Christie (1990) and Wooldridge (Wooldridge, 2003): based on the large sample size (n=5279) and the significance of many parameter estimates at the 0.01 level, the statistically significant independent variables remain consistent predictors of the ceteris paribus effect on the dependent variable, security investment rate. Second, R-square values are normally lower for cross-section data than for time series data.

From the parameter estimates, the model equation can be written as follows:

$$Log_e(\text{SEC\_INV\_RATE}) = -0.689 + 0.025\text{N\_TARGETED} + 0.012\text{N\_UNTARGETED}$$
$$+0.276\text{AG\_FR\_FI\_DUM} + 0.158\text{WS\_DUM} + 0.201\text{LOFI\_TEL\_DUM}$$
$$+0.371\text{FIN\_INS\_DUM} + 0.126\text{RE\_REN\_BI\_DUM}$$
$$+0.227\text{FIRM\_SIZE} + 0.480\text{AW\_IS\_EDU\_DUM}$$

Since a negative binomial estimation is nonlinear, the effects of changes in independent variables on a dependent variable cannot be directly interpreted form the magnitudes of coefficients. For instance, the parameter estimate of AG_FR_FI_DUM is 0.2763 and indicates

that firms in the 'agriculture, forestry and fisheries' industry have a log 'security investment rate' that is 0.2763 higher than that of firms in the 'other services' industry. To facilitate more direct interpretation, therefore, this value needs to be exponentiated. That is, if other things are equal, firms in the 'agriculture, forestry and fisheries' industry has a higher security investment rate by $e^{0.2763} = 1.3182$ compared to firms in the 'other services' industry. The following table 4-9 lists the exponentiated coefficients which are statistically significant at a 0.05 significant level.[46]

Table 4-9. Effect Sizes (Exponentiated Coefficients)

Exponentiated Estimates			
Effect	Point Estimate	95% Wald Confidence Limits	
N_TARGETED	1.0250	1.0040	1.0465
N_UNTARGETED	1.0124	1.0050	1.0198
AG_FR_FI_DUM	1.3183	1.0946	1.5876
WS_DUM	1.1714	1.0321	1.3295
LOGI_TEL_DUM	1.2228	1.0673	1.4010
FIN_INS_DUM	1.4497	1.2896	1.6297
RE_REN_BI_DUM	1.1346	1.0076	1.2776
FIRM_SIZE	1.2548	1.2118	1.2993
AW_IS_EDU_DUM	1.6164	1.5101	1.7302

Table 4-9 shows that, similar to firms in the 'agriculture, forestry and fisheries' industry, other things being equal, firms in the 'wholesaling', 'logistics and telecommunications',

[46] It should be noted that the table should be interpreted carefully because of the different measurement scales for each variable.

‘financial and insurance’, and ‘real estate, renting and business activities’ industries have higher security investment rates than firms in the ‘other services’ industry by 1.17, 1.22, 1.45 and 1.13, respectively. The exponentiated value of the variable AW_IS_EDU_DUM indicates that, ceteris paribus, firms which are aware of the necessity of security training are likely to have a 1.62 times higher security investment rate compared to firms without such awareness.

Since the variables N_TARGETED, N_UNTARGETED and FIRM_SIZE have polytomous levels, the interpretation of the exponentiated estimates in Table 4-9 is somewhat different than the interpretation of such estimates for binary variables. That is, the estimates should be interpreted as the magnitude of the effects of a one-unit change in independent variables on the rate change in the security investment. Therefore, the exponentiated values for the parameter estimates of the numbers of targeted and untargeted attacks imply that a one unit increase in the number of targeted or untargeted attacks results in an increase in the security investment rate by 1.025 or 1.012, respectively. Similarly, a one unit increase in the firm size causes a 1.616 increase in the security investment rate.

To test H1, we compare the parameter estimates and the exponentiated estimates of N_TARGETED and N_UNTARGETED. The positive signs of the parameter estimates indicate that firms increased the security investment rate as the numbers of both types of attacks rose. At the same time, the magnitude of the exponentiated estimates shows that a one unit change in the number of targeted attacks has a higher impact on the security investment rate than a one unit change in the number of untargeted attacks. Therefore, based on the point estimates, H1 is supported. In contrast, the statistical insignificance of the variable, P_LOSS, suggests that H2 should be rejected.

4.4.2.2 Testing H3 and H4

To test the hypotheses, H3 and H4, this study uses a logistic regression model. Before proceeding with the analysis, the goodness-of-fit of the study model is examined. Table 4-10 lists various values for assessing the fit of the model: The Akaike Information Criterion (AIC), the Schwarz Criterion (SC) and -2 Log L. The difference between the values with 'intercept only' and 'intercept and covariates' in each criterion shows the significance of the additional explanatory variables and can be tested using the chi-square test with a degree of freedom equal to the additional number of explanatory variables. For example, since there are 17 degrees of freedom and -2 Log L equals $-2\times(1765.425-2223.884)=917.138$, it can be concluded that the model fits the data well (i.e., $p<0.0001$ with 17 degrees of freedom). The same results can be demonstrated for AIC and SC.

Table 4-10. Goodness-of-Fit Statistics: AIC, SC and -2 Log L

Model Fit Statistics		
Criterion	Intercept Only	Intercept and Covariates
AIC	2225.884	1795.425
SC	2232.455	1893.997
-2 Log L	2223.884	1765.425

The model fit can be assessed by other strategies as well. The following table provides alternative statistical approaches, the deviance (known as the likelihood ratio statistic) and the Pearson chi-square, for assessing goodness-of-fit. These statistics provide criteria pertaining to whether a saturated model relative to the current model can improve the model fit. From the values 607.157 and 1,537.170 of the deviance and Pearson chi-square with 1,577 degrees of

freedom, it can be identified that a saturated model does not enhance the fit of the model. However, as Stokes (2000) noted, the large dissimilarity of the values between the two statistics indicates that the goodness-of-fit test using deviance and the Pearson chi-square might not be appropriate.[47]

Table 4-11. Goodness-of-Fit Statistics: Deviance and Pearson Chi-square

Deviance and Pearson Goodness-of-Fit Statistics				
Criterion	Value	DF	Value/DF	Pr > ChiSq
Deviance	607.1569	1577	0.3850	1.0000
Pearson	1537.1700	1577	0.9747	0.7591

In this case of value dissimilarity, we need to conduct an additional goodness-of-fit test.[48] Although several strategies can be applied to conduct an additional evaluation for model fit, this study uses the goodness-of-fit test proposed by Hosmer and Lemeshow (2000). This test divides the sample into ten groups based on the predicted probabilities of the model and tests the model fit based on the observed and predicted number of cases in ten groups using the Pearson chi-square statistic (Stokes, et al., 2000). If this statistic supports the model fit together with the previous goodness-of-fit tests, it implies that the study model is adequately constructed. Table 4-12 shows the result of the Hosmer and Lemeshow goodness-of-fit test. Since the chi-square value is 13.216 with 8 degrees of freedom, we can conclude that the model fits well with the data.

---

47 According to Stokes (2000), to use deviance or the Pearson chi-square goodness-of-fit test, the sample size of each event should be at least 5 or more. However, if a model includes some continuous independent variables, the requirement for the sample size almost always cannot be satisfied (Stokes, et al., 2000).

48 Note that while a small sample size in each group requires an further goodness-of-fit test, the analysis of a model is identical to the case where the sample size in each group is large (Stokes, et al., 2000).

Table 4-12. Goodness-of-Fit Statistic: Hosmer & Lemeshow Chi-square

Chi-Square	DF	Pr > ChiSq
13.2155	8	0.1046

Since the model adequacy has been verified, we next discuss the main effects of the parameter estimates. The following table, Table 4-13 lists the estimated coefficients of the model. The variables N_TARGETED, N_UNTARGETED, AG_FR_FI_DUM, RET_DUM, RES_LODGE_DUM, LOGI_TEL_DUM, FIN_INS_DUM, FIRM_SIZE and AW_IS_EDU_DUM are statistically significant at the 0.01 level. The variables P_LOSS and WS_DUM are also statistically significant at a 0.1 significance level.

Table 4-13. Analysis of Maximum Likelihood Estimates

Logistic regression — Number of obs = 5279; LR chi2(14) = 458.46; Prob > chi2 = 0.0000; Log likelihood = -882.71232; Pseudo R2 = 0.2062

CYB_INS	Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
N_TARGETED	.1166326	.0404846	2.88	0.004	.0372841	.195981
N_UNTARGETED	-.0835567	.0256003	-3.26	0.001	-.1337324	-.033381
P_LOSS	.0009962	.0005643	1.77	0.078	-.0001098	.0021022
AG_FR_FI_DUM	1.791522	.3973827	4.51	0.000	1.012667	2.570378
MANU_DUM	.3517926	.3708066	0.95	0.343	-.3749749	1.07856
CONS_DUM	-.6398261	.6401207	-1.00	0.318	-1.89444	.6147873
WS_DUM	.7103172	.3910768	1.82	0.069	-.0561791	1.476814
RET_DUM	1.641192	.3309809	4.96	0.000	.9924819	2.289903
RES_LODGE_~M	1.504927	.3747044	4.02	0.000	.7705197	2.239334
LOGI_TEL_DUM	1.644083	.337243	4.88	0.000	.9830991	2.305067
FIN_INS_DUM	3.112903	.2881629	10.80	0.000	2.548114	3.677692
RE_REN_BI_~M	-.0135722	.4474634	-0.03	0.976	-.8905842	.8634399
FIRM_SIZE	.1914811	.0722131	2.65	0.008	.0499459	.3330162
AW_IS_EDU_~M	.7382095	.1500768	4.92	0.000	.4440644	1.032355
_cons	-5.039324	.3287436	-15.33	0.000	-5.683649	-4.394998

Note: Statistically significant coefficients are highlighted

The R-square value for the model is 0.206. As explained in the previous section, although the

R-square is relatively low, the large sample size and the statistical significance of most of the variables indicate that the independent variables remain reliable predictors of the ceteris paribus effect on the dependent variable – the purchase of a cyber insurance policy. However, since the R-square value for the logistic regression model is less meaningful than for the OLS model, we investigate whether the overall predictive power of the model is better than a null model (i.e., the intercept-only model) using 'hit rate(%)' which shows the correct prediction of the model. The hit rate of the model is 78.44% and that of a null model is 5.42%. This indicates that our research model performs much better than a null model. In addition, looking at the overall explanatory power of the model by its -2 log likelihood, it is identified that the introduction of the variables in the model significantly improves the fit of the null model.

The estimated model equation can be written as follows:

$$Logit(\frac{p}{1-p}) = -5.039 + 0.117\text{N\_TARAGETED} - 0.084\text{N\_UNTARGETED}$$
$$+1.792\text{AG\_FR\_FI\_DUM}+0.710\text{WS\_DUM}+1.641\text{RET\_DUM}$$
$$+1.505\text{RES\_LODGE\_DUM}+1.644\text{LOGI\_TEL\_DUM}+3.113\text{FIN\_INS\_DUM}$$
$$+0.191\text{FIRM\_SIZE}+0.738\text{AW\_IS\_EDU\_DUM}$$

As shown in the equation, all of the statistically significant variables are positively associated with CYB_INS except the variable N_UNTARGETED which presents a negative relationship with CYB_INS.

As was also the case with the previous negative binomial regression model, the effect of a change in an independent variable on a dependent variable cannot be directly interpreted from the estimated parameters because of the nonlinearity of a logistic estimation. As a result, in order to assess the relationships between the dependent variable and the explanatory variables, we calculate the odds ratios of the dependent variable. Odds ratios are useful since these values standardize the parameters. The odds ratios can be calculated by exponentiating the coefficients.

For example, by exponentiating the parameter estimate for N_TARGETED, $e^{0.1166} = 1.1237$, we obtain the odds ratio of CYB_INS for this parameter. The following table 4-14 lists the odds ratios and the confidence limits of the estimated parameters which are statistically significant.

From Table 4-14, of the industry dummy variables, it can be identified that, ceteris paribus, firms have 6 times higher odds of the cyber insurance purchase than firms in the 'other services' industry if the firms are in the 'agriculture forestry and fisheries' industry; 2 times higher odds if the firms are in the 'wholesaling' industry; 5 times higher odds if the firms are in the 'retailing' industry; 4.5 times higher odds if the firms are in the 'restaurant and lodging' industry; 5 times higher odds if the firms are in the 'logistics and telecommunications' industry; and 22.5 times higher odds if the firms are in the 'financial and insurance' industry.

Regarding the variable AW_IS_EDU_DUM, other things being equal, firms which are aware of the necessity of security training have two times higher odds of purchasing cyber insurance compared to firms without the awareness of the necessity of security training.

Since the variable FIRM_SIZE has multi-level values, the interpretation should take this polytomous aspect into account: that is, a one unit increase in the firm size causes the increase in the odds of a cyber insurance purchase by 1.124.[49]

The variables N_TAGETED and N_UNTARGETED which also have the polytomous values can be interpreted similarly with the FIRM_SIZE variable. The odds ratios of the cyber insurance purchase for the numbers of targeted and untargeted attacks are 1.124 and 0.920, respectively: one unit increase in the number of targeted attacks results in the increment in the odds of the cyber insurance purchase by 1.124, while a one unit increase in the number of untargeted attacks

[49] However, it should be noted that if the unit of the firm size changes by 2, the increase in the odds is not 1.124×2 but $e^{(0.191)\times 2} = 1.465$. Therefore, an odds ratio increases with a decreasing rate.

is associated with an increase of the odds by 0.920, or, in other words, a decrease of the odds by 0.080 (i.e., 1-0.920).

Table 4-14. Predicted Odds Ratios for the Purchase of Cyber Insurance

Odds Ratio Estimates			
Effect	Point Estimate	95% Wald Confidence Limits	
N_TARGETED	1.124	1.038	1.217
N_UNTARGETED	0.920	0.875	0.967
P_LOSS	1.001	1.000	1.002
AG_FR_FI_DUM	5.998	2.753	13.070
WS_DUM	2.035	0.945	4.379
RET_DUM	5.161	2.698	9.873
RES_LODGE_DUM	4.504	2.161	9.387
LOGI_TEL_DUM	5.176	2.673	10.024
FIN_INS_DUM	22.485	12.783	39.553
FIRM_SIZE	1.211	1.051	1.395
AW_IS_EDU_DUM	2.092	1.559	2.808

Regarding the variable P_LOSS which is a continuous variable, it is identified that while the increase in productivity loss raises the odds of the cyber insurance purchase, this increase in the odds is fairly small (i.e., odds ratio=1.001).

The analysis of the parameter estimates and the odds ratios demonstrates that, while H3 is strongly sported, H4 is only moderately supported: firms experiencing targeted attacks are more likely to purchase a cyber insurance product compared to firms experiencing untargeted attacks

at the same level as the targeted attacks; and firms with higher losses are more likely to purchase a cyber insurance product.

4.4.2.3 Testing H5

In order to test H5, we use the linear trend test since other econometric instruments for testing an association between discrete categorical variables, such as contingency table analyses and loglinear models, ignore the ordinality of variables. The following table shows the levels of security investment rate with respect to the purchase of cyber insurance. The percentage of cyber insurance purchase has roughly an increasing trend across the security investment rates except for the levels of security investment rates, 1 and 6. This suggests a possible tendency for cyber insurance purchases to be more likely at firms with higher security investment rates.

Table 4-15. Purchase of Cyber Insurance and Security Investment Rate

SEC_INV_RATE	CYB_INS		Total	Percentage of CYB_INS
	No	Yes		
0	2,159	72	2,231	3.23
1	1,238	33	1,271	2.60
2	754	59	813	7.26
3	378	44	422	10.43
4	162	21	183	11.48
5	268	54	322	16.77
6	34	3	37	8.11

To use a linear trend test, we compute r and M^2 as shown in the table below. The sample correlation between SEC_INV_RATE and CYB_INS is $r = 0.1609$. The test statistic

$M^2 = (5,279)(0.1609)^2 = 136.595$ has $P - value = 0.0001$, suggesting a highly significant linear trend between the variables. Consequently, we identified strong support for H5.

Table 4-16. Correlation and Summary Statistics for Security Investment Rate by Cyber Insurance Purchase

Pearson Correlation Coefficient	
Correlation	0.1609
ASE	0.0169
95% Lower Conf Limit	0.1278
95% Upper Conf Limit	0.1939

Cochran-Mantel-Haenszel Statistics (Based on Table Scores)				
Statistic	Alternative Hypothesis	DF	Value	Prob
1	Nonzero Correlation	1	136.5953	<.0001

4.5 Discussion and Conclusions

A distinctive characteristic of IT security risk managements involves interdependent risks. The purpose of this chapter was to empirically investigate the effects of interdependent security risks on information security investments and cyber insurance coverage strategies. Using various econometric instruments, we verified that H1, H3 and H5 were supported ($p<0.01$), H2 was rejected ($p>0.1$) and H4 was only moderately supported ($p<0.1$).

From these results, several important implications emerge. The support for H1 and H3 indicates that interdependent risks seem to affect firms' risk management strategies. Specifically, as we identified in Chapter 3, firms whose activities are afflicted with negative externalities spend more on self-protection and cyber insurance than do firms whose activities are afflicted with positive externalities. This implies that firms experiencing targeted attacks overinvest in information security and/or firms experiencing untargeted attacks underinvest in information security. However, in spite of the strong support for H3, we found that the relationship between

the number of untargeted attacks and the purchase of a cyber insurance product is negative: as the number of untargeted attacks increases, the underinvestment in cyber insurance becomes more severe. This unexpected negative relationship might be caused by four reasons:

First, as explained in Section 4.3, the total risk of firms experiencing untargeted attacks is higher than that of firms experiencing the same level of targeted attacks since firms experiencing untargeted attacks invest less in self-protection than do firms experiencing targeted attacks. Because of the size of the total risk, therefore, insurers might raise insurance premiums for covering untargeted attacks while they offer insurance policies for targeted attacks at the prices comparable to the independent risk case. Consequently, as firms experience more severe untargeted attacks, they tend to have much higher insurance premiums relative to coverage offered, compared to the case of firms with the same level of targeted attacks.

Second, due to the relatively short history of cyber insurance, there are still only a few cyber insurance products which cover losses caused by untargeted attacks such as computer viruses and malware, compared to the products focusing on targeted cyber attacks. For example, as shown in Table 1-1, most of the cyber insurance policies only offer coverage for targeted attacks such as DDoS and hacking except for Net Secure Comprehensive Insurance.

Third, although targeted attacks such as hacking and DDoS are usually detected, many untargeted attacks are not detected by attacked firms, and thus management might underestimate the effects of untargeted attacks on their information systems. As a result, firms will try to increase their detection and prevention abilities by investing in self-protection, rather than reducing losses through cyber insurance.

Fourth, as we assumed in the previous chapter, while targeted attacks do not cause damages to third parties connected to an attacked firm, untargeted attacks could generate losses to the

other parties via network connections with an attacked firm. In addition, several insurance products cover the insured's own loss as well as damages to others caused by the malware-infected insured. As a result, some firms, rather than buying cyber insurance policies, will try to cover their damages from untargeted attacks through insurance products purchased by their business partners. It can thus be inferred that firms experiencing untargeted attacks have little incentive to purchase cyber insurance products.

