The Dissertation Committee for Xia Zhao Certifies that this is the approved version of the following dissertation:

Economic Analysis on Information Security and Risk Management

Committee:

Andrew B. Whinston, Supervisor

Anant Balakrishnan

John Mote

Jennifer Huang

Vitaly Shmatikov

Economic Analysis on Information Security and Risk Management

by

Xia Zhao, M.S.; B.S.

Dissertation

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Doctor of Philosophy

The University of Texas at Austin

August 2007

Acknowledgements

I would like to thank my advisor, Dr. Andrew B. Whinston, for his support and guidance throughout my dissertation work.

Economic Analysis on Information Security and Risk Management

Publication No._____

Xia Zhao, Ph.D.

The University of Texas at Austin, 2007

Supervisor: Andrew B. Whinston

This dissertation consists of three essays that explore economic issues on information security and risk management. In the first essay, we develop an economic mechanism which coordinates security strategies of Service Providers (SPs). SPs are best positioned to safeguard the Internet. However, they generally do not have incentives to take such a responsibility in the distributed computing environment. The proposed certification mechanism induces SPs to voluntarily accept the liability of Internet security. SPs who take the liability signal their capability in conducting secure computing and benefit from such recognition. We use a game-theoretic model to examine SPs' incentives and the social welfare. Our results show that the certification mechanism can generate a more secure Internet communication environment.

The second essay studies the impact of cyberinsurance and alternative risk management solutions on firms' information security strategies. In the existing literature, cyberinsurance has been proposed as a solution to transfer information risks and reduce security spending. However, we show that cyberinsurance by itself is deficient in addressing the overinvestment issue. We find that the joint use of cyberinsurance and risk

pooling arrangement optimizes firms' security investment. In the case with a large number of firms, we show that firms will invest at the socially optimal level.

The third essay examines the information role of vendors' patching strategies. Patching after software release has become an important stage in the software development cycle. In the presence of quality uncertainty, we show that vendors can leverage the patch release times to signal the quality of their software products. We define a new belief profile and identify two types of separating equilibria in a dynamic setting.

Table of Contents

Chapter 1: Introduction

Information security and risk management have drawn increasing attention due to the recent explosions of viruses, worms, Distributed Denial of Services (DDoS) attacks, phishing, pharming and other malicious activities. The economics of information security and risk management has recently become a thriving and fast-moving research area. It has been recognized that information security problems can be understood in terms of economic concepts. Economic solutions in addition to technology innovations are able to address various security issues. In this dissertation, we use the tools and concepts of game theory and microeconomic theory to examine different security issues.

The growing proliferation of malware is raising doubts about the Internet's future. Security has become a priority investment in public and private organizations; security technologies are being continually refined and more and more information security personnel hired. Nevertheless, the attacks and malicious activities in general are still rising in scope and viciousness in a global scale. An important reason is that SPs who are best positioned to safeguard the Internet lack incentives to take the responsibility for security. In Chapter 2, we propose a certification mechanism to induce SPs to voluntarily accept the liability for security. By taking the liability, SPs can signal their capability in conducting secure network communications and benefit from such recognition. We use a game-theoretic model to examine SPs' incentive and the social welfare. We show that the proposed mechanism can improve Internet security. This study provides economic rationale for reengineering the organizational structure of the Internet.

Recently the security-related spending is growing fast at the corporate level. Existing literature on security investment has primarily focused on the issue of underinvestment, while the issue of overinvestment in security has not been sufficiently

studied. In Chapter 3, we discuss multiple causes of security overinvestment and explore how firms can adopt risk management solutions to optimize their security spending. We show that risk pooling arrangement (RPA) can outperform a mature cyberinsurance market in addressing overinvestment issue. The key insight is that firms can leverage the moral hazard associated with RPA, known as the *moral hazard in team*, to mitigate the overinvestment incentive and destructive competition. Moreover, we illustrate that firms benefit by adopting both RPA and commercial cyberinsurance. In the case with a large number of firms, the joint use of RPA and commercial insurance induces firms to invest at the socially optimal level. This research generates important managerial implications regarding security risk management and policy implications regarding the development of mutual insurance for cybersecurity.

Software vulnerabilities or flaws are an important reason for security breaches. Patching after software release has become an integrated stage in the software development cycle. As information asymmetry exists in the software market, the strategic aspects of vendors' patching decisions need to be studies. In chapter 3, we investigate the information role of vendors' patching strategies. In the presence of quality uncertainty, we show that vendors can leverage the patch release time to signal the quality of their software products. In a dynamic setting, we define a new belief profile and identify two types of separating equilibria. The study deepens the understanding on strategic aspects of vendors patching policy.

Chapter 2: An Economic Mechanism for Better Internet Security

2.1 INTRODUCTION

Security problems, including spam and malware, plague the Internet to the point of distracting from productive use of the network. Technology is waging an admirable battle against these problems, but its solutions may not be sufficient by themselves to provide adequately secure environments. Fundamental issues with the design and interconnection policies of the Internet infrastructure contribute to the vulnerability to generation and dissemination of new attacks. Instead of relying exclusively on technology solutions in the context of the current policy framework, we consider the implication of a possible altered framework that could relate interconnection to security. Policy changes, rather than protocol changes, are considered.

The Internet can be viewed as an economic system besides being a technology-based environment. Such a view focuses attention on the interdependence and incentives of participating economic agents, who include service providers, users, and purveyors of malware and spam. It has been recognized that Internet security problems can be understood in terms of economic concepts, such as externality, liability, and moral hazard (Varian, 2000; Kunreuther and Heal, 2003; Lichtman and Posner 2004; Anderson and Moore 2006). While this is a useful insight, we need to go further and explore whether economic concepts can help us frame a pragmatic proposal to alleviate security problems by influencing some of the economic factors that govern the actions and interdependence of the participants. Such a proposal may also draw from public policy and law which have also dealt with the need to control socially harmful actions by some of the members of various communities.

In our proposal we recognize certain features of the Internet. As distinct from the legal approach to controlling crime, the information infrastructure has no clear delineation of jurisdiction, or corresponding enforcement powers. To illustrate by an analogy, with traditional criminal behavior such as bank theft, there are national laws that govern this behavior and associated police actions. Assigning the liability to the perpetrators and expecting the police to apprehend them are considered reasonable ways to reduce crime. Prosecution of a crime is focused on the perpetrator, precisely because the scope of jurisdiction, and the powers of investigation, enforcement, verification and punishment are well defined and can be vested into formal institutions and policies. With the Internet, the analogy is to view the crackers as the liable entity to be apprehended and punished. The analogy breaks down since the cracker could be in a foreign jurisdiction that does not recognize the laws of the country that suffered the attack of the crackers. Of course, this assumes that the crackers could be identified which could be impossible.

The natural assignment of liability to the perpetrators is not a practical way of looking at the Internet security problem. Instead we propose to consider the service provider (SP) as the entity to assume liability for the actions of its customers. Service providers are businesses or organizations who provide Internet access and related services to their customers or users, such as Yahoo!, AOL, universities, government agencies and large companies. Since the SP itself does not carry out any attack, but only transports traffic from customers some of who may be crackers, it appears unreasonable to place blame on SPs. It is common practice for public policy and law to make allowances for aspects of practical deployment of enforcement policies while formulating them. Accordingly, it may be seen that controls are sometimes applied at those nodes in organizational or community hierarchies which have the highest ability to influence the targeted criminal activity.

It would also be reasonable to assume that SPs would not voluntarily accept such a status since they would not accept a liability for a criminal action that they did not commit. Thus we need to show that a case can be made for SPs to voluntarily accept liability. In other words, we need to show that SPs may find it in their interest to subscribe to a framework that makes them responsible for security problems initiated by their customers. We denote the SPs that subscribe to the proposed policy framework as being "certified".

To induce a SP to accept liability and thus to become certified, we propose that all of the certified SPs' traffic once identified be carried to other certified SP without any additional reduction in performance for inbound filtering. In contrast, traffic from a non-certified SP may be blocked or significantly slowed down by certified SPs for carefully screening. Thus customers of a certified SP would obtain better service quality compared with customers of a non-certified SP and should be willing to pay a higher price for the service. However, the value to customers of a certified SP depends, in general, on how many other SPs decide to become certified. Since certification brings with it the liability obligation, a SP has both the issue of how many other SPs, it believes, will choose certification and how capable it is in monitoring and detecting possible traffic from its customers that could result in costly penalties. The latter decision is a one based on private information that the SP possesses but the former information is a guess or a conjecture.

This is especially complex since each SP is facing the same conjectural decision and the result could easily lead to inconsistent results where SPs make conjectures about the composition of the certified group which turns out to be incorrect. Is there a possibility of a solution where the conjecture or expectation of the SP are consistent and creates a subset of SPs that form a certified group and thus a viable and more secure

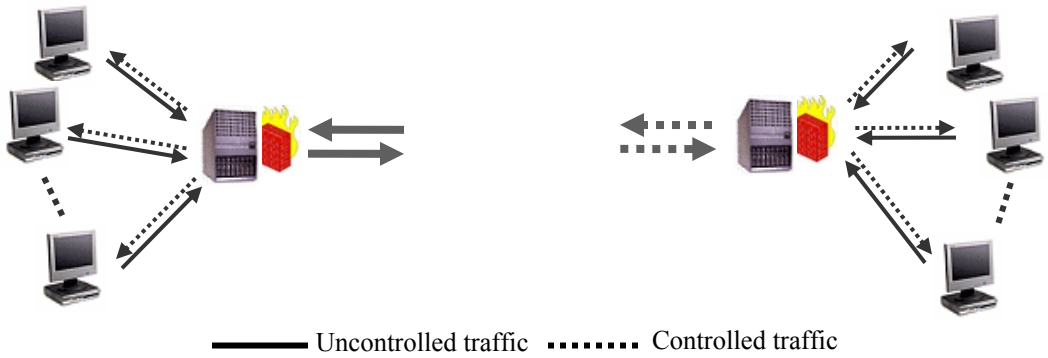
environment within the Internet? It is possible but this depends on the number of capable SPs and the number of users who could financially appreciate the benefits of a more secure Internet environment. So the challenge of voluntarily creating a collection of certified SPs with their associated customers is in the end an empirical issue. That is, we need to validate the conceptual framework by conducting experimental investigations into whether certification can attain sufficient critical mass to generate significant improvements for the certified providers and their customers, and that such gains are not offset by partial degradation of connectivity to the non-certified environment.

To summarize, our approach is to assign liability to those SPs who in turn voluntarily accept it. For a SP that has accepted responsibility there is a strong incentive to monitor and also to write contracts with customers that hold them responsible both financially and possibly in term of reputation. Even without explicit liability, the approach induces that SPs monitor the behavior of their computing environments to ensure that it is not used explicitly or otherwise to cause damage.

2.1.1 Security Practices

Before investigating SPs' incentives to accept the liability for security, we need to examine SPs' choices of security practices. We classify technologies and methods for SPs to control security into two categories, regulative practices and protective practices.

We refer to the set of technologies and methods for SPs to minimize the possibility of sending out malicious traffic as *regulative practices*, for example, the technologies used to monitor users and filter outgoing traffic. We refer to the set of technologies and methods for SPs to minimize the possibility of receiving malicious traffic as *protective practices*, for example, the technologies used to filter incoming traffic. Figure 2.1 demonstrates the impact of protective and regulative practices on Internet traffic.



(a) Protective practices (b) Regulative practices

Figure 2.1 Internet Traffic with Protective Practices vs. Regulative Practices

Regulative practices are more effective/efficient[1] than protective practices for three reasons. First, it is easier for SPs to perform regulative practices than protective practices because of information advantages. SPs have direct relationship with their customers and are able to acquire more information about their customers. For example, a SP can monitor its customers and analyze abnormal communication patterns to identify malicious users. It can contact customers to detect third-party hacking. In contrast, it is very difficult for SPs to determine malicious traffic originating from other networks. Second, SPs have administrative powers. They can slow down a connection, quarantine zombie computers, or directly disconnect crackers, spammers or phishers. Finally, regulative practices alleviate network congestion by dropping malicious traffic before it passes through the Internet.

[1] In this paper, we use both effectiveness and efficiency to characterize security practices. Effectiveness represents the probability/ability of security practices to successfully identify malicious activities. Efficiency represents the investment/cost of security practices. Thus, "A is more effective than B" means that A can identify malicious activities with a higher probability than B if the same amount of money is invested in A and B. "A is more efficient than B" means that less investment is needed by A than B in order to achieve the same level of effectiveness. In essence, they are equivalent.

2.1.2 Certification Mechanism

Currently, not all SPs are willing to deploy regulative practices to examine the traffic they are forwarding. SPs either assume no responsibility and hence take no security action or only deploy protective practices to improve local security. By assigning liability, our certification mechanism can induce the deployment of regulative practices within the certified network to improve overall Internet security.

The certification mechanism includes three kinds of players, the certification provider, SPs and customers. They interact in two stages as follows.

In the first stage—the subscription stage

- The certification provider determines a subscription fee for certification services;
- SPs voluntarily subscribe to certification services;
- The certification provider issues certificates to subscribed SPs and maintains a list of certified SPs.

In the second stage—the communication stage

- SPs invest in security practices, determine customers' Internet access fees and initiate network services;
- Certified SPs are required to compensate other certified SPs for damage caused by malicious traffic originating from their networks;
- Certified SPs are required to compensate their own customers for damage caused by malicious traffic regardless of its source.

Certificates serve as informative signals in this mechanism. Certification status of a SP is publicly observable. For example, the certification provider maintains a list of certified SPs. Customers can learn a SP's commitment and capability by observing whether it is on the list. However, only certified SPs can read the certificates and

accurately distinguish whether the traffic comes from a certified SP or a non-certified SP in the communication process. Put it differently, even though all SPs know the certification status of other SPs, only certified SPs can verify the source of inbound traffic by implementing the certification technology. Non-certified SPs may identify the source of the traffic by commonly available source IP address information in packets. However, they cannot prove the origin or guarantee its accuracy. Certification technologies must guarantee authentication and non-repudiation. That is, certified SPs are confident of identifying the source of the traffic; and certified SPs cannot deny the traffic that they send out or claim receiving traffic that they have never received. Candidate technologies which fulfill these characteristics of certification include digital signatures. The network with the certification mechanism is demonstrated in Figure 2.2.

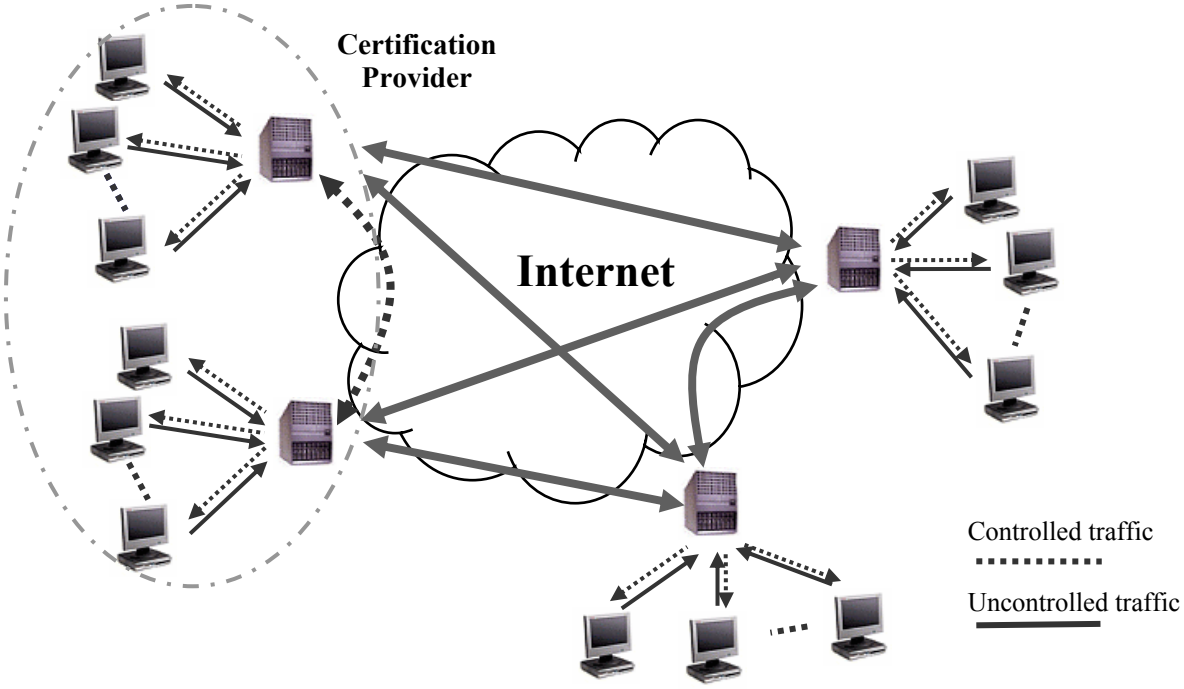


Figure 2.2 The Network with the Certification Mechanism

The certification provider plays a significant role in controlling Internet security in our mechanism. It motivates all certified SPs to watch the traffic sent to the Internet. It moderates and arbitrates disputes among SPs about the occurrence of security breaches and the subsequent compensation. In addition, the certified provider can share breach information among certified SPs, helping them prevent new breaches. For example, once compensation is transferred between certified SPs, the certified provider will solicit the detailed breach information and publicize it within the "certified network".

We use a game-theoretic model to examine SPs' incentive and evaluate the efficiency of the certification mechanism. In addition to the traditional screening and signaling mechanism, our model also incorporates network externality which is an important feature of Internet communications. In traditional screening and signaling games, choices by players generally depend only on their own inherent characteristics. In our model, a SP's choice depends not only on its own characteristics but also the expected choices of other SPs. For example, when a SP decides whether to subscribe to certification services, it will also consider other SPs' expected subscription decisions, i.e., the expected numbers of SPs in the certified network and the non-certified network. As a result, when the certification provider makes the decision on separating SPs, it should consider the interdependency among SPs' decisions.

The organization of this chapter is as follows. In Section 2.2, we review recent literature on information security. In Section 2.3, we outline a game-theoretic model and derive important conditions. In Section 2.4, we analyze strategies of various players and derive equilibria. Section 2.5 examines the efficiency (i.e. system surplus) of the proposed mechanism. Section 2.6 concludes the chapter with a discussion of implementation issues.

2.2 LITERATURE REVIEW

As information security has been extensively studied from a technological perspective, there is an emerging body of literature exploring security issues from an economic perspective. Anderson and Moore (2006) indicate that incentive misalignment significantly undermines information security and emphasize that incentives should be considered in security design. Varian (2000) also points out that besides identifying weak points and indicating who might be in position to fix them, a security analysis should further examine incentives of those who are responsible for security. Liability should be assigned to those who are best positioned to improve security. Lichtman and Posner (2004) propose that holding ISPs liable or partially liable can help improve the efficiency of security protection[2]. Parameswaran et al. (2007) specifically point out that SPs who provide direct Internet access to end users should protect their users and safeguard the overall network. This paper shares the view that SPs should be responsible for security and introduces incentives for them to achieve this goal.

This paper also connects to research exploring the optimal security investment. Gordon and Loeb (2002) develop an economic model to study the optimal investment in information security. Huang et al. (2006) further extend Gordon and Loeb's paper (2002) and consider a security threat scenario where attacks from multiple agents occur simultaneously. Cavusoglu et al. (2004b) use a game-theoretical model to analyze the impact of IT security investment on manual monitoring, firewall and IDS configurations considering the difference in costs. All these papers ignore the interdependency between individuals and organizations on the Internet and take a firm' risks as exogenously given.

The Internet risks and the incidents of security breaches are highly interdependent due to the global connectivity of the Internet. Kunreuther and Heal (2003) demonstrate

[2] We thank Dr. Rahul Telang for providing this helpful reference.

that firms fail to coordinate their security investment in the presence of interdependent risks. An entity will significantly underinvest if it believes that there are other weak nodes in the network, leading to an inefficient equilibrium. Ogut et al. (2005) show that risk interdependency lowers firms' incentive to invest in security protection and buying insurance coverage. These papers capture the nature of Internet security and exhibit its impact on firms' decisions and market equilibria. However, eliminating the source of insecurity is generally not considered.

Researchers have started to examine the impact of various security mechanisms and policies on Internet security. Kannan and Telang (2005) compare the social efficiency between a CERT-type mechanism and a market-based mechanism on vulnerability disclosure. August and Tunca (2006a) compare the impact of different security policies on individual user's incentive to patch software taking account of patching costs and negative network externalities. Huang et al. (2007) discuss the weaknesses of existing solutions to DDoS attacks and then propose two approaches to counter such attacks. In this study, we propose a novel economic mechanism, a certification mechanism, to enhance collaboration among SPs and eliminate sources of malicious activities.

2.3 MODEL

2.3.1 Model Setup

We consider a classical network with N SPs. Each SP serves n customers. For notational simplicity, we use $M = Nn^2$ to represent the network effect. A SP is either of high-type or low-type. Users of high-type SPs generate less malicious traffic than those of low-type SPs. Let q denotes the ratio of the potential malicious traffic volume to the regular traffic volume originating from a SP's network. $q \in \{q_h, q_l\}$, where $q_h < q_l$. The

distribution of SPs' types is exogenously given and is common knowledge. $\Pr(q = q_h) = \delta$. A customer benefits from communicating with other customers and loses from receiving malicious traffic. A customer's average valuation of a unit of regular traffic is *V*. We normalize the expected volume of unidirectional Internet data stream between two customers to 1. The expected damage per unit of malicious traffic on customers is *v*. SPs charge a flat fee, *p*, for Internet access services to each customer. In the network without any security practices, a customer's expected utility can be expressed as $2NnV - Nnv(\delta q_h + (1-\delta)q_l) - p$.

SPs can deploy two types of security practices, protective practices and regulative practices. To successfully identify a unit of malicious traffic with probability $x \in [0,1]$ from inbound (outbound) traffic, a SP needs to invest $C_1(x)$ ($C_2(x)$) in protective practices (regulative practices). $C_1'(x) > 0$, $C_1''(x) > 0$, $C_2'(x) > 0$, $C_2''(x) > 0$ where x characterizes the effectiveness of security practices. $C_1(x)$ and $C_2(x)$ are the same for all SPs. For simplicity, we assume that the probability for regular traffic to be erroneously marked and discarded is 0. In addition, we assume $C_1(x) > C_2(x)$, $C_1'(x) > C_2'(x)$ for every $x \in [0,1]$. That is, the investment in regulative practices is more efficient than that of protective practices. We use quadratic investment cost functions. $C_1(x) = \frac{1}{2}\alpha x^2$ and $C_2(x) = \frac{1}{2}\beta x^2$, where $\alpha > \beta$. We assume that the effectiveness of security practices is observable to their customers.

The certification provider charges a subscription fee, *t*, for certification services to each SP. Certified SPs must compensate other certified SPs at the level of *s* per unit of malicious traffic originating from their networks. They also compensate their customers at the level of *s* per unit of malicious traffic regardless of its source. The timeline of the game is shown in Figure 2.3.

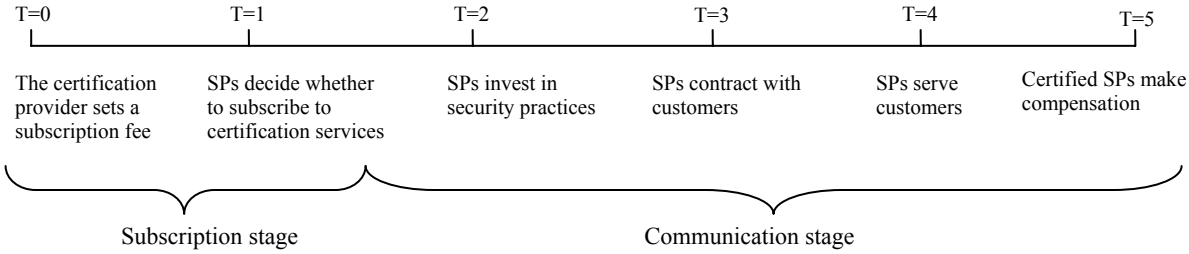


Figure 2.3: The Timing of the Dynamic Game

2.3.2 Conditions

The certification mechanism is designed to induce SPs to control malicious traffic. Such a mechanism is valuable when the following conditions hold. First, $2V > vq_l$ (Condition 1). That is, the damage created by malicious traffic from low-type SPs, although significant, does not offset the overall value of the communication. Second, $\alpha \geq Mvq_l$ (Condition 2). Condition 2 says that the efficiency of protective practices investment is low. Third, $MV - Mvq_l + \frac{1}{2\alpha}\left(Mvq_l\right)^2 \leq 0$ (Condition 3). Condition 3 ensures that no SP will let in any traffic from other SPs if all SPs are of low-type and hence the Internet data stream can go nowhere. It implies that the damage caused by low-type SPs is so drastic that the Internet will collapse if all SPs are of low-type. It seems that Condition 1 and Condition 3 contradict each other. However, they together characterize the reality of Internet communication. On the one hand, SPs generate positive values from communicating with one another. On the other hand, once a SP knows that another SP has a large number of malicious and incompetent customers, it will completely block inbound traffic from that SP. For example, email originating from regions with high rates of spam such as China, Russia, and South Korea has been blocked by many providers. Finally, we require that the compensation per unit of malicious traffic be equal to the damage that a unit of malicious traffic causes. That is, $s = v$ (Condition 4).

It is fair to let SPs be completely accountable for the loss entailed by forwarding malicious traffic.

2.4 ANALYSIS

In this section, we analyze SPs' and the certification provider's strategies and derive equilibria. We consider two cases: (i) a benchmark case without the certification mechanism, and (ii) the case with the certification mechanism. In the second case, we focus on the symmetric Perfect Bayesian Equilibria where SPs with the same types will adopt the same strategies. There are potentially three mutually exclusive and collectively exhaustive symmetric equilibrium outcomes, (1) a separating outcome that only high-type SPs subscribe to certification services; (2) a pooling outcome that all SPs subscribe to certification services; and (3) a pooling outcome that no SP subscribes to certification services. We use backward induction to derive the equilibria. We first analyze the following strategies of SPs in each outcome:

- the subscription strategy: whether to subscribe to certification services;
- the blocking strategy: whether to completely block the inbound traffic;
- the pricing strategy: how much to price their services;
- the investment strategy: whether to invest in protective and/or regulative practices and how much to invest.

The above strategies are controlled by the subscription fee charged by the certification provider. We then investigate the certification provider's pricing strategy and derive the equilibrium based on the certification provider's profitability.

2.4.1 Benchmark Case

In the benchmark case, we analyze strategies of SPs and identify the equilibrium without the regulation of certification services. Since protective practices have a direct

impact on SP's quality of service, a SP has incentive to invest in protective practices to improve its profitability. In contrast, SPs will not deploy regulative practices because it only benefits the recipient customers who are mostly in other SPs' networks. Therefore, a customer's willingness to pay to SP *i* is

$$u_{ib} = 2NnV - Nnv\left(1 - x_{ib}\right)E\left[q\right] \tag{2.1}$$

Here *b* refers to the benchmark case. The first term of equation (2.1) is a customer's expected benefit from communicating with other Internet users. The second term of equation (2.1) is a customer's expected loss caused by malicious traffic. x_{ib} represents the effectiveness of SP *i*'s protective practices. A customer's expected value is independent of her SP's type, but is affected by distribution of SPs' types in the network. Thus we drop subscript *i*. The price that SPs charge is equal to the customers' willingness to pay $p_b = u_b$. We state a SP's profit as follows:

$$\pi_b = p_b n - C_1\left(x_b\right) = 2MV - Mv\left(1 - x_b\right)E\left[q\right] - C_1\left(x_b\right) \tag{2.2}$$

Proposition 2.1 shows the SP's strategies, profit and the system surplus[3] in the benchmark case.

Proposition 2.1: *In the equilibrium of the benchmark case,*

(1) a SP only invests in protective practices and the level of the investment is $\frac{1}{2\alpha}\left(MvE[q]\right)^2$*;*

(2)a SP charges $2NnV - NnvE\left[q\right] + \frac{1}{\alpha}\left(NnvE\left[q\right]\right)^2 n$ *for Internet access services to its customers;*

(3) a SP's profit is $2MV - MvE\left[q\right] + \frac{1}{2\alpha}\left(MvE\left[q\right]\right)^2$*;*

(4) the system surplus is $\left(2MV - MvE\left[q\right] + \frac{1}{2\alpha}\left(MvE\left[q\right]\right)^2\right)N$

Proof: Using FOC, we get $x_b^* = \min\left\{\frac{1}{\alpha}MvE[q], 1\right\}$. From Condition 2, $x_b^* = \frac{1}{\alpha}MvE[q]$. Substituting x_b^* into Equation (2.1), we obtain the optimal price. Substituting x_b^* into

[3] The system surplus comprises ISPs' profit and customers' utilities.

Equation (2.2), we obtain a SP's profit. The system surplus is equal to the total profit of SPs. Q.E.D.

No SP will invest in the more efficient regulative practices to control the malicious traffic when they are autonomous due to the public good nature of regulative practices. Although all SPs suffer from rampant malicious activities via the Internet, none has incentive to eliminate the harmful code at its origin to benefit others. They only spend money to protect themselves.

2.4.2 The Network with the Certification Mechanism

We now analyze the case where the certification mechanism is introduced. SPs decide whether to subscribe to certification services considering the benefit and the cost of following the rules specified by the certification provider. If they subscribe to certification services, they have to pay a subscription fee and compensate for the loss caused by malicious traffic that they pass to their customers or other certified SPs. On the other hand, they can charge a higher price to their customers and solicit compensation whenever they are hit by malicious traffic from other certified SPs.

2.4.2.1 Separating Outcome

We first analyze SPs' strategies in the separating outcome. Certified SPs have incentives to invest in regulative practices to control the outbound traffic due to their accountability. However, they have no incentive to control the inbound traffic from other certified SPs since they are fully insured from Condition 4.[4] Regarding inbound traffic from non-certified SPs, certified SPs can choose whether to completely block it or not. If they let in such traffic, they need to control the inbound traffic by deploying protective practices. SPs adjust the price based on the expected quality of service which they can

[4] For the traffic transmitted within a SP's network, the SP does not have to use protective technology to examine the traffic again at the receiver side

provide to their customers. Lemma 2.1 gives the optimal blocking, pricing, investment strategies and profit of a certified SP in such a separating outcome.

Lemma 2.1 *In the separating outcome, the optimal strategies of a certified SP of type* q_i *are as follows:*

(1) it completely blocks inbound traffic from non-certified SPs;

(2) it only invests in regulative practices and the level of the investment is $\frac{1}{2}\beta\left(\min\left\{1,\frac{1}{\beta}Mv\delta q_h\right\}\right)^2$ *;*

(3) it charges $V\delta Nn + VNn$ *for Internet access services to its customers;*

(4) its profit is $MV\delta + MV - \left(1-\min\left\{1,\frac{1}{\beta}Mvq_h\delta\right\}\right)Mv\delta q_i - \frac{1}{2}\beta\left(\min\left\{1,\frac{1}{\beta}Mv\delta q_h\right\}\right)^2 - t$

If a low-type SP subscribes to certification services, it has to invest more in regulative practices than a high-type SP does because it has more potential malicious traffic originating from its network. As a result, the profit of a certified low-type SP is lower than that of a certified high-type SP. This result is critical for the certification provider to be able to exclude low-type SPs from certification services using the subscription fee.

If a SP does not obtain a certificate, its strategy is similar to a SP in the benchmark case. They are not responsible for malicious traffic from their networks and hence have no incentive to prevent malicious traffic from being sent out. They will only invest in protective practices for their own customers. Lemma 2.2 gives a non-certified SP's optimal strategies.

Lemma 2.2 *In the separating outcome, a non-certified SP's strategies are as follows:*

(1) it only invests in protective practices and the level of investment is $\frac{1}{2\alpha}\left(Mvq_l\left(1-\delta\right)\right)^2$ *;*

(2) it charges $NnV + NnV\left(1-\delta\right) - NnvE\left[q\right] + \frac{1}{\alpha}N^2n^3\left(vq_l\left(1-\delta\right)\right)^2 + Nnv\delta q_h\min\left\{1,\ \frac{1}{\beta}Mvq_h\delta\right\}$

for Internet access services to its customers;

(3) its profit is $VM + MV\left(1-\delta\right) - MvE\left[q\right] + \frac{1}{2\alpha}\left(Mvq_l\left(1-\delta\right)\right)^2 + Mv\delta q_h\min\left\{1,\ \frac{1}{\beta}Mvq_h\delta\right\}$

Certified SPs generate positive externality by deploying regulative practices, such as detecting the malicious users, filtering outbound malicious traffic and eliminating sources of malicious activities. Non-certified SPs receive less malicious traffic from certified SPs and directly benefit from certified SPs' regulative practices to the level of $Mv\delta q_h \min\left\{1,\ \frac{1}{\beta} Mvq_h\delta\right\}$. In addition, non-certified SPs indirectly benefit from certified SPs' investment. They can save by having to invest in protective practices only at the level of $\frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2$, unlike $\frac{1}{2\alpha}\left(MvE[q]\right)^2$ in the benchmark case.

Corollary 2.1 *Certified SPs can charge a higher price than non-certified SPs.*

Corollary 2.1 insures that SPs benefit from possessing certificates and are willing to subscribe to certification services. In the separating outcome, the Internet is partially separated into two parts, certified networks and non-certified networks. In certified networks, certified SPs can block the unprofitable communication from low-type SPs and can collaborate with other certified SPs to implement more efficient security practices. Consequently, they cooperatively maintain a better communication environment for their customers. Even though certified SPs must shoulder the cost of malicious activities, they may still benefit from subscribing to certification services if the subscription fee is appropriately priced.

The subscription fee charged by the certification provider plays an important role in supporting the separating outcome that only high-type SPs subscribe to certification services: it must be high enough so as to intimidate low-type SPs from mimicking high-type SPs, but not too high to frustrate high-type SPs from subscribing to certification services.

Lemma 2.3 *When* $\beta \geq Mvq_h\delta$ *, there exists a range of subscription fees, t, all of which support the separating outcome. The optimal subscription fee for certification services to induce separating outcome is* $MV(2\delta-1) + Mvq_l(1-\delta) - \frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2 - \frac{1}{2\beta}\left(Mvq_h\delta\right)^2$.

$\beta \geq Mvq_h\delta$ is used to ensure that certified SPs with different types make different profit and hence guarantees that the certification provider can charge a fee to induce the separating outcome. For each β, there exists a continuum of fees which support the separating outcome.

2.4.2.2 Pooling Outcome: If All SPs Get Certified

If all SPs subscribe to certification services, they will all invest in regulative practices to control outbound traffic and they do not need to deploy protective practices to filter inbound traffic from certified SPs. Lemma 2.4 gives certified SPs' optimal strategies in the pooling outcome.

Lemma 2.4 *In the pooling outcome where all SPs are certified, the optimal strategies of a certified SP of type* q_i *are as follows:*

(1) it completely blocks the inbound traffic from non-certified SPs if there is any;
(2) it only invests in regulative practices and the level of investment is $\min\left\{1,\ \frac{1}{\beta}Mvq_i\right\}$*;*

(3) it charges $2VNn$ *to its customers for Internet access services;*
(4) its profit is $2VM - Mv\left(1-\min\left\{1,\ \frac{1}{\beta}Mvq_i\right\}\right)q_i - \frac{1}{2}\beta\left(\min\left\{1,\ \frac{1}{\beta}Mvq_i\right\}\right)^2 - t$

In this case, non-certified networks diminish, leaving only certified networks. All SPs take the responsibility of security and focus on the relatively more efficient regulative practices instead of protective practices. Lemma 2.5 gives the optimal subscription fee that the certification provider can charge to induce the pooling outcome.

Lemma 2.5 *There exists a range of subscription fees, t, all of which support the pooling outcome. The optimal fee for the certification provider to induce pooling outcome is*

$$\begin{cases} t \leq VM + Mvq_h\delta - Mvq_l\delta + \frac{1}{2\beta}\left(Mvq_l\right)^2 - \frac{1}{\beta}\left(Mvq_l\right)^2\left(1-\delta\right) - \frac{1}{\beta}\left(Mvq_h\right)^2\delta & \text{if } \beta \geq Mvq_l \\ t \leq VM - \frac{1}{2}\beta + Mvq_h\delta - \frac{1}{\beta}\left(Mvq_h\right)^2\delta & \text{if } Mvq_h \leq \beta < Mvq_l \\ t \leq VM - \frac{1}{2}\beta & \text{if } \beta < Mvq_h \end{cases}$$

If a SP does not subscribe to certification services, its outbound traffic is blocked by certified SPs. Although a SP must pay for certification services and subsequently be financially responsible for the malicious traffic from its network, it still has an incentive to subscribe to certification services for two reasons. First, by subscribing to certification services, a SP stays in a bigger network and provides more extensive and secure communication services to its customer. Secondly, it is able to concentrate on the more efficient regulative practices.

In the pooling outcome where no SP subscribes to certification services, SPs' pricing and investment strategies are the same as those in the benchmark case. Since the certification provider makes zero profit, it always prefers to the other pooling outcome. In the rest of the paper, the pooling outcome refers to the pooling outcome where all SPs subscribe.

2.4.2.3 The Certification Provider's Profit

The certification provider's revenue comes from certification fees. Such a potential business will survive only when there is justifiable profit. For a for-profit certification provider, Proposition 2 characterizes the certification provider's strategies.

Proposition 2.2*: The certification provider induces the pooling equilibrium if (1)* $\beta \le Mvq_h\delta$*, or (2)* $Mvq_h\delta < \beta \le Mvq_h$ *and* $\frac{1}{2}vq_h + \frac{1}{3}vq_l - V < 0$*; the certification provider induces the separating equilibrium when the proportion of high-type SPs is higher than* $\bar{\delta}$ *if (1)* $\beta > Mvq_h$*, or (2)* $Mvq_h\delta < \beta \le Mvq_h$ *and* $\frac{1}{2}vq_h + \frac{1}{3}vq_l - V > 0$.

There are two countervailing forces which affect the certification provider's preference to the pooling equilibrium. They are the network effect and the inferior nature of low-type SPs. On the one hand, the certification provider wants to have as many SPs as possible to subscribe to its services. On the other hand, it has to lower the certification fee to induce the low-types to participate (as corllorary 2.1 shows). The efficiency of the

regulative practice investment and the level of damage caused by malicious traffic moderate the tradeoff. When regulative practices are very efficient (i.e., $\beta \le Mvq_h\delta$), low-type SPs are as good as high-type SPs in controlling outbound traffic. The certification provider is willing to serve both high-type and low-type SPs. The certification mechanism only has a pooling equilibrium. When the regulative practice investment is rather efficient (i.e., $Mvq_h\delta < \beta \le Mvq_h$), the level of damage caused by malicious traffic is important. Specifically, when the damage caused by malicious traffic is relatively low (i.e., $\frac{1}{2}vq_h + \frac{1}{3}vq_l - V < 0$), the network effect dominates the inferior nature of low-type SPs. The certification provider prefers to serve low-type SPs since the certification provider can charge subