National Cheng Kung University

Department of Transportation and Communication Management Science

Doctoral Dissertation

Network Externality and Incentive to Invest in Network Security

網路安全外部性與投資誘因之研究

Student: Chun-Wei Chen

Advisor: Dr. Chun-Hsiung Liao

June, 2014

國立成功大學

交通管理科學研究所

博士論文

網路安全外部性與投資誘因之研究

Network Externality and Incentive to Invest in Network Security

研究生：陳俊偉

指導教授：廖俊雄博士

中華民國一百零三年六月

國立成功大學
博士論文

網路安全外部性與投資誘因之研究
Network Externality and Incentive to Invest in Network Security

研究生：陳俊偉

本論文業經審查及口試合格特此證明

論文考試委員：

指導教授：

系(所)主管：

中　華　民　國　103　年　6　月　5　日

Abstract

In today's information-based economy, the network evolution is one of the greatest innovations and has changed lives of individuals and business organizations. Computer technology and the Internet play a ubiquitous role in economic activities related to consumption and transactions. Home shopping Home economics has been booming in recent decades since public consumption behavior has substantially changed. For this reason most organizations depend on information technology (IT) systems to store, process and exchange critical information with their customers, partners and shareholders. This dependency comes along with major risks to the information and its IT systems. As a result Network security incidents frequently occur along with the rapid evolution of new cyber crimes. Breaches of network security can result in substantial losses for businesses. With the results of shown in 2008 CSI/FBI computer crime and security survey, the average loss per respondent was $288,618 for 144 respondents, down from $345,005 in 2007, but up from the low of $167,713 in 2006. This is the main reason why organizations are investing in Network security systems, which are designed to protect the confidentiality, integrity and availability of information assets. The importance of information security has led many organizations to pay close attention to related investment decisions.

This research examined how network externality influences the optimal strategy of a firm with regard to investments in network security (NS). A theory-based model is developed to investigate in the short run how network externality influences the optimal strategy of competing online firms producing homogenous services related to investment in NS. The incentive of a firm to invest in NS is derived, and the impact of the survival probability, market size, and the effect of the number of firms investing in NS on a firm's incentive to invest in NS are also analyzed. Policy implications drawn from the research are provided at the end the work.

Keywords: Network externality, network security investment, technology effectiveness of NS, survival probability

摘要

在當今的信息經濟，網絡演進是最偉大的發明之一，並已經改變了個人和企業組織的日常活動。在消費和交易的經濟活動中，電腦技術和互聯網無所不在。近 20 年來大眾消費行為已顯著改變，宅經濟正蓬勃發展。正因如此，企業大多採用資訊科技系統來存儲、處理和交換與他們的客戶、合作夥伴和股東的關鍵資訊。然而，對網路系統的依存性，其風險也隨之產生。因此新式網絡犯罪的迅速發展造成網絡安全事件頻頻發生。網絡安全漏洞可能會導致企業重大的損失。根據 2008 年 CSI / FBI 計算機犯罪和安全調查顯示的結果，在 144 企業受訪者中，2007 年平均最高損失為 345005 美元。. 這就是為什麼企業要投資網絡安全系統的主要原因，其目的是為了保護資訊資產的機密性，完整性和可用性的。

本研究欲探討網絡外部性如何影響企業對網絡安全投資的策略。本文根據電子商務產業中，同質商品的競爭，建立一個理論模型來分析在短期內網絡外部性如何影響企業對網絡安全投資的最適策略。藉由廠商對網絡安全投資誘因的推導，進而分析生存機率、市場規模、投資廠商家數對投資誘因的影響。最後根據研究結論得到政策意函，冀期電子商務產業甚至整體網路環境安全能有所提升。

關鍵字：網路外部性、 網路安全投資、網路安全技術效率、存活機率

誌謝

這篇論文的完成，首先要感謝我的指導教授 廖俊雄老師。感謝老師當年的收留以及為學生在論文指導上所花費的精力與時間，讓學生的文章能被國際期刊刊登順利畢業。而且除了論文的指導外，老師平常對學術圈中為人處世的提點，使我對未來再更進一步延修時有更深刻的認識，老師不但是我的授業老師，更是一位重要的人生導師。 感謝鄭永祥博士、康信鴻博士、胡政成博士、翁明宏博士、呂錦山博士、胡均立博士、吳健瑋博士、陳建良博士提供了寶貴且專業的意見，使得本論文的內容更加完備充實，而對我而言也啟發了許多未來研究的點子。

在成大交管這大家庭待了近五年，很感謝交電管系學弟妹的陪伴，讓乏味的研究象牙塔添加許多歡樂，也感激系上老師們指導，尤其交管道義、承先啟後的傳統，讓學生的頓悟特別深。無論是在前期課業上一起奮鬥的老師、學長姐、同學，或是遇到瓶頸時陪我發洩放鬆的小連、小米學弟妹們；給我許多研究方面建議的柏興學長以及 YY 學姊；在相關行政程序上、欣怡、易宸等學弟妹以及系上助教的幫忙。

最後我還要感謝我的父母，感謝您們的支持，感謝您們對我付出的一切，並與您們分享我的喜悅。

Table of Contents

List of Figures

Chapter One

Introduction

Electronic commerce (e-commerce) is playing an increasingly important role in both daily life and in the business world due to rapid advances in information technology (IT). According to the U.S. Census Bureau (2010), the percentage of e-commerce sales to total U.S. retail sales increased from 3.4 percent (137 billion) in 2007 to 3.6 percent (142 billion) in 2008, as more and more consumers now shop and carry out financial transactions online, without the need to leave their homes. However, this has been accompanied by a rise in the number of network security (NS) breaches, with new patterns of online fraud behavior being discovered each year. The Computer Security Institute and Federal Bureau of Investigation surveyed 522 Internet-related firms about their financial losses due to computer crime and security breaches, and the results showed that the average loss per respondent in 2008 was $288,618.00, a sharp increase of 72.1% from $167,713.00 in 2006 (Richardson, 2008).

The use of network systems in e-commerce businesses is driven by the lower costs and increased customer satisfaction that they offer, as well as by the trend toward greater globalization. The development of e-commerce has had profound impacts in individual sectors of the economy, as well as in macroeconomic performance and economic policies (Coppel, 2000). The use of e-commerce in the U.S. software industry provides a good example of the cost advantages of this form of delivery, as it is estimated that seller transaction costs are $15 for face-to-face transactions, $5 for telephone transactions, and only between 20 and 50 cents for those occurring online (Bollier, 1996).Similar results have been found in the Australian market, in which seller transaction costs are $300 for a sales representative visit and less than 25 cents for an Internet transaction (Callaghan, 1999).

However, as firms have to rely more and more on the Internet to promote and sell their products and services, there has been a corresponding rise in the number of security attacks on their online systems. The types of security threats that such firms face include denial of service (DoS) attacks, Trojan horses that come with other software applications, viruses that reproduce by attaching themselves to executable files, worms that create copies of themselves and spread by using e-mail address books, and logic bombs that are dormant until an event triggers them (e.g., a specific date or user action). Such attacks can cause a loss of services or system crashes, leading to damage to or the destruction of data, the loss of sensitive information to hostile parties, the use of information to steal items of monetary value or otherwise negatively affect an organization's customers, and damage to the reputation of the compromised organization.Global Payments, a leader in payment processing services, announced on Friday, March 30, 2012, that had it identified and self-reported unauthorized access into its processing system. In the latest case, a massive theft of customer data from three major credit card firms in South Korea indicated security lapses in the financial industry on January, 2014. The country's largest-ever theft of personal financial data from KB Kookim Bank, LotteCard and NH Nonghyup Card involved more than 40 percent of the country's 50 million population. Warrington, Abgrab, and Caldwell (2000) concluded that initiating consumer trust and developing stable relationships with online shoppers are the keys to exploiting the full potential of e-commerce and to improving its profitability. Strategic decision-making in an online context must thus take into account issues of network security.

In order to avoid these problems, it is necessary for organizations to invest in network security, and related technologies include firewalls, intrusion detection systems, and anti-virus software, while specific network layout approaches can also be useful. CompTIA (2007), based on a survey of more than 1,000 U.S. corporations, revealed that companies spent, on average, 20 percent of their total technology budget in 2006 on security measures, up from 12 percent in 2004, and nearly one-half of those surveyed planned to continue to increase IT security

spending. While firms that spend too little on such security may suffer more losses due to network attacks, if they spend too much, then this will also reduce their profits. Therefore, it is necessary to develop an optimal NS strategy in order to maximize both security and profits, and that is the aim of the current work.

Reliable network security is necessary to protect online business operations because harmful consequences can arise if unauthorized users can gain access to the information and services in a network. In particular, the security risks associated with malicious hackers and viruses can lead to financial losses and the loss of customer confidence and even force companies to leave their online markets (Kumar, Park, &Subramaniam, 2008). Various NS technologies (e.g., firewalls, anti-virus software and intrusion detection systems) are thus used in order to maintain and protect the online business operations and information assets of firms from malicious security incidents.

Investments in NS have two effects; one is a decrease in the potential losses resulting from security incidents, and the other is an increase in operating costs. A firm thus has to make a choice from among various security investment options depending on the level of threats that it faces and its budget constraints (van Kessel, 2009). Therefore, the issue of selecting the optimal NS strategy against computer-related risks has attracted considerable academic attention, with the literature assessing the influence of network vulnerability and evaluating both threat probability and the value of the assets to be protected (Gordon & Loeb, 2002; Hoo, 2000; Schechter & Smith, 2003). Various financial metrics and forms of cost-benefit analysis have been adopted to compare potential losses and the costs of NS investments based on quantitative decision analyses.

A qualitative risk analysis prioritizes the identified project risks using a pre-defined rating scale. Risks will be scored based on their probability or likelihood of occurrence and the impact on project objectives should they occur. Probability/likelihood is commonly ranked on a zero to one scale, and the impact scale is organizationally defined. A qualitative risk analysis will also include the

appropriate categorization of the risks, either source-based or effect-based. A quantitative risk analysis is a further analysis of the highest priority risks in which a numerical or quantitative rating is assigned in order to develop a probabilistic analysis of the project. In order to conduct a quantitative risk analysis, high-quality data, a well-developed project model, and a prioritized lists of project risks arerequired. While a qualitative risk analysis should generally be performed on all risks, for all projects, a quantitative risk analysis has more limited uses, based on the type of project, the project risks, and the availability of data to use to conduct the quantitative analysis (Passionate Project Management, 2013).

In particular, most studies of the losses related to an NS breach event only consider its immediate effects rather than those that are indirect. However, indirect effects can have serious impacts on firms, as they can harm their reputations, lead to the loss of trust felt by customers and supplier partners, and damage relationships with partner companies (Dynes, Johnson, Andrijcic, & Horowitz, 2007; Camp & Wolfram, 2004; Rowe & Gallaher, 2006). Since a firm's optimal investment amount is based on the results of a cost-benefit analysis, ignoring the indirect effects of NS breaches related to network externalities will lead to suboptimal decisions being made.

The externality of a good as it relates to consumption refers to a phenomenon in which an entity is affected by another entity's usage of that good (e.g., mobile phones, social networking applications, and public goods). Network security in a communication network depends not only on the security-related prevention investments made by individual users, but also on the reciprocal relationships among the users. Without taking network externalities into consideration, the optimal NS investment will be underestimated. Hence, equilibrium without externality will deviate from a socially optimal level and will in turn result in market failure (Jiang, Anantharam, & Walrand, 2008b; Yue, Cakanyildirim, Ryu, & Liu, 2007).

The main goal of this research is to investigate how network externalities, interaction strategies and market size affect the incentive to invest in NS, and what the resulting optimal investment strategy should be. This research analyzes, by considering a game theory-based threat versus an investment model, the optimal strategy in the short run for investing in NS in cases where competing online firms produce homogenous services. This research is structured as follows:Chapter 2 reviews the related studies on the optimal strategy for NS investment. Chapter 3 sets up the model for firm NS investment incentives within a competing online market and derives the results and propositions. Finally, the conclusions of this work and its managerial implications are presented in Chapter 4, with the aim of promoting a better NS environment.Chapter 5 suggests directions for future work. Finally, the list of references is included at the end of the dissertation.

Chapter Two

Literature Review

A network security architecture is essential for businesses that sell products through both physical store channels and online. However, the severe consequences of financial and indirect losses from network security breaches in an organization due tospecific security vulnerability have increasingly attracted academic attention along with the adoption of network systems for e-commerce businesses. The three main aims in the literature on optimal NS investment are preventing and/or reducing the potential losses caused by security breaches, reducing the problem of "free riders" among stakeholders who do not contribute their fair share to the related investments, and the balance of monetary and technical resources input by firms vs. those of attackers with regard to this issue (Huang, Hu, &Behara, 2008).Various approaches to optimal NS investment decisions have been adopted in different types of firms and in different environments, and studies since Anderson (2001) have adopted an economic perspective of the assessment of the necessary level of investment in security technology that can be divided into two streams according to the methodologies used, those based on decision theory and those based on game theory.

In the literature that takes a decision theory-based approach, NS strategy is assessed by calculating the costs and benefits of NS investments by identifying the key variables (e.g., asset value, security risk, degree of threats, cost of breaches). This quantifying approach adopts financial metric indexes by using multiple

economic indexes of annual loss expected (ALE), return on investment (ROI) (Bojanc&Jerman-Blažič, 2008a; Hausken, 2006; Tsiakis&Stephanides, 2005; Iheagwara, Blyth, Kevin, &Kinn, 2004; Purser, 2004), net present value (NPV) (Bojanc&Jerman-Blažič, 2008b), and internal rate of return (IRR) (Bojanc&Jerman-Blažič, 2008a).

For example, Bayuk (2001) provided a risk analysis model of ROI-maximizing NS investments and illustrated how much money had to be spent to achieve a "reasonable" degree of security. In this approach, the risk is assumed to be quantifiable as a dollar amount, such as the loss of revenue that would be incurred by a given order-processing system or manufacturing line when an attack is successful. The optimal IS investment is derived at the point where the dollar amount at risk is equal to the price of the security improvement. Iheagwara et al. (2004) measured the financial benefits of deploying an intrusion detection system (IDS) by incorporating a standard risk analysis framework with a cascading threat multiplier (CTM). A CTM is a security breach that results in two types of costs: the direct cost of lost integrity, confidentiality, and/or availability, and the indirect cost of the compromised component serving as a potential stepping stone for future attacks. Their paper attempted to capture the second type of CTM costs, which are typically ignored in the classic risk analysis framework. The proposed risk analysis formulas included incorporating the concept of CTM in the ROI calculations and provided an illustration of an effective decision-making process used to indicate which techniques are most appropriate for the cost effective management of IDS in a given environment. Iheagwara et al. (2005) further developed multiple metrics that enable risk and cost-benefit assessments to be made to calculate the ROI of information assurance technology investments.

Similarly, Bojanc and Jerman-Blažič (2008b) introduced methods for identifying the assets, threats, and vulnerabilities of Information and Communications Technology systems, and proposed a procedure to recommend the optimal investment choice for the necessary security technology based on the

quantification of various values of the protected systems (e.g., an economic index combination of ROI, NPV and IRR). The efficiency of different NS options was evaluated, and the optimal NS investment was then selected under various scenarios. Wang and Song (2008) proposed a flexible NS investment model that addresses the conflict between costs and benefits. First, the model quantifies the risk and effectiveness of a certain tool or policy and then obtains the optimal investment strategy using a multi-objective decision-making framework. It can be applied by IT managers and stakeholders to make more confident assessments of NS infrastructure spending decisions.

However, no single index can be used to assess the optimal investment required for the prevention of security threats, and thus the application of these simple rules has not been fully validated, as they fail to take into account the wide range of factors and constraints that may influence the NS investment process, such as network externalities and market size. The probability, frequency and size of true network security losses and benefits therefore remain difficult to identify and estimate using the approaches in these referenced works.

Another stream of the literature, the widely used social scientific knowledge, the so-called game theory, has been applied in modeling and analyzing the optimal NS investment (Cavusoglu, Mishra, & Raghunathan, 2004; Garcia & Horowitz, 2007; Liu, Zang, & Yu, 2005; Wang et al., 2012). A game is a description of a strategic interaction which places constraints on the actions that the players can take and their interests, but does not specify the actions that the players do take. A solution is a systematic description of the outcomes that may emerge in a family of games. In brief, game theory suggests reasonable solutions for classes of games and also examines their properties.

Cavusoglu et al. (2004) considered a game tree used to depict the strategies of a firm and a hacker in order to evaluate the investments in an NS architecture. Both a firewall and an intrusion detection system were examined, leading to a value assessment of the two technologies. The firm minimized its investment cost and loss,

but the hacker maximized its utility from the intrusion and cost if detected. The intrusion action of the hacker and successful detection using the two technologies of the firm were given with probabilities. The results provided a guideline for choosing an alternative security technology in which to invest and concluded that firms should evaluate the value of an additional security mechanism based on already existing controls before estimating its return.

Liu et al. (2005) presented a methodology to model the interactions between an attacker and a network administrator. This approach suggested that the ability to model and infer attacker intent, objectives, and strategies (AIOS) is important as it can lead to effective risk assessment and harm prediction. An incentive-based game-theoretic model to infer AIOS was discussed in this work. A few bandwidth parameters were used as the metric to measure the impact of the attack and the countermeasure, which in turn measures both the attacker's and the defender's incentives. The work also proposed that the best game model to choose depends on the degree of accuracy of the employed intrusion detection system (IDS) and the degree of correlation among the attack steps. The study used a specific case to show how attack strategy can be inferred in real-world attack-defense scenarios.

Garcia and Horowitz (2007) presented a game-theoretic model that applies the economic motivations for investment in added NS and attempted to discover a possible market failure in the underinvestment of NS. They considered the competitive market of two symmetric firms in which the firms plan NS investment taking into account the likelihood of a security breach. The result relies on the fact that social value is derived from Internet usage, which is at least equal to a fraction of the surplus derived from e-commerce. It was concluded that when the ratio of social value to revenue at stake to Internet providers continues to grow, the likelihood of underinvestment in security becomes higher and some form of regulation may become necessary.

Wang et al. (2012) proposed stochastic game nets for the purpose of modeling and analyzing the competitive behaviors of enterprise networks in a dynamic game.

The interactions between administrators of enterprises and the attackers, as well as the probability of a successful intrusion action by the attacker and the mean time of administrative repair were incorporated into the model. The results showed that the mean time for a successful attack is longer when the mean time to repair is shorter with a high transition firing rate after a specific time point. Further, the availability is better with a high transition firing rate in practice. Nevertheless, these studies ignored the existence of network externality, which is the essential characteristic in networks.

Regardless of whether it is the decision-theory-based evaluation method or game theory that is considered, these approaches have somehow been constrained from the difficulties in estimating and identifying the probability, frequency, and size of network security loss and benefit, as well as other parameters. In their model setup, they neglected the effect of externality. Hence, the model used in the current researchendogenizes network externalities because they affect the likelihood of vulnerabilities in the online market. Furthermore, we focus on the incentive of increasing-decreasing direction influenced by the factors under the partitions of the situation.

Network security investment in one firm is usually dependent on other firms' security investments in the connected network. This is sometimes referred to as "neighborhood effects", and economists call this a network externality. That is, network security is characterized by a positive "externality." If one firm takes more precautions to protect their IT system, the security of other firms, as well as their own, is enhanced. However, such settings lead to the classic free-rider problem (Varian, 2004). In the absence of a market for security, individuals will choose less security than is socially optimal (Kunreuther & Heal, 2003; Ogut, Menon, & Raghunathan, 2005 ;Powell, 2005; Tsiakis, Katsaros, &Gritzalis, 2012).

Kunreuther and Heal (2003) formalized the concept of interdependent security with their primary example stemming from the airline industry.In this case, the individual airlines were concerned about a major single attack that could originate

at some point in the network and could be propagated to another airline in the system. Airlines could defend themselves against direct attacks, but were weak in regard to dangerous loads received from other aviation entities. Varian (2004) started a formal discussion on the role of security as a public good and the effects of individuals working in teams with varying incentives and the effects on NS. The property of interdependent security is similar to that of network externality in the field of economics. The network externality of security investments often induces firms to invest inefficiently from a socially optimal perspective(Ogut et al., 2005; Powell, 2005). The conclusion that network externalities influence network security investment is also provided by Yue et al. (2007). They demonstrated that network externalities have a negative influence on network security investment by showing that the expected IT security risk for organizations is underestimated when this is not considered.

Jiang, Anantharam, and Walrand (2008a) used a network security game where strategic players chose their investments in security. Their model explicitly considered the network topology, thedifferent cost functions of players, and their relative importance to each other. They showed that in a strategic-form game, the price of anarchy (POA) can be very large and tends to increase with the network size, as well as with the dependency and imbalance among the players. This finding indicates that the overall network security can be far from optimum in the case of selfish players. However, the best equilibrium in the repeated game usually results in much better performance, allowing the possibility of achieving a social optimum if that does not conflict with individual interests. In the model, they considered the externality with a linear combination setup. Comparatively, in this study, we take the externality into account with the concave function of the number of players with network security investments. The setting relatively tallies with intuition in actuality.

Lelarge (2009) further modeled and quantified the impact of such externalities on the adoptability and deployment of security features and protocols on the

Internet. Bolot and Lelarge (2009) considered a network of interconnected agents which are subject to epidemic risks, such as those caused by propagating viruses and worms, and which can decide whether or not to invest some amount to deploy security solutions. Their models combined the propagation of epidemics among networked agents and the payoffs for agents. Agents, interacting with the cyber-attackers, are meant to reduce both riskand loss. The optimal strategy for agents, by simulations of random graphs, was found to be the maxminimizer strategy. In particular, the positive impact of network externalities on the security investments was explicitly identified. They illustrated in detail how network externalities impact investment in network security. However, their approach did not scale the efficiency of NS technology while the potential loss is fixed. This researchis intended to release those limitations.

Tsiakis, Katsaros, &Gritzalis (2012) proposed an impact pathway approach that distinguished the economic tradeoffs for security investments along with security measures and investments in private and public goods. Externalities are social costs that are not carried by the private costs and prices of market goods/services. Their results suggested the establishment of a policy to consider and reduce the social costs that systems generate either by regulating such operations or by imposing high economic penalties, or both.

The role of incentive for investment in NS is a relatively new research issue. August and Tunca (2006) investigated the effect of user incentives on software security in a network of individual users under costly security investment patching and negative network security externalities. Gal-Or and Ghose (2005) found that security technology investments and security information sharing act as “strategic complements” in regard to equilibrium. The results suggest that information sharing is more valuable when product substitutability is higher, implying that such sharing alliances yield greater benefits in more competitive industries. Bolot and Lelarge (2009) showed that if a premium discriminates against users that do not invest in security, then insurance is a strong incentive to invest in NS. These results imply

that the incentive for investing in NS will increase when externalities exists and have a positive effect on each other.

Nevertheless, the above studies have seldom considered the existence of network externality. Some studies have assumed a constant potential loss of a successful attack in which the efficiency of NS technology cannot thus be measured (Bolot & Lelarge, 2009; Lelarge, 2009), and others have ignored the strategic interactions among agents in the decision to engage in NS investment (Jiang et al., 2008a). Overall, these studies were also constrained from the difficulties involved in estimating and identifying the probability and frequency of attack and the benefits induced by NS investment. This research investigates how network externalities influence the optimal strategy of competing online firms producing homogenous services with regard to investing in NS.The self-protect rate of a firm and survival probability against security incidents differ depending on whether or not it invests inNS.

Some restrictions embedded in the literature mentioned above are relaxed in this work, and the level of network externality in this research is endogenous and varies with the number of firms that invest in NS. In a departure from the prior literature, in this research, the prior probabilities of survival with NS-investing and non-NS-investing are conjectured, and thus are not necessarily equal to the real survival rates with and without NS investments. The next chapter presents the model framework in which firms are strategically interconnected with regard to their NS investments, with specific levels of NS threat and effectiveness of NS technologies. The effectiveness of NS technology is evaluated by measuring the revenue a firm generates in the market when NS successfully defends a firm against security incidents.

Chapter Three
Methodology

This chapter sets up the framework of a firm's incentive to invest in NS within a competing online market and investigates the influence of survival probability and network externality on this incentive. The chapter is divided into four sections. Section 3.1 describes the model settings in the early design scenario. Section 3.2 demonstrates howthe levels of survival probability affect a firm's incentive toward network security. Section 3.3 investigates the effects of the numbers of surviving NS/non-NS firms and the related network externalities on these incentives. Section 3.4illustrates the influences of network effects and market competition.

3.1 Model Description

Consider a perfectly competitive market whereexists a finite number*n*of symmetric firms, $N = \{1, 2, ..., n\}$, providing homogenous services online under the threat of potential cyber crime risks. In the short run, the profit of a competitive firm could be anything that is above its fixed cost (Mankiw, 2012).These firms face threats from security incidents that result in the collapse of a firm's service systems and the loss of customers. In the model, firms simultaneously and independently decide whether or not to invest in NS that increases the ability to prevent such attack threats. If an attack is successful, the firm's system is shutdown,and it is forced to leave the market, giving it zero profit. Otherwise, a firm successfully defends against the attack and maintains its system operations. The decisions are made in the form of a one-shot game. For simplicity, assume zero production cost for the service, and assume that the total profit of the market is normalized to 1.

Consider firm 1 in *N*, and let *M*be the set of firms that invest in NS (hereafter, NS firms), giving $M \subseteq N / \{1\}$. The number of NS firms is *m*, $0 \le m = |M| \le n-1$. Let $f(\bullet)$, $f(\bullet) \ge 1$, be the spillover effect of NS externality, which is an increasing

function of m, $f'(m) > 0$, $f''(m) < 0$. If no firm invests in NS (i.e., $m = 0$), then $f(0) = 1$, and no network externality exists. Each firm that invests in NS incurs a fixed cost and has a self-protection rate, $\tilde{\alpha} = f(m) \cdot \alpha$, which indicates its ability to successfully protect itself from security incidents,and which is the prior probability of survival with NS.[1] A firm that does not invest in NS (hereafter, a non-NS firm) has a probability of survival $\tilde{\beta} = f(m) \cdot \beta$. Here, α represents the effectiveness of an NS technology in defending against an attack, and β represents the probability of a firm successfully protecting itself without NS.

In this model, the network externality refers to the capability of protecting firms from security incidents, indicating a firm's investment increases the survival probability of other firms. It is assumed that $0 < \tilde{\alpha}, \tilde{\beta} \leq 1$, and $\tilde{\alpha} > \tilde{\beta}$. Let n_1 be the survival number of NS-investing firms, $0 \leq n_1 \leq m$, and let n_2 be the survival number of non-NS firms, $0 \leq n_2 \leq n-1-m$, after security incidents. Then $\frac{n_1}{m}$ and $\frac{n_2}{n-1-m}$ are the actual survival rates with NS and without NS, respectively, which are not necessarily equal to the conjectured prior survival probabilities with and without NS in the model. Therefore, the probabilities of the events in which n_1 NS investing firms survive out of *m* and in which n_2 non-NS firms survive out of *n-1-m* are the binomial distributions of $C_{n_1}^{m} \tilde{\alpha}^{n_1} (1-\tilde{\alpha})^{m-n_1}$ and $C_{n_2}^{(n-1-m)} \tilde{\beta}^{n_2} (1-\tilde{\beta})^{(n-1-m)-n_2}$, respectively. The profit of the firm 1 is $\frac{1}{1+n_1+n_2}$, shared equally among n_1 NS survival firms and n_2 non-NS survival firmswhen surviving in the market with the probability $\tilde{\alpha}$.Note thata firm'sprofit is zero when it fails to survive in the market, and the probabilityis $1-\tilde{\alpha}$. The profit function could be reduced as follows:

[1] Note that the self-protection rate of the security system represents the effectiveness of NS technology against attacks and is the opposite of the vulnerability of the system.

$$\begin{cases} R^{\tilde{\alpha}} = \dfrac{1}{1+n_1+n_2} \text{ with the probability of } \tilde{\alpha}\cdot C_{n_1}^{m}\tilde{\alpha}^{n_1}(1-\tilde{\alpha})^{m-n_1}\cdot C_{n_2}^{(n-1-m)}\tilde{\beta}^{n_2}(1-\tilde{\beta})^{(n-1-m)-n_2} \\ R^{\tilde{\beta}} = \dfrac{1}{1+n_1+n_2} \text{ with the probability of } \tilde{\beta}\cdot C_{n_1}^{m}\tilde{\alpha}^{n_1}(1-\tilde{\alpha})^{m-n_1}\cdot C_{n_2}^{(n-1-m)}\tilde{\beta}^{n_2}(1-\tilde{\beta})^{(n-1-m)-n_2} \end{cases}$$

where

$R^{\tilde{\alpha}}$: the profits of firm 1 with NS-investment.

$R^{\tilde{\beta}}$: the profits of firm 1 without NS-investment.

n_1 : the survival number of NS-investing firms.

n_2 :the survival number of non-NS firms.

3.2Firm Incentives in Network Security

The maximal willingness of firm 1 to invest in NS is defined by *W*, $W = E(R^{\tilde{\alpha}}) - E(R^{\tilde{\beta}})$. Thus, the expected profit from NS investment is no less than that of that derived with no NS investment. The formula can be rewritten as

$$\begin{aligned} W &= \frac{\tilde{\alpha}-\tilde{\beta}}{1+n_1+n_2}\left[C_{n_1}^{m}\tilde{\alpha}^{n_1}(1-\tilde{\alpha})^{m-n_1}C_{n_2}^{(n-m)}\tilde{\beta}^{n_2}(1-\tilde{\beta})^{(n-1-m)-n_2}\right] \\ &= \frac{\tilde{\alpha}-\tilde{\beta}}{1+n_1+n_2}\left[\tilde{\alpha}^{n_1}(1-\tilde{\alpha})^{m-n_1}\tilde{\beta}^{n_2}(1-\tilde{\beta})^{n-1-m-n_2}\right]\times \\ &\quad \frac{\left[m(m-1)\cdots(m-n_1+1)\right]\left[(n-1-m)(n-m-2)\cdots(n-m-n_2)\right]}{n_1!\cdot n_2!} \\ &= \frac{\tilde{\alpha}-\tilde{\beta}}{1+n_1+n_2}\left[\tilde{\alpha}^{n_1}(1-\tilde{\alpha})^{m-n_1}\tilde{\beta}^{n_2}(1-\tilde{\beta})^{N-1-m-n_2}\right]\times \\ &\quad \left[\prod_{l_1=1}^{n_1}\frac{m-l_1+1}{l_1}\cdot\prod_{l_2=1}^{n_2}\frac{n-m-l_2}{l_2}\right]. \end{aligned}$$

The relationship between a firm's willingness to invest in NS and the survival probability is summarized in the following proposition:

Proposition 1. There are two kinked points in a firm's incentive to invest in NS along with the level of the survival probability with NS. When the survival probability with NS is in either the low range or high range, the incentive of a firm

to invest in NS increases with NS-investment survival probability. On the other hand, when the survival probability with NS is in the medium range, the incentive of a firm to invest in NS decreases with NS-investment survival probability.

Proof. The natural logarithm on both sides of the incentive of a firm to invest in NS is

$$\ln W = \ln\frac{\tilde{\alpha}-\tilde{\beta}}{1+n_1+n_2} + n_1\ln\tilde{\alpha} + m - n_1\ln(1-\tilde{\alpha}) + n_2\ln\tilde{\beta} + (n-1-m-n_2)\ln(1-\tilde{\beta}) + \sum_{l_1=1}^{n_1}\ln\left(\frac{m-l_1+1}{l_1}\right) + \sum_{l_2=1}^{n_2}\ln\left(\frac{n-m-l_2}{l_2}\right)$$

Total differentiation of the equation would be

$$\begin{aligned}\frac{1}{W}dW = &\left[\frac{1}{(\tilde{\alpha}-\tilde{\beta})} + \frac{n_1}{\tilde{\alpha}} - \frac{m}{(1-\tilde{\alpha})} + \frac{n_1}{(1-\tilde{\alpha})}\right]d\tilde{\alpha} + \left[-\frac{1}{(\tilde{\alpha}-\tilde{\beta})} + \frac{n_2}{\tilde{\beta}} - \frac{(N-1)}{(1-\tilde{\beta})} + \frac{m}{(1-\tilde{\beta})} + \frac{n_2}{(1-\tilde{\beta})}\right]d\tilde{\beta} \\ &+ \left[-\frac{1}{(1+n_1+n_2)} + \ln\tilde{\alpha} - \ln(1-\tilde{\alpha})\right]dn_1 + \left[-\frac{1}{(1+n_1+n_2)} + \ln\tilde{\beta} - \ln(1-\tilde{\beta})\right]dn_2 \\ &+ \left[\ln(1-\tilde{\beta}) + \frac{1}{n-m-1} + \frac{1}{n-m-2} + \cdots + \frac{1}{n-m-n_2}\right]dn \\ &+ \left[\ln(1-\tilde{\alpha}) - \ln(1-\tilde{\beta}) + \frac{1}{m} + \frac{1}{m-1} + \cdots + \frac{1}{m-n_1+1} + \frac{1}{n-m-1} + \frac{1}{n-m-2} + \cdots + \frac{1}{n-m-n_2}\right]dm\end{aligned}$$

Then, the first order condition of W with respect to the survival probability with NS becomes

$$\frac{dW}{d\tilde{\alpha}} = W\left[\frac{\tilde{\alpha}(1-\tilde{\alpha}) + (\tilde{\alpha}-\tilde{\beta})(n_1-\tilde{\alpha}m)}{\tilde{\alpha}(\tilde{\alpha}-\tilde{\beta})(1-\tilde{\alpha})}\right].$$

Therefore, the signs of the derivative are

$$\frac{dW}{d\tilde{\alpha}} > 0 \quad \text{if } 0 < \tilde{\alpha} < A \text{ or if } \tilde{\alpha} > B$$
$$\frac{dW}{d\tilde{\alpha}} < 0 \quad \text{if } A < \tilde{\alpha} < B$$

where

$$A=\frac{\left(1+n_1+m\tilde{\beta}\right)-\sqrt{\left(1+n_1+m\tilde{\beta}\right)^2-4(m+1)n_1\tilde{\beta}}}{2(m+1)}$$

$$B=\frac{\left(1+n_1+m\tilde{\beta}\right)+\sqrt{\left(1+n_1+m\tilde{\beta}\right)^2-4(m+1)n_1\tilde{\beta}}}{2(m+1)}.$$ □

The relationship between a firm's willingness to invest in NS and the survival probability is depicted in Figure 1.

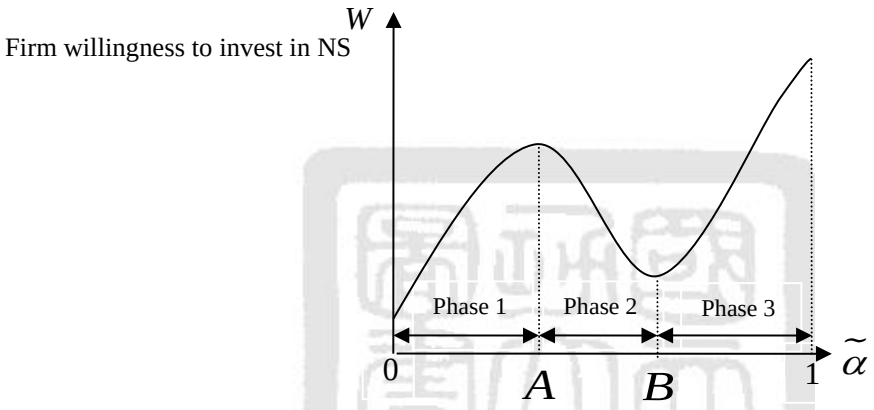

Figure 1. Firm willingness to invest in NS and survival probability

There are three phases for the relationship between firm willingness to invest in NS and survival probability. In Phase 1, the survival probability of a firm with NS-investment is low. This is because there is either no NS technology (or an ineffective technology), and few firms have invested in NS. Hacker attacks pose significant threats to network security. The marginal increase in $\tilde{\alpha}$ when an additional non-NS firm invests in NS is larger in the early stage than in the late stage due to the properties of NS externality, $f'(m)>0$ and $f''(m)<0$. This result is consistent with the weaker protection model in (Lelarge, 2009). This externality has a positive effect on the incentive of a firm to invest in NS, which in turn increases the incentives for non-NS firms to invest in NS because a greater share of total market profits is then available to them if they survive. This implies that an NS investment has the characteristic of a first mover advantage. Therefore, the willingness (*W*) to invest in NS increases along with the survival probability ($\tilde{\alpha}$)

with NS-investment.

In Phase 2, NS technology sophisticatedly develops the ability to counter most hacker attacks, and the survival probability of a firm with NS-investment increases. The relationship between the willingness to invest in NS and the survival probability with NS-investment reverses. The effectiveness of NS against online threats is not obvious, but the externality effect is large enough to encourage firms to choose to become free riders in NS. This spillover effect of externality thus drives down the incentive to make an NS investment. In short, when the externality effect is sufficiently large, the incentive to make an NS investment decreases, and firms are more likely to become free-riders. In this phase, the negative effect of NS investment (i.e., the externality effect) offsets the positive effect (i.e., surviving in the market). Therefore, relevant authorities should encourage firms to invest in NS by such measures as, for example, periodically publishing the status of current network threats and establishing NS regulations for on-line firms.[2]

Finally, in Phase 3, NS technology is mature enough to counter most threats, and the survival probability of a firm with NS-investment continuously increases. In this phase, NS investments can raise the probability that a firm will survive in the market, and thus the uncertainties associated with NS-investments become lower. Therefore, non-NS firms have a greater incentive to invest in NS since the survival probability of such investments is high, as is the related externality. Similarly, willingness to invest in NS increases along with the survival probability associated with NS-investment. These results are supported by Lelarge's (2009) epidemic risk model, in which firms' expected losses due to NS investments decrease due to the externalities of other firms' NS investments whenever network security is well developed.

A firm's willingness to invest in NS varies with the level of the survival probability with NS. When $n_1/m > \tilde{\alpha}$, a positive relationship between the survival

[2] Similarly, theISO/IEC 27001 was published by the International Organization for Standardization and the International Electrotechnical Commission.

probability with NS-investment and willingness holds. This condition implies that the actual survival ratio (i.e., the realized effectiveness of NS) is higher than the prior survival probability with NS-investment (i.e., the prior expected effectiveness). This would then increase the incentive for firms to invest in NS. Contrarily, the relationship reverses when the condition reverses.

Likewise, it can also be shown that the relationship between a firm's willingness to invest in NS and the survival probability without NS investment has a similar shape to that shown in Figure 1. In the model, the NS externality effects of NS firms and non-NS firms imply the isotonicity of the two survival probabilities with and without NS investment thus leading to the following corollary:

Corollary 1. When the probability of survival without NS is in the low range and when it is in the high range, the incentive of a firm to invest in NS increases with the non-NS survival probability. However, when the probability of survival without NS is in the medium range, the incentive of a firm to invest in NS decreases with the non-NS survival probability.

There is a positive influence of network externality on the incentive to invest in NS when the survival probability is at a relatively low or high level, independent of firm NS investment decisions. In addition, firm survival probability depends on the interaction between attacks and security, and thus developing a secure network environment that enables a higher survival probability against security incidents would be preferable. With a higher survival probability, the uncertainties related to NS-investment can be reduced, and NS technologies can be viewed as mature. This can be achieved by lowering the cost of NS implementation and by diffusing NS technology (Attewell, 1992; Walsh, 2003). However, when the survival probability is at the medium level, the influence of network externality on the incentive to invest in NS is negative, and the incentive to invest in NS is reduced for a firm if it anticipates that others will make these investments instead. This finding is in accordance with the results of Lelarge (2009), which showed that the decision made by all firms to remain unprotected may be a Nash equilibrium.

3.3 Interaction Strategy

The next proposition describes the impact of the number of NS firms on willingness to invest in NS.

Proposition 2. A firm's incentive to invest in NS increases with the number of NS firms whenever the ratio of prior non-survival probability with NS investment to that without NS investment is more than the ratio of the actual non-survival rate with NS investment to that without NS investment. Otherwise, a negative relationship holds.

Proof: Take the derivative of a firm's willingness to invest in NS with respect to the number of NS firms. Then

$$\frac{dW}{dm} = W\left[\ln(1-\tilde{\alpha}) - \ln(1-\tilde{\beta}) + \left(\frac{1}{m} + \frac{1}{m-1} + \cdots + \frac{1}{m-n_1+1}\right) - \left(\frac{1}{n-m-1} + \frac{1}{n-m-2} + \cdots + \frac{1}{n-m-n_2}\right)\right].$$

Note that $\frac{1}{n-m-1} + \frac{1}{n-m-2} + \cdots + \frac{1}{n-m-n_2} = \sum_{i=1}^{n_2} \frac{1}{n-m-i} = \sum_{i=1}^{n-m-1}\left(\frac{1}{i}\right) - \sum_{i=1}^{n-m-n_2-1}\left(\frac{1}{i}\right)$ is the difference of two Harmonic series $S(k) = \sum_{i=1}^{k}\left(\frac{1}{i}\right)$, where $k=n-m-1$ and $n-m-n_2-1$.

Hence, the derivative is

$$\frac{dW}{dm} = W\left\{\ln\frac{(1-\tilde{\alpha})}{(1-\tilde{\beta})} + \left[\sum_{i=1}^{m}\left(\frac{1}{i}\right) - \sum_{i=1}^{m-n_1}\left(\frac{1}{i}\right)\right] - \left[\sum_{i=1}^{n-m-1}\left(\frac{1}{i}\right) - \sum_{i=1}^{n-m-n_2-1}\left(\frac{1}{i}\right)\right]\right\}. \quad (1)$$

This leads to the Harmonic series $S(k) \approx \ln(k) + 0.5772156649$. Then

$$\sum_{i=1}^{m}\left(\frac{1}{i}\right) - \sum_{i=1}^{m-n_1}\left(\frac{1}{i}\right)$$
$$\cong \left[\ln(m) + 0.5772156649\right] - \left[\ln(m-n_1) + 0.5772156649\right]$$
$$\cong \ln\frac{(m)}{(m-n_1)},$$

and

$$\sum_{i=1}^{n-m-1}\left(\frac{1}{i}\right)-\sum_{i=1}^{n-m-n_2-1}\left(\frac{1}{i}\right)\cong\ln\frac{(n-m-1)}{(n-m-n_2-1)}.$$

The derivative in (1) can be rewritten as:

$$\frac{dW}{dm}\cong\ln\frac{(1-\tilde{\alpha})}{(1-\tilde{\beta})}+\ln\frac{m}{m-n_1}-\ln\frac{n-m-1}{n-m-n_2-1}$$
$$=\ln\frac{(1-\tilde{\alpha})}{(1-\tilde{\beta})}+\ln\frac{m(n-m-n_2-1)}{m-n_1(n-m-1)}.$$

Therefore, the relationship of the derivative's sign would be as follows:

$$\frac{dW}{dm}>0 \text{ if and only if } \frac{(1-\tilde{\alpha})}{(1-\tilde{\beta})}>\frac{1-(n_1/m)}{1-(n_2/n-m-1)}. \quad (2) \quad \square$$

Note that, on the right side of the inequality, the ratio of non-survival probability with NS investment to the one without NS investment is equivalent to the odds of NS investment. Thus, the equation in (2) implies that the willingness to invest in NS increases as the number of NS firms increases if and only if the prior ratio of non-survival probability with NS investment to non-NS investment is more than the actual prior ratio of non-survival probability with NS investment to non-NS investment.Proposition 2 can also be further interpreted as follows: The positive relationship between firm willingness to invest in NS and the number of NS firms holds whenever the prior probability of survival with NS (i.e., $\tilde{\alpha}$) is less than its actual survival rate (n_1/m), and the prior probability of survival without NS (i.e., $\tilde{\beta}$) is higher than its actual survival rate (n_2/n-m-1). When the NS technology is more effective,the announcing probability of survival and the survival rate for firms without NS is worse off than the expected one. The result could be explained by the fact that the suppliers of network security must consolidate their NS technological effectiveness to make it be worth firm investment in NS.

In addition, the researchis also interesting in regard to the effect of the number of surviving firms among NS or non- firms. Therefore, the relationship between a

firm's incentive to invest in NS and the number of surviving firms with and without NS is summarized in the following:

Proposition 3. The incentive to invest in NS decreases with the number of surviving NS firms when the probability of survival with NS is less than half. However, once the survival probability with NS-investment is greater than half, the relationship is still negative when $\ln(\tilde{\alpha}/1-\tilde{\alpha}) < 1/(1+n_1+n_2)$. Otherwise, the incentive to invest in NS increases with the number of surviving NS firms.

Proof: Take the derivative of the incentive to invest in NS with respect to the number of NS surviving firms. Then

$$\frac{dW}{dn_1} < 0 \text{ if } \tilde{\alpha}<0.5 \text{ and } \tilde{\alpha}>0.5 \text{ and } \ln\frac{\tilde{\alpha}}{(1-\tilde{\alpha})} < \frac{1}{(1+n_1+n_2)}$$

$$\frac{dW}{dn_1} > 0 \text{ if } \tilde{\alpha}>0.5 \text{ and } \ln\frac{\tilde{\alpha}}{(1-\tilde{\alpha})} > \frac{1}{(1+n_1+n_2)} \quad \square$$

It is shown that the relationship between the incentive to invest in NS and the number of surviving NS firms is negative if the probability of survival with NS is less than half. However, when the effectiveness of NS is sufficiently large, $\tilde{\alpha} > 0.5$, the relationship depends on the relative survival ratio and the inverse of the number of surviving firms.

The reason for this can be explained by the fact that when NS technology is mature enough to counter most threats, the natural logarithm of the relative survival ratio for an NS firm is more than the inverse of all surviving firms. In this circumstance, NS investments can raise the probability that a firm will survive in the market, and thus the uncertainties associated with such investments become lower. Therefore, non-NS firms have greater incentive to invest in NS since the survival probability related to such spending is high, as is the related externality. Similarly, the willingness to invest in NS increases along with the survival probability associated with NS investment. These results are supported by Lelarge's

(2009) epidemic risk model, in which firms' expected losses due to NS investments decrease due to the externalities of other firms' NS investments whenever network security is well developed.

However, when the number of surviving NS firms continuously increases, the odds ratio of the probability of survival of an NS firm is less than the inverse of all surviving firms. Moreover, when the effectiveness of NS is not clear, but the effects of externalities are adequately large, then this will encourage firms to become free riders with regard to security. The negative effects of NS investment (i.e., the effects of externalities) can thus offset the positive effects (i.e., survival in the market).

Likewise, it can also be shown that the relationship between a firm's incentive to invest in NS and the number of surviving non-NS firms, n_2, corresponds to the probability of survival without NS, leading to the following corollary:

Corollary 2. The incentive of a firm to invest in NS decreases along with the number of surviving non-NS firms when $\tilde{\beta} < 0.5$ or when $\tilde{\beta} > 0.5$ and $\ln\left(\tilde{\beta}/\left(1-\tilde{\beta}\right)\right) < 1/\left(1+n_1+n_2\right)$.

If the survival probability without NS-investment is not over half, the incentive of a firm to invest in NS will decrease along with the number of surviving non-NS firms. However, once the survival probability without NS-investment is greater than half, the incentive of a firm to invest in NS will increase along with the number of surviving non-NS firms except in the case where the natural logarithm of the odds ratio for a non-NS firm is less than the inverse of the number of surviving firms.

Proof: Take the derivative of the incentive to invest in NS with respect to the number of non-NS surviving firms. Then

$$\frac{dW}{dn_2} < 0 \text{ if } \begin{matrix}\tilde{\beta}<0.5 \\ \tilde{\beta}>0.5 \text{ and } \ln\dfrac{\tilde{\beta}}{(1-\tilde{\beta})} < \dfrac{1}{\left(1+n_1+n_2\right)}\end{matrix}$$

$$\frac{dW}{dn_2} > 0 \text{ if } \tilde{\beta}>0.5 \text{ and } \ln\frac{\tilde{\beta}}{(1-\tilde{\beta})} > \frac{1}{\left(1+n_1+n_2\right)}.$$

Proposition 3 and Corollary 2 state that the odds ratio is a key strategic parameter for NS and non-NS firms under the probability of survival with/without NS being larger than half. In addition, when the probability of survival with (without) NS is less than half, the number of surviving NS (non-NS) firms certainly has a negative effect on the incentive to invest in NS.

3.4 Market Size

The market size not only has influences on the level network effect, but also has intuitive influence on the market share through competition (Shankar &Bayus 2003; Desmet&Parente 2010). To the best of our knowledge, the competition between the prior probability of survival and actual survival rate is the first rigorous computation of this macro function from the parameters of a micro-model in the context of security. It allows an understanding of how the incentive to invest in NS is affected by effective security technology. The next proposition describes the relationship between a firm's incentive to invest in NS and market size. Here, there is an optimal market size, and this is influenced by the prior survival probability of non-NS firms.

Proposition 4: If the prior survival probability of non-NS firms is less than their actual survival rate, then market size has a positive effect on the incentive to invest in NS, and if not, it then has a negative influence. There is thus an optimal market size in a competitive market. Moreover, the relationship between the survival probability without NS and the market size is negative.

Proof: Take the derivative of a firm's willingness to invest in NS with respect to the market size. Then

$$\frac{dW}{dn} = W\left[\ln(1-\tilde{\beta}) + \left(\frac{1}{n-m-1} + \frac{1}{n-m-2} + \cdots + \frac{1}{n-m-n_2}\right)\right]$$

Note that $\frac{1}{n-m-1} + \frac{1}{n-m-2} + \cdots + \frac{1}{n-m-n_2} = \sum_{i=1}^{n_2} \frac{1}{n-m-i} = \sum_{i=1}^{n-m-1}\left(\frac{1}{i}\right) - \sum_{i=1}^{n-m-n_2-1}\left(\frac{1}{i}\right)$ is

the difference between two harmonic series $S(k)=\sum_{i=1}^{k}\left(\frac{1}{i}\right)$, where $k=n-m-1$ and $n-m-n_2-1$.

Hence, the derivative is

$$\frac{dW}{dn}=W\left\{\ln\left(1-\tilde{\beta}\right)-\left[\sum_{i=1}^{n-m-1}\left(\frac{1}{i}\right)-\sum_{i=1}^{n-m-n_2-1}\left(\frac{1}{i}\right)\right]\right\}.$$

These harmonic series $S(k)\approx\ln(k)+0.5772156649$. Then

$$\sum_{i=1}^{n-m-1}\left(\frac{1}{i}\right)-\sum_{i=1}^{n-m-n_2-1}\left(\frac{1}{i}\right)\cong\ln\frac{(n-m-1)}{(n-m-n_2-1)}.$$

The derivative in (1) can be rewritten as:

$$\frac{dW}{dn}=\ln\left(1-\tilde{\beta}\right)-\ln\frac{(n-m-1)}{(n-m-n_2-1)}.$$

Therefore, the relationship for the derivative's sign would be as follows:

$$\frac{dW}{dn}>0 \text{ if } \tilde{\beta}<\ln\frac{n_2}{(n-m-1)}$$
$$\frac{dW}{dn}<0 \text{ if } \tilde{\beta}>\ln\frac{n_2}{(n-m-1)}.$$

The second derivatives are

$$\frac{d^2W}{dn^2}=\frac{dW}{dn}[\bullet]+W\frac{d[\bullet]}{dn},$$
$$\text{where } [\bullet]=\left[\ln\left(1-\tilde{\beta}\right)-\ln\frac{(n-m-1)}{(n-m-n_2-1)}\right]$$

The second part of the second term, $d[\bullet]/dn$ is negative. If the two parts of the first term have the same sign, and the value of the first term is smaller than that of the second, then the graph of the incentive to invest in NS in response to the number of firms in the market is concave. Therefore, the second-order condition is satisfied

for incentive maximization. The optimal market size is $n^* = \frac{\tilde{\beta}m + \tilde{\beta} + n_2}{\tilde{\beta}}$.

If the prior survival probability of non-NS firms is less than their actual

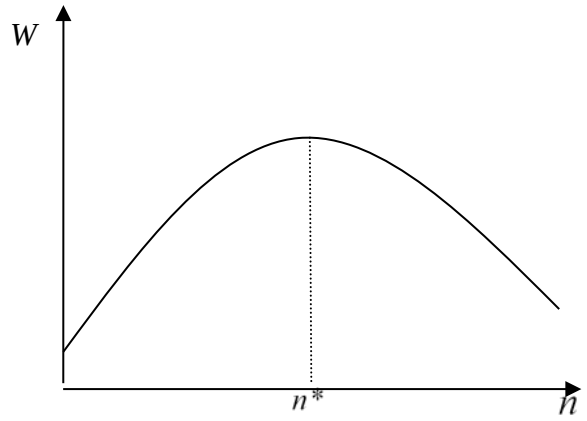

Figure 2.The willingnessto invest in NS with respect to *n*.

survival rate, new entrants wouldn't be likely to decrease the actual survival rate of any of these firms,unless all entrants invest in NS. With other things being equal, the non-NS firms are worse off. The need to compete with new entrants who did not invest in NS will increase the incentive to invest in NS among other firms. However, the prior survival probability of non-NS firms is larger than the actual survival rate, and a higher prior survival probability of non-NS firms will make these companies more willing to rely on luck for protection as more new entrants enter the market. If the number of firms exceeds the optimal amount, the incentive to invest in NS will fall, and this could be interpreted as firms deciding to share the risk as competition increases in the market. Once there are fewer firms in the market, then this may increase the probability of a specific firm being attacked and thus increase the incentive to invest in NS. The derivative of the optimal number function with respect to the probability of survival without NS is $dn^*/d\tilde{\beta} = -n_2/\tilde{\beta}^2 < 0$. This implies the probability of survival without NS negatively influences the optimal market size. Specifically, the higher negligibility of network security to the firms is, the less competitive this market becomes, leading to imperfect competition. In contrast, when network security is mandatory to firms, the market will become perfectly competitive.

Chapter Four

Conclusions, Discussion, and Future Research

Investments in network security are indispensable, although generally expensive, for all firms that sell products in both physical stores and online. Network externality in this research refers to one firm's choices made by other firms' influence resulting from investments in security.

4.1 Summary

In this research, the incentive of a firm to invest in network security is first formulated. According to maximization of the market share benefit, a firm's incentive for investment in network security is derived from the expected profits of that firm. Next, by algebraic calculation, the relationship between the influences, such as the prior probability of survival or the number of NS-investing firms, onmarket size will be explicit. Finally, the conclusions of this work and its managerial implications are offered to companies and relevant institutions, with the purpose being to promote a better NS environment.

4.2 Conclusions

This researchwas aimed at assessing the importance of network externalities and exploring how to secure a network through an incentive mechanism. However, such investments are generally expensive. Firms adopt network security to assure their anticipative profit, and so it is necessary to examine these investment strategies.

In sum, the risk is high since it is difficult for a firm without NS to survive when an attack takes place when few firms have invested in NS. The incentive for NS-investment increases along with survival probability due to a bigger share of profits. In such cases, security investments have the characteristic of first-move

advantage,but the incentive of NS-investment also increases when the survival probability with NS-investment is high. When the technology effectiveness of NS against the threats is indeterminate, the relationship between the survival probability and willingness becomes negative because the spillover effect of NS externality decreases the incentive for NS investment. The consequences could be a response to a result indicating the effects of network externalities are too significant under conditions with the same surviving firms and number of firms with NS investment, then some firms will choose to be free-riders. This finding is in accordance with the results in Lelarge (2009), which show that the decision made by all firms to remain unprotected may be a Nash equilibrium. Hence, moderate facilitations should be made by relevant authorities to encourage firm investment in NS. For example, they could periodically publish the status of current network threats and construct essential NS regulations for on-line firms.

The results indicate that the number of NS-investing firms has a positive influence on the incentive for investment in NS when the ratio of prior non-survival probability with NS-investment to that without NS-investment is more than the ratio of the actual non-survival rate of firms with NS-investment to those without NS-investment. Moreover, some ratiocination can be obtained from the model analysis results. First, if the externality to the firms with NS-investment is actually stronger than it is for those without, then a firm will have more incentive to invest in NS. Once the network externality of firms without NS-investment is more significant than it is for those with NS-investment, then firms who did invest in NS will begin to leave the group of firms with NS-investment. The consequences could be a response to results in phase 2 from proposition 1. Second, if the prior survival probability with NS-investment is over-rated, or the prior survival probability without NS-investment is overshot,in truth, the relationship tends to be negative. However, if the prior survival probability with and without NS-investment is over-rated, the relationship tends to be positive. Third, the willingness for NS-investment will diminish with more sharing by surviving firms in the market.

With regard to the number of surviving firms both with and without NS, the

incentive to invest will decrease when the NS risk is shared by more surviving firms. However, once the probability of survival with NS investment is greater than half, the incentive to invest will increase except when the natural logarithm of the relative survival ratio is less than the inverse of all surviving firms. This may be because network threats are transferred from firms that invest in NS to those that do not. The relationship between the optimal level of investment and the level of potential profit found in this work is consistent with the finding of Cavusoglu et al. (2004b) suggesting that the more dependent a firm is on a network, the more significant the consequences of an attack will be on its financial health. The results suggest that the authorities in charge of NS should encourage firms not only to invest in NS, but also in R&D related to NS technology.

It is important to consider the level of competition in the market. If the prior probability of survival of non-NS firms is less than their survival rate, then a greater market size will have a positive impact on the incentive to engage in NS investments. If the prior survival probability of non-NS firms is less than their survival rate, new market entrants will decrease the likely survival rate of non-NS firms unless all of them invest in NS. In order to compete with new entrants, firms that previously did not invest in NS will have a greater incentive to do so. Once there is more than the optimal number of firms in a market, the incentive to engage in an NS investment will be less. One reason for this may be that when the prior probability of survival of non-NS firms is greater than the actual survival rate, the higher prior probability of survival of non-NS firms will lead more firms to rely on luck with regard to NS as more companies enter the market.

4.3Discussion

Based on the results of this research, a positive influence exists between network externality and the incentive to invest in NS. A possible explanation for this might be the higher expected marginal benefit from NS-investment in the earlier stage. The reason could be viewed as first-mover advantages (Ross Anderson, 2001;

Ross Anderson, 2002; Shostack, 2005) and could increase the incentive for NS-investment to improve survival probability in order to increase profit sharing. This highlights the importance of innovation in NS technology and in management for on-line firms. Another possible explanation for this is that the uncertainty of NS-investment is low in the earlier stage. This is similar to economies of scale in NS-investment, regardless of whether it is due to the cost of implementation or the diffusion of security technologies (Attewell, 1992; Walsh, 2003). This means that the quality of NS technologies is good.

However, network externalities could still have negative effects in some situations that are caused by firms believing in luck. The incentive to invest in NS is possibly diminished if a firm anticipates other firms will invest in protective network security measures. This finding is in agreement with those of Lelarge, 2009, who showed that the decisions by all agents of firms to remain unprotected may be a Nash equilibrium. However, in contrast to the prisoner's dilemma problem, there may also be a Nash equilibrium where some or all firms will have high incentive to protect network security. The challenge is to provide an incentive-compatible mechanism to convince each of the firms' security manager agents that it is in their best interest to invest in security (Kunreuther & Heal, 2003).

Hence, the overall effect of network externality on the NS investment incentivesdepends on the trade-off between the effects on NS firms and non-NS firms. If the negative effect is more significant than the positive effect, then firms who did invest in NS will begin to leave the group of NS-investing firms. The consequences will be in accordance with ab outcome in whichsome firms choose to be free-riders (Kunreuther & Heal, 2003) and further correlate with the strong protection of the epidemic risk model (Lelarge, 2009).

The contribution of this study is that it incorporates endogenous network externality in firm decisions to make NS investments, and it investigates how network externality influences the optimal strategy of competing online firms to invest in NS in the face of security threats. Many studies on NS investment

(Anderson, 2001; Bojanc&Jerman-Blažič, 2008a, 2008b; H. Cavusoglu et al., 2004b) have ignored the existence of network externality although it is an essential characteristic of NS. Further, some studies that do consider network externality simply have assumed a constant potential loss related to a successful attack, and thus the effectiveness of NS technology cannot be measured (Bolot&Lelarge, 2009; Lelarge, 2009; Lelarge&Bolot, 2008; Yue et al., 2007), while others have completely ignored the strategic interactions among agents in the decision to make NS investments (Jiang et al., 2008a).

The results derived in this research provide some managerial policy implications. In the research, the prior effectiveness of NS technology and the number of NS firms are found to positively affect the incentive of firms to invest in NS. In a security breach incident, firms do not have any legal responsibility except for the violation of the personal information act. Hence, the penalties on firmsfor such personal information violations should be increased, so they are forced to endogenize the possible losses due to security breaches and to increase investment in NS. On thepositive side, the NS investment of firms should be further encouraged by governments via various channels including subsidies and tax deductions. Next, generous governmental subsidies and tax deductions can also be granted to the vendors of anti-virus products and services. By doing so, the profitability within the market would potentially attract more vendors to enter the market, and the competitiveness would cause vendors to invest more resources in research and development. Thus, the effectiveness of NS technology is promoted, and the incentive of firms to invest in NS increases.

4.4 Future Research

The critical e-commerce success factors vary with the scale of enterprises due to different levels of difficultyrelated toreaching targeted consumers (Chappell & Feindt, 1999). In this research, a conceptual and operational model that simultaneously considers network externalities and demonstrates the influences on

incentive was presented. This research was intended to investigate how an optimal NS strategy is affected by network externalities. Since preventive NS is adopted by firms to assure increased profit in the long-term, simultaneous analysis is necessary to examine the network externality for each circumstance which changes with the numberof firms investing in NS. This type of analysis provides insight into how e-commerce market participants manage NS strategy and what the role of NS investments is under conditions of both uncertainty and externality.

There are a few possible directions for future research. In the current research, the number of firms in the market is exogenously fixed, but more firms in the market imply a more intense level of competitiveness, which in turn reduces the profitability of firm survival. Therefore, it would be of interest to relax the assumption of a fixed number of firms in the market and investigate whether market competitiveness negatively influences the incentive to invest in NS. In this research, the interaction of firm investment of NE in a one-shot game under network externality was the goal of the analysis. In other words, hackers are not viewed as players in this game. Namely, hacker behavior is exogenously assumed. The threat of hackers is illustrated by the vulnerability of the system that is the opposite of the self-protection rate of the security system against attacks and security incidents. To model hackers as evolving and learning players in the model can serve as a direction of future research to measure the impact of hacker behavior on firm network security.

Finally, it would also be of interest to empirically examine the factors which influence online firms' actual NS investment behavior, as this has received little attention in the literature. Cavusoglu, Mishra, and Raghunathan (2004a) empirically demonstrated the significant impact of security breaches on the market values of breached firms in the US and found that these firms lost an average of 2.1% of their market value (equivalent to US$1.65 billion per breach) within two days of the announcement. Tanaka, Matsuura, and Sudoh (2005) also derived a concave relationship between the security investments of e-local governments in Japan and network vulnerability. In a future empirical study, the data for firm profits and NS

investments could be retrieved from the annual reports and the surveys released from the related market research institutes, such as the Market Intelligence Center (MIC) and the Computer Security Institute (CSI). The percentage of detected security incidents over actual network traffic and the weighted number of viruses announced by anti-virus venders, such as Avira Antivir, Symantec and Trend, could be used as proxies for the prior effectiveness of NS technology and threat probability, respectively.

References

Anderson, R. (2001). *Why Information Security is Hard-An Economic Perspective*. Paper presented at the Proceedings of the 17th Annual Computer Security Applications Conference.

Anderson, R. (2002). *Maybe we spend too much? Unsettling Parallels Between Security and the Environment*. Retrieved from http://www.cl.cam.ac.uk/~rja14/econws/37.txt.

Attewell, P. (1992). Technology Diffusion and Organizational Learning - the Case of Business Computing. *Organization Science, 3*(1), 1-19.

August, T., & Tunca, T. I. (2006). Network software security and user incentives. *Management Science, 52*(11), 1703-1720. doi: DOI 10.1287/mnsc.1060.0568

Bayuk, J. L. (2001). Security metrics: How to justify security dollars and what to spend them on. *Computer security journal, 17*(1), 1-12

Bojanc, R., & Jerman-Blažič, B. (2008a). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413-422. doi: 10.1016/j.ijinfomgt.2008.02.002

Bojanc, R., & Jerman-Blažič, B. (2008b). Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces, 30*(4), 216-222. doi: 10.1016/j.csi.2007.10.013

Bollier, D. (1996). *The future of electronic commerce: a report of the fourth annual Aspen Institute Roundtable on Information Technology*. Washington, D.C.: Aspen Institute.

Bolot, J., & Lelarge, M. (2009). Cyber Insurance as an Incentivefor Internet Security. 269-290. doi: 10.1007/978-0-387-09762-6_13

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the Acm, 47*(7), 87-92.

Chappell, C., & Feindt, S. (1999). *Analysis of E-commerce practice in SMEs*.

Coppel, J. (2000). *E-commerce: Impacts and Policy Challenges*: OECD.

Dynes, S., Johnson, M. E., Andrijcic, E., & Horowitz, B. (2007). Economic costs of firm-level information infrastructure failures: Estimates from field studies in manufacturing supply chains. *The International Journal of Logistics Management, 18*(3), 420-442. doi: 10.1108/09574090710835147

Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research, 16*(2), 186-208. doi: 10.1287/isre.1050.0053

Garcia, A., & Horowitz, B. (2007). The potential for underinvestment in internet security: implications for regulatory policy. *Journal of Regulatory Economics, 31*(1), 37-55. doi: 10.1007/s11149-006-9011-y

CompTIA, 2007. Information security spending on the rise. http://www.comptia.org/home.aspx

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Trans. Inf. Syst. Secur., 5*(4), 438-457. doi: 10.1145/581271.581274

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers, 8*(5), 338-349. doi: 10.1007/s10796-006-9011-6

Hoo, K. J. S. (2000). *How Much is Enough? A Risk Management Approach to Computer Security*: Stanford University.

Huang, C. D., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics, 114*(2), 793-804. doi: DOI 10.1016/j.ijpe.2008.04.002

Iheagwara, C., Blyth, A., Kevin, T., & Kinn, D. (2004). Cost effective management frameworks: the impact of IDS deployment technique on threat mitigation. *Information and Software Technology, 46*(10), 651-664. doi: 10.1016/j.infsof.2003.11.004

Iheagwara, C., Arthur, S. & Acar, Y. (2005). The Different Metrics of ROI: Implications for Information Assurance, www.isaca -washdc.org/pages/articles/article-nov2005-print.htm

Jean Camp, L., & Wolfram, C. (2004). Pricing SecurityEconomics of Information Security. In L. Camp & S. Lewis (Eds.), (Vol. 12, pp. 17-34): Springer US.

Jiang, L., Anantharam, V., & Walrand, J. (2008a). *Efficiency of selfish investments in network security*. Paper presented at the Proceedings of the 3rd international workshop on Economics of networked systems, Seattle, WA, USA.

Jiang, L., Anantharam, V., & Walrand, J. (2008b). How Bad are Selfish Investments in

Network Security? : EECS Department, University of California, Berkeley.

Kumar, R., Park, S., & Subramaniam, C. (2008). Understanding the Value of Countermeasure Portfolios in Information Systems Security. *J. Manage. Inf. Syst., 25*(2), 241-280. doi: 10.2753/mis0742-1222250210

Kunreuther, H., & Heal, G. (2003). Interdependent Security. *Journal of Risk and Uncertainty, 26*(2), 231-249. doi: 10.1023/a:1024119208153

Lelarge, M. (2009). *Economics of malware: epidemic risks model, network externalities and incentives*. Paper presented at the Proceedings of the 47th annual Allerton conference on Communication, control, and computing, Monticello, Illinois, USA.

Liu, P., Zang, W., & Yu, M. (2005). Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Trans. Inf. Syst. Secur., 8*(1), 78-118. doi: 10.1145/1053283.1053288

Ogut, H., Menon, N., & Raghunathan, S. (2005). *Cyber Insurance and IT Security Investment: Impact of Interdependent Risk*. Paper presented at the 4th Workshop on the Economics of Information Security, Cambridge, MA, USA.

Passionate Project Management, 2013. . Retrieved from http://www.passionatepm.com/.

Powell, B. (2005). Is Cybersecurity a Public Good? Evidence from the Financial Services Industry. *Journal of Law, Economics and Policy, 1*, 497-510.

Purser, S. A. (2004). Improving the ROI of the security management process. *Computers & Security, 23*(7), 542-546. doi: 10.1016/j.cose.2004.09.004

Richardson, R. (2008). CSI Computer Crime & Security Survey *This is the 13th year of the survey*: Computer Security Institute

Rowe, B., & Gallaher, M. P. (2006). Could IPv6 improve network security? And, if so, at what cost? *Cybersecurity. I/S: A Journal of Law and Policy for the Information Society, 2*(2), 231-267.

Schechter, S. E., & Smith, M. D. (2003). *How Much Security Is Enough to Stop a Thief?: The Economics of Outsider Theft via Computer Systems and Networks*. Paper presented at the Financial Cryptography. http://dblp.uni-trier.de/db/conf/fc/fc2003.html#SchechterS03

Shostack, A. (2005). *Avoiding Liability: An Alternative Route to More Secure Products*. Paper presented at the Fourth Workshop on the Economics of Information Security, Cambridge, MA. http://infosecon.net/workshop/pdf/44.pdf

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security.

Computers & Security, 24(2), 105-108. doi: 10.1016/j.cose.2005.02.001

U.S. Census Bureau, E-Stats (Washington, D.C.: 2010), available online athttp://www.census.gov/econ/estats/2008/2008reportfinal.pdf.

van Kessel, P. (2009). *Outpacing Change12th Annual Global Information Security Survey*: Ernst & Young.

Varian, H. (2004). System reliability and free riding. In L. J. Camp & S. Lewis (Eds.), *Economics Of Information Security*. New York Springer: Kluwer Academic Publishers.

Walsh, K. R. (2003). Analyzing the application ASP concept. *Communications of the Acm, 46*(8), 103-107. doi: 10.1145/859670.859677

Wang, Y. Z., Yu, M., Li, J. Y., Meng, K., Lin, C., & Cheng, X. Q. (2012). Stochastic game net and applications in security analysis for enterprise network. *International Journal of Information Security, 11*(1), 41-52. doi: DOI 10.1007/s10207-011-0148-z

Wang, Z. & Song, H. (2008). Towards an Optimal Information Security Investment Strategy. In Book Towards an Optimal Information Security Investment Strategy. Security, L.J. Camp and S. Lewis (eds.), Kluwer Academic Publishers, New York Springer.

Warrington, T. B., Abgrab, N. j., & Caldwell, H. M. (2000). Building trust to develop competitive advantage in e-business relationships. *Competitiveness Review, 10*(2), 160-168. doi: 10.1108/eb046409

Yue, W. T., Cakanyildirim, M., Ryu, Y. U., & Liu, D. (2007). Network externalities, layered protection and IT security risk management. *Decision Support Systems, 44*(1), 1-16. doi: DOI 10.1016/j.dss.2006.08.009