The tests of H2 and H4 indicate that the losses caused by cyber incidents do not result in a higher level of IT security investment and are likely to result in a very small increase in the probability of a firm's cyber insurance purchase. These findings might be due to the following reasons: as shown in Figure 4-6, only a small fraction of firms experienced more than 100 hours of productivity loss (i.e., 47 firms). Further, because of the low rate of productivity loss, firms might not conceive the losses as a predictor of future losses, but rather considering them as a one-time event. This might make our hypotheses invalid or only moderately supported. However, it should be noted that the rejection of H2 and the acceptance of H4 (albeit only moderately supported) could also indicate that to hedge against losses from cyber incidents, firms are more likely to try to reduce the size of losses (i.e., the purchase of cyber insurance products) rather than reduce the probability of losses (i.e., investment in self-protection).

From the result of testing H5, this study identified a strong association between IT security investment and the purchase of a cyber insurance product. This implies that, unlike the argument that increased spending on insurance substitutes for investment in self-protection (Ehrlich & Becker, 1972), firms which purchase cyber insurance products have higher security investment rate than those firms without cyber insurance.

Figure 4-6. Frequency of Productivity Loss

Regarding the control variables, the results indicate that managers' awareness of the importance of IT security is strongly associated with firms' spending on information security (i.e., security investments and the cyber insurance purchase). In addition, some industries tend to spend more on information security than do firms in the default industry, 'other services'. Firms in the classes 'agriculture, forestry, and fisheries', 'wholesaling', 'logistics and telecommunications' and 'financial and insurance' showed particularly strong positive relationships with information security investment and the purchase of a cyber insurance product.

The combination of the results allows deriving further implications. The support of H1 and the rejection of H2 imply that firms' spending on information security would not be determined by the amount of losses due to cyber incidents, but by the incident types that firms have experienced. In addition, it was identified that managers' awareness of the importance of IT security is an important factor for determining the level of information security investments. Taken together, one might be able to conclude that, if managers consider targeted attacks as more

serious danger than untargeted attacks, the overinvestment problem in the context of security investment might not be reduced, despite the adoption of cyber insurance.

Most of the traditional risk management studies have not captured the unique aspect of IT security risks – interdependence. Further, although some of the studies have considered this aspect, they have failed to provide empirical evidence of the effects of interdependent risks. The significance of this chapter lies in the empirical analysis of this unique characteristic of IT security risks.

CHAPTER 5
DISCUSSION

5.1 Overview

This chapter synthesizes the main findings of the dissertation. Limitations of the chosen approach and possible future research directions will be stated as well. The main focus of the dissertation was to investigate firms' risk management activities in the case of interdependent security risks. The research presented in the previous chapters breaks new ground by examining in detail the role and effects of insurance mechanisms in IT security risk management. We employed theoretical and empirical economic analysis to study the characteristics of IT security risk management strategies within the context of externality problems caused by interdependent risks.

Chapter 1 introduced the idiosyncratic aspects of cyber attacks and information security risks, and addressed the problems in information security risk management; in particular, this chapter illustrated that a firm's traditional security risk activities cannot effectively combat cyber attacks because of residual security risks. We then discussed a security investment model which combines the traditional risk management strategies, self-protection and self-insurance, with market insurance in case of interdependent security risks.

Chapter 2 surveyed the existing technological and economic literature addressing IT security problems. The review indicated that finding a socially optimal security investment is complicated by unique aspects of information security such as misaligned incentives and externalities. The chapter also reviewed studies of cyber insurance which address the potential benefits of using cyber insurance in lessening a problem of inefficient security risk management.

Chapters 3 and 4 presented the main contributions of the dissertation. In chapter 3, the theoretical approach to study a firm's security risk management strategy was developed. Using multiple scenarios of different information security circumstances, the chapter investigated the effects of interdependent risks on firms' defense strategies. The scenarios were formalized as a one-period and two firm symmetric investment game. By analyzing the equilibrium for several scenarios, it was found that, given interdependent security risks, firms use different security risk management strategies depending on different types of cyber attacks. Based on this analysis, fundamental insights were derived and stated as propositions that show the effect of interdependent security risk on the levels of IT security investment and cyber insurance coverage in each scenario. In particular, we showed that interdependent security risks cause an underinvestment problem for untargeted attacks (i.e., a positive externality case) and an overinvestment problem for targeted attacks (i.e., a negative externality case), and increase in security risks results in the increases in security investment and insurance coverage.

Further, the study identified that, unlike the argument that insurance will substitute self-protection (Ehrlich & Becker, 1972), IT security investment occurs at a higher rate in firms that purchase a cyber insurance policy than in those firms that do not purchase a cyber insurance policy. That is, the results illustrated that, firms complement security investments for self-protection with spending on cyber insurance (i.e., a complementary effect of cyber insurance on information security investments). Lastly, the introduction of cyber insurance leads to a reduction of the overall level of information security investments. From the social planner's point of view, it can therefore be an effective market-based solution for managing an overinvestment security problem since the adoption of a cyber insurance market results in lower investment in information security. We thus concluded that the adoption can potentially improve social welfare

in the case of targeted attacks by at least partially reducing the overinvestment problem; in contrast, it may lead to a lower level of social surplus in the case of untargeted attacks since the underinvestment problem might become more severe.

Chapter 4 introduced empirical models based on the previous chapter's findings. Using data extracted from the 2007 and 2008 Korean Information Security Surveys published by the KISA (2007, 2008), this chapter established congruence between the empirical analysis and the propositions derived in the previous chapter. Specifically, by using a variety of econometric techniques, the empirical analysis identified: first, firms' security protection for targeted attacks result in the higher level of security investments than the protection for untargeted attacks. Second, firms experiencing targeted attacks spend more in cyber insurance products than do firms experiencing untargeted attacks. Third, while firms experiencing higher losses spend more on cyber insurance, it cannot be said that those firms invest more in information security. Fourth, firms which have an insurance coverage invest more in IT security. We therefore concluded that, as found from the theoretical results, self-protection and cyber insurance work as complements: the purchase of a cyber insurance policy leads to a more demand for information security investments.

5.2 Research Implications

Although previous studies have suggested that recognizing the effects of IT security overinvestment may be as crucial as recognizing those of IT security underinvestment (Powell, 2005), the security overinvestment problem has drawn relatively little attention in academia (Xia Zhao, 2007). To help remedy this shortcoming, this dissertation therefore investigated security underinvestment issue as well as security overinvestment issues. Furthermore, in this dissertation,

we reasoned about firms' motive that drive them to over- or underinvest in information security, and showed conceptually and empirically that targeted cyber attacks might cause an overinvestment problem due to negative externalities and untargeted cyber attacks might bring about an underinvestment problem because of positive externalities. This dissertation also explored the effects of the newly introduced security risk management tool, cyber insurance, on the traditional security risk management strategy, self-protection. One of the key insights is that, even if cyber insurance cannot solve an underinvestment security investment problem, cyber insurance can mitigate firms' overinvestment incentive since it reduces the overall level of security investments. This study of firms' activities to reduce IT security risks not only generates implications for effective security risk management, but also offers a new knowledge regarding the role of cyber insurance. This section discusses the managerial and policy implications generated by the previous theoretical and empirical analyses.

5.2.1 Managerial Implications

The study explored whether externalities caused by interdependent security risks lead firms to make inefficient IT security investments. The study's findings evidence that a negative externality results in overinvestment in IT security whereas a positive externality results in underinvestment in IT security. These inefficient security investments lead firms to either engage in "destructive competition" in the case of security overinvestment or undermine a safe security environment in the case of security underinvestment. It follows then that understanding and solving an inefficient security investment problem is critical in order for firms to streamline their resource allocation to IT security and deal efficiently with a competitive business environment (Xia Zhao, 2007).

To make a firm's security risk management strategies effective in eliminating inefficient security investment, therefore, a firm needs to thoroughly evaluate the characteristics of the security risks it is facing: a firm needs to identify whether there are certain types of cyber attacks that particularly weaken a safe security environment or cause something akin to an arms race among firms; a firm needs to recognize that certain types of cyber attacks bring about either negative or positive externalities to other firms; and a firm need to consider which types of cyber attacks are most dangerous to the firm (Xia Zhao, 2007). A firm therefore has an incentive to use different security risk management strategies to effectively respond to various types of security risks and cyber attacks.

Correspondingly, risk managers, such as chief information officers and chief security officers, have adopted various types of strategies and initiatives to mitigate IT security risks. However, as discussed in the earlier chapters, it is still difficult to mitigate such risks since IT security measures are reactive in nature – developed in response to newly revealed security holes (Bandyopadhyay, 2006; Majuca, et al., 2006). Moreover, the effectiveness of security measures depends not only on one firm's security strategies but also on those of others (Bandyopadhyay, 2006; Ogut, Menon, et al., 2005). As a result, risk managers cannot determine how much residual security risk remains, even after having extended great effort to reduce IT security risks.

Risk managers, therefore, have incentives to adopt cyber insurance as a security risk management tool. As with information security outsourcing, cyber insurance allows organizations to effectively transfer risks to third parties after the organizations have deployed IT security measures (Richardson, 2008).

Using cyber insurance may be beneficial for a firm in managing IT security risks for the following reasons. First, cyber insurance can serve as a complement to information security

investments in protecting firms against residual risks caused by new aspects of cyber risks such as lagged development of security solutions, interdependent risks and intangible damages. Second, it can prevent firms from engaging in "destructive competition" in the case of targeted attacks. For example, cyber incidents caused by DDoS attacks are likely to affect a firm's competitive advantage since the incidents result in the reduction of competitive advantages such as declines in productivity and loss of reputation. When faced with this type of attack, firms may be excessively competitive in security investments in order to reduce the probability of these attacks. Using a cyber insurance mechanism is a particularly useful strategy for this situation since it can mitigate the incentives of firms to overinvest in information security. As a result, firms can prioritize security spending and can divert resources which would be otherwise overinvested in information security to other areas which require investments.

The decision to employ cyber insurance should, however, be carefully evaluated. As explained in Section 4.3, insurance premiums for covering untargeted attacks would be higher than those for covering targeted attacks due to the tendency of underinvestment in the case of untargeted attacks. In this scenario, firms need to compare the costs and benefits of purchasing a cyber insurance policy.

In sum, firms need to conduct accurate risk assessment which can appropriately evaluate the security risks that they are facing to guide proper security risk management strategies.

5.2.1 Policy Implications

The primary managerial implication of this study was that firms benefit from employing a cyber insurance mechanism because this mechanism reduces the security overinvestment problem and can help managers redirect the freed resources into other productive uses.

Cyber insurance provides benefits to society as well. It offers various social benefits and improves the information security environment overall. Adopting cyber insurance can reduce IT security overinvestment in the case of targeted attacks; from the social planner's point of view, a negative externality problem caused by interdependent risks can be at least partially resolved by the employment of a cyber insurance market.

Second, cyber insurance promotes an improved information security environment since insurance companies offering cyber insurance products can monitor insureds and encourage them to use proper security risk management methods. For example, the companies can encourage insureds to use more secure solutions or to establish a security policy by discriminating insurance premiums or coverage. In addition, insurance companies would try to monitor security threats and provide insureds with proper security measures for the identified threats in order to reduce the amount of potential indemnity that might be caused by these threats (Majuca, 2006). Consequently, cyber insurance is a useful market-based mechanism to improve the security environment by providing proper incentives to insurers and insureds.

Another benefit of employing cyber insurance is that, as with other market-based mechanisms, cyber insurance can be used more practically and flexibly than other legal mechanisms such as liability and commitment rules enacted by regulators. Since the diverse security threats change forms rapidly in response to whatever security measures are being employed at a particular time, law enforcement might not be able to develop appropriate countermeasures in a timely fashion. In contrast, cyber insurance products can be developed more rapidly than legal mechanisms. In sum, cyber insurance or other market-based mechanisms would be a better method in certain contexts than are legal mechanisms in managing security risks (Ogut, 2006).

It should be noted, however, that cyber insurance may not be an appropriate resolution for mitigating the underinvestment problem caused by positive externalities since it will result in more severe problems of inefficient security investment. However, this problem might be solved by using mechanisms such as subsidies, as we explained. Therefore, government policies can improve the effect of cyber insurance.

Consequently, it is worthwhile for policy-makers to reexamine the existing cyber security environment and develop new policies on security risks, such as information sharing[50], to complement cyber insurance.

5.3 Limitations and Possible Avenues for Future Research

Its new findings notwithstanding, this study has certain limitations, some of which are inherent in the data and some are related to peculiarities of the theoretical model. First, in terms of data limitations, although more detailed data would give a clearer insight into information security risk management strategies, the data used in this study was mostly based on binary or categorized values, rather than qualitative and quantitative values. In particular, the lack of precise information on cyber insurance such as premium rates and coverage rates was a limitation in the data. For example, the report published by Ridd and Information Assurance Advisory Council (IAAC) (2002) indicated that cyber insurance premiums are relatively high compared to other insurance policies. The report further argued that the premiums will become more competitive as the cyber insurance market mature (i.e., the numbers of cyber insurers and insureds increases). From the data, however, we are not able to identify the maturity and competitiveness of a cyber insurance market.

[50] According to Ogut et al. (2005), when there is a positive externality, information sharing yields higher IT security investment than do no information sharing.

Furthermore, the data was available for only two points in time, and, therefore, it was not possible to systematically explore dynamic aspects of firms' risk management strategies.

Finally, in terms of empirical findings, although the theoretical exploration presented in this study can be applied to any country, the empirical study might only reflect the situation in one particular national context. Whereas the findings in our sample can be generalized to the South Korean economy in general, one cannot assume generalizability to other nations without additional triangulation. As a result, the findings and their implications from the empirical study may be more applicable to nations with comparable economic structures and legal and regulatory institutions. This may include other OECD member countries but the transferability of this study's findings to nations in the developing world maybe more limited.

In sum, it would be highly desirable to expand the work begun here with a more standardized and more detailed information basis across countries.

Other limitations stem from the theoretical model. The discussion of these limitations will include proposals for future research topics that may constitute interesting directions for independent research. First, this study did not take the behavior of cyber attackers into account. For example, if a cyber attacker substitutes its target for another target, the targets' decision about security risk management strategies will be altered. Although this study did not take this factor about cyber attacks into account, given that our empirical data did not have information about attackers' behavior, including that behavior in the analysis would be very helpful to understand the dynamic aspects of cyber security.

Second, this study did not consider other security risk management mechanisms such as information sharing, markets for vulnerabilities, fines and subsidies, and liability rules. As indicated in the earlier sections, we found that cyber insurance can only offer a partial solution

for inefficient security investment (i.e., the overinvestment problem). By considering alternative methods in combination, we would be able to propose the constellation of risk mitigation mechanisms which could result in a better social outcome.

Third, although this study investigated cyber insurance related issues, it did not include an analysis of implementation problems (i.e., moral hazard and adverse selection) which is an analysis widely conducted in the field of insurance economics. In the field of cyber security, since a market failure can occur not only because an inefficient level of information security investment but also because of moral hazard and adverse selection in a cyber insurance market, including this aspect in a model would be beneficial and yield potentially interesting results.

In sum, since the adoption of a cyber insurance market can only be a partial solution for inefficient security investment, we suggest that further research consider a comprehensive approach which incorporates technology-based, economic-based and policy-based security risk management mechanisms.

5.4 Concluding Remarks

By linking theoretical findings with empirical evidence, the present study contributes to the efforts of cyber security researchers to improve the understanding of firms' decisions about information security risk management strategies, despite certain limitations noted in the preceding section. This study found theoretically and empirically that risks resulting from untargeted attacks cause positive externalities on information security investments while those generated by targeted attacks result in negative externalities.

Further, as the first econometric analysis using actual survey data, the dissertation will hopefully contribute to the efforts of managers and policy-makers to improve the management of

information security strategies. It showed which combination of risk management strategies works best for firms in dealing with interdependent risks and in allocating resources efficiently. The study also discussed which policies are effective to manage interdependent security risks. In sum, the findings should be beneficial to both researchers and practitioners in deepening their understanding of cyber security and related strategies.

REFERENCES

REFERENCES

Anderson, J. (1972). *Computer Security Technology Planning Study*: U.S. Air Force Electronic Systems Division.

Anderson, J. (2003). Why We Need a New Definition of Information Security *Computers & Security, 22*(4), 308-313.

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

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

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

Arrow, K. J. (1963). Uncertainty and the Welfare Economics of Medical Care. *The American Economic Review, 53*(5), 941-973.

Axelsson, S. (1998). *Research in Intrusion-Detection Systems: A Survey*. Sweden: Department of Computer Engineering, Chalmers University of Technology.

Ayres, I., & Levitt, S. D. (1998). Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack. *The Quarterly Journal of Economics, 113*(1), 43-77.

Böhme, R. (2005). *Cyber-insurance Revisited.* Paper presented at the Workshop on the Economics of Information Security 2005, Cambridge, MA.

Böhme, R., & Kataria, G. (2006). *Models and measures for correlation in cyber-insurance.* Paper presented at the Workshop on the Economics of Information Security, Cambridge, England.

Böhme, R., & Kataria, G. (2007). On the Limits of Cyber-Insurance. In S. Fischer-Hübner, S. Furnell & C. Lambrinoudakis (Eds.), *Trust and Privacy in Digital Business* (pp. 31-40). Berlin: Springer.

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

Bandyopadhyay, T. (2006). *Mitigation and transfer of information security risk: Investment in financial instruments and technology.* The University of Texas at Dallas.

Bank, D., & Richmond, R. (2005, July 18). Where the Dangers Are. *The Wall Street Journal*. Retrieved from http://www.crime-research.org/articles/1369/

Beh, H. G. (2001). Physical Losses in Cyberspace. *Connecticut Insurance Law Journal, 8*(1), 55-68.

Belsley, D. A., Kuh, E., & Welsch, R. E. (2004). *Regression Diagnostics: Identifying Influential Data and Sources of Collinearity*: Wiley-IEEE.

Bolot, J., & Lelarge, M. (2008a). *Cyber insurance as an incentive for Internet security.* Paper presented at the Workshop on the Economics of Information Security 2008, Hanover, NH.

Bolot, J., & Lelarge, M. (2008b). *A new perspective on internet security using insurance.* Paper presented at the the 27th Conference on Computer Communications (INFOCOM '08), Phoenix, AZ.

Borch, K. (1960). The safety loading of reinsurance premiums. *Scandinavian actuarial journal, 43*, 163-184.

Breuer, M. (2006). Optimal insurance contracts without the non-negativity constraint on indemnities: revisited. *The Geneva Risk and Insurance Review, 31*(1), 5-9.

Brodkin, J. (2007). TJX breach may spur greater adoption of credit card security standards. *Network World*. Retrieved from http://www.networkworld.com/news/2007/032907-tjx-breach-adopt-standards.html

Buzzard, K. (1999). Computer security -- What should you spend your money on? *Computers & Security, 18*(4), 322-334.

Cameron, C. A., & Trivedi, P. K. (1998). *Regression analysis of count data*. Cambridge, UK: Cambridge University Press.

Camp, L. J. (2006). Economics of Information Security. *SSRN eLibrary*.

Camp, L. J., & Wolfram, C. (2000). *Pricing security.* Paper presented at the The CERT Information Survivability Workshop, Boston.

Campbell, K., Gordon, L., Loeb, M., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach

announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70-104.

Cavusoglu, H., & Raghunathan, S. (2004). Economics of IT security management: Four improvements to current security practices. *Communications of the Association for Information Systems, 14*, 65-75.

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

Claflin, B. (2001). Information Risk Management at 3Com. *Secure Business Quarterly, 1*(2).

Clark, T. H., & Hammond, J. H. (1997). Reengineering channel reordering processes to improve total supply-chain performance. *Production and Operations Management, 6*(3), 248-265.

Cohen, F. B. (1995). *Protection and security on the information superhighway*. New York: John Wiley & Sons, Inc.

Crane, M. (2001). International liability in cyberspace. *Duke Law & Technology Review, 23*(1).

Denning, D., & Denning, P. J. (1997). *Internet besieged: Countering cyberspace scofflaws*. Reading, MA: ACM Press.

Doherty, N. A., & Schlesinger, H. (1983). Optimal Insurance in Incomplete Markets. *The Journal of Political Economy, 91*(6), 1045-1054.

Doll, M. (2002). Security & Technology Solutions: The 2002 Ernst & Young Digital Security Overview: An Executive Guide and Diagnostic. *Ernst & Young LLP*.

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

Ehrlich, I., & Becker, G. S. (1972). Market Insurance, Self-Insurance, and Self-Protection. *The Journal of Political Economy, 80*(4), 623-648.

Evers, J. (2005). Hacking for dollars. Retrieved August 15, 2010, from CNET News: http://news.cnet.com/Hacking-for-dollars/2100-7349_3-5772238.html

Finne, T. (1998). A conceptual framework for information security management. *Computers & Security, 17*(4), 303-307.

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

Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: the real threats in the new millennium? *Computers & Security, 18*(1), 28-34.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *INFORMATION SYSTEMS RESEARCH, 16*(2), 186.

Geer, D. (1998). Risk management is where the money is. *The Risks Digest, 20*(6).

Geer, D. (2003). Risk management is still where the money is. *IEEE Computer, 36*(12), 129-131.

Gold, J. (2002). Insurance Coverage for Internet and Computer Related Claims. *Computer and Internet Law., 19*(4), 8-16.

Gollier, C. (1996). Optimum Insurance of Approximate Losses. *The Journal of Risk and Insurance, 63*(3), 369-380.

Gordon, L., & Loeb, M. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security, 5*(4), 438-457.

Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2004). 2004 CSI/FBI computer crime and security survey. *COMPUTER SECURITY JOURNAL, 20*(3), 33-51.

Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI computer crime and security survey*: Computer Security Institute.

Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2006). *2006 CSI/FBI Computer crime and security survey*: Computer Security Institute.

Gordon, L., Loeb, M., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81-85.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2002). An economics perspective on the sharing of information related to security breaches: Concepts and empirical evidence. University of California, Berkeley.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. [doi: DOI: 10.1016/j.jaccpubpol.2003.09.001]. *Journal of Accounting and Public Policy, 22*(6), 461-485.

Gralla, P. (2001). Electronic safety net: Cyberinsurance policies can offer protection when technology fails. *CIO Magazine, 15,* 126-129.

Grance, T., Hash, J., Peck, S., & Smith, J. (2002). Security guide for interconnecting information technology systems. *NIST Special Publication*, 800-847.

Greene, W. H. (2003). *Econometric analysis* (5th ed.). Upper Saddle River, NJ: Pearson Education Inc.

Grubbs, F. (1969). Procedures for detecting outlying observations in samples. *Technometrics, 11*(1), 1-21.

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy, 26*(6), 639-688.

Hausman, J., Hall, B. H., & Griliches, Z. (1984). Econometric Models for Count Data with an

Application to the Patents-R & D Relationship. *Econometrica, 52*(4), 909-938.

Hofmann, A. (2007). Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks. *The Geneva Risk and Insurance Review, 32*(1), 91-111.

Hosmer, D., & Lemeshow, S. (2000). *Applied logistic regression*. New York: Wiley-Interscience.

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

Hulme, G. (2002, January 28). Businesses Keep Spending On Security. *InformationWeek*. Retrieved from http://www.informationweek.com/news/software/showArticle.jhtml?articleID=6500479

Johnson, M., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, 16-24.

Kang, J. (2010, April 1, 2010). A hakcer threatened online shopping malls for ransoms *The Digital Times*.

Kannan, K., & Telang, R. (2005). Market for software vulnerabilities? Think again. *Management Science, 51*(5), 726-740.

Karofsky, E. (2001). Insight into return on security investment. *Secure Business Quarterly, 1*(2).

Kesan, J., Majuca, R., & Yurcik, W. (2005a). *Cyber-Insurance as a Market-Based Solution to the Problem of Cybersecurity.* Paper presented at the The Workshop on the Economics of Information Security, Cambridge, MA

Kesan, J., Majuca, R., & Yurcik, W. (2005b). *The Economic Case for Cyberinsurance*. Paper presented at the Securing Privacy in the Internet Age Symposium.

Korean Internet & Security Agency. (2007). *2007 Korean Information Security Survey*. Seoul, Korea: Korean Internet & Security Agency.

Korean Internet & Security Agency. (2008). *2008 Korean Information Security Survey*. Seoul, Korea: Korean Internet & Security Agency.

Kovacs, P., Markham, M., & Sweeting, R. *Cyber-Incident Risk in Canada and the Role of Insurance* (No. 38). Toronto, ON: Institute for Catastrophic Loss Reduction.

Kruyer, P. (1997). *Recent Developments in Organised Crime*. Paper presented at the Information Warfare Conference 1997.

Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty, 26*(2), 231-249.

Lai, C., Medvinsky, G., & Neuman, B. (1994). *Endorsements, licensing, and insurance for*

distributed system services. Paper presented at the 2nd ACM Conference on Computer and Communications Security Fairfax, VA.

Lakdawalla, D., & Zanjani, G. (2005). Insurance, self-protection, and the economics of terrorism. *Journal of Public Economics, 89*(9-10), 1891-1905.

Lelarge, M., & Bolot, J. (2009). *Economic incentives to increase security in the internet: The case for insurance.* Paper presented at the The IEEE Conference on Computer Communications, Rio de Janeiro, Brazil.

Liu, W., Tanaka, H., & Matsuura, K. (2008). Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms. *Information and Media Technologies, 3*(2), 464-478.

Long, S. (1997). *Regression models for categorical and limited dependent variables*. Thousand Oaks, CA: Sage Publications, Inc.

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

Main, A., & van Oorschot, P. (2003). Software protection and application security: Understanding the battleground. *International Course on State of the Art and Evolution of Computer Security and Industrial Cryptography, Heverlee, Belgium*.

Majuca, R. P. (2006). *Three essays on the law and economics of information technology security.* University of Illinois at Urbana-Champaign.

Majuca, R. P., Yurcik, W., & Kesan, J. (2006). *The evolution of cyberinsurance. In ACM Computing Research Repository (CoRR), Technical Report cs.CR/0601020*.

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

Martin, R. A. (2001). Managing vulnerabilities in networked systems. *Computer, 34*(11), 32-38.

Meadows, C. (2001). A cost-based framework for analysis of denial of service in networks. *Journal of Computer Security, 9*(1), 143-164.

Moon, B. (2008, October 10, 2010). DDoS attackers hold website to ransom. *Electronic Times Internet*.

Muermann, A., & Kunreuther, H. (2008). Self-protection and insurance with interdependencies. *Journal of Risk and Uncertainty, 36*(2), 103-123.

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

Mukhopadhyay, T., Kekre, S., & Kalathur, S. (1995). Business value of information technology:

a study of electronic data interchange. *MIS Quarterly, 19*(2), 137-156.

National Information Society Agency. (2006). *2006 Information Society Statistics*. Seoul, Korea: National Information Society Agency.

Norman, R. P. (2001). Virtual Insurance Risks. *The Brief, 31*(1), 14-27.

Ogut, H. (2006). *Information technology security risk management.* Unpublished 3210675, The University of Texas at Dallas, Dallas, Texas.

Ogut, H., Menon, N., & Raghunathan, S. (2005). *Cyber Insurance and IT Security Investment: Impact of Interdependent Risk.* Paper presented at the The Workshop on the Economics of Information Security, Cambridge, MA

Ogut, H., Raghunathan, S., & Menon, N. (2004). Self Protection and Insurance in IT security: The case of Interdependencies. The University of Texas at Dallas.

Ogut, H., Raghunathan, S., & Menon, N. M. (2005). Information security risk management through self-protection and insurance. The University of Texas at Dallas.

Ozment, A. (2004). *Bug auctions: Vulnerability markets reconsidered.* Paper presented at the 3rd Annual Workshop on Economics of Information Security, Minneapolis, Minnesota.

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

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

Powell, B. (2005). Is cybersecurity a public good? Evidence from the financial services industry. *Journal of Law, Economics and Policy, 1*(2), 497-510.

Radianti, J., & Gonzalez, J. (2007). *A Preliminary Model of The Vulnerability Black Market.* Paper presented at the 25th International System Dynamics Conference, Boston, MA.

Rathmell, A. (1999). Cyber-Terrorism: The Shape of Future Conflict? *Journal of Financial Crime, 6*.

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

Richardson, R. (2008). *2008 CSI Computer Crime and Security Survey*: Computer Security Institute.

Ridd, J., & Information Assurance Advisory Council. (2002). *Insuring Digital Risk: A Roadmap for Auction*: Information Assurance Advisory Council.

Ridd, J., & Rand Europe. (2002). *Insuring Digital Risk: A Roadmap for Action*. Cambridge, U.K.: Information Assurance Advisory Council.

Rothschild, M., & Stiglitz, J. (1976). Equilibrium in Competitive Insurance Markets: An Essay

on the Economics of Imperfect Information. *The Quarterly Journal of Economics, 90*(4), 629-649.

Schechter, S. (2002). *Quantitatively Differentiating System Security.* Paper presented at the 1st Annual Workshop on Economics of Information Security, Berkeley, California.

Schlesinger, H. (1981). The Optimal Level of Deductibility in Insurance Contracts. *The Journal of Risk and Insurance, 48*(3), 465-481.

Schlesinger, H. (1997). Insurance Demand without the Expected-Utility Paradigm. *The Journal of Risk and Insurance, 64*(1), 19-39.

Schneier, B. (2001). Insurance and the computer industry. *Communications of the ACM, 44*(3), 114-115.

Schneier, B. (2002). *Computer security: It's the economics, stupid.* Paper presented at the 1st Annual Workshop on Economics of Information Security, Barkeley, CA.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Srinivasan, K., Kekre, S., & Mukhopadhyay, T. (1994). Impact of electronic data interchange technology on JIT shipments. *Management Science, 40*(10), 1291-1304.

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

Stokes, M., Davis, C., & Koch, G. (2000). *Categorical data analysis using the SAS system*: SAS publishing.

Straub Jr, D. (1990). Effective IS Security. *Information Systems Research, 1*(3), 255-276.

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

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

Symantec. (2007). *Symantec Internet Security Threat Report*: Symantec Corp.

Symantec. (2010). *Symantec Internet Security Threat Report*: Symantec Corp.

Tally, G. (2009). *Phisherman: A Phishing Data Repository.* Paper presented at the Conference For Homeland Security, 2009. CATCH '09. Cybersecurity Applications & Technology.

Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy, 24*(1), 37-59.

Taylor, P. A. (1999). *Hackers: crime in the digital sublime*. New York, NY: Routledge.

Tukey, J. (1977). *Exploratory Data Analysis*. Massachusetts: Addison-Wesley.

Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review, 23*(1), 8.

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

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

Varian, H. (2004). System reliability and free riding. In J. Camp & S. Lewis (Eds.), *Economics of Information Security* (pp. 1-15). Norwell, MA: Kluwer Academic Publishers.

Vatis, M. A. (2001). *Cyber attacks during the war on terrorism: A predictive analysis*. McLean, VA: Institute for Security Technology Studies at Dartmouth College.

Vaughn, R., Henning, R., & Siraj, A. (2003). *Information assurance measures and metrics: State of practice and proposed taxonomy.* Paper presented at the HICSS '03, Hawaii.

Weiss, T. R. (2002, Febraury 27). Security holes closed in New York Times intranet after hacker intrusion. *Computerworld*. Retrieved from http://www.computerworld.com/s/article/68662/Security_holes_closed_in_New_York_Times_intranet_after_hacker_intrusion

Wiseman, S. (1986). *A secure capability computer system.* Paper presented at the IEEE Symposium on Security and Privacy, Los Alamitos, CA.

Wooldridge, J. (2003). *Introductory econometrics: A modern approach* (2nd ed.). Mason, OH: Thomson South-Western.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the Minds of Hackers. *Information Systems Management, 24*(4), 281 - 287.

Yurcik, W., & Doss, D. (2002). *Cyberinsurance: A market solution to the internet security market failure.* Paper presented at the The Workshop on the Economics of Information Security, Berkeley, CA.

Zhao, X. (2007). *Economic analysis on information security and risk management.* The University of Texas at Austin, Texas.

Zhao, X., Xue, L., & Whinston, A. (2009). *Managing Interdependent Information Security Risks: An Investigation of Commercial Cyberinsurance and Risk Pooling Arrangement*. Paper presented at the Thirtieth International Conference on Information Systems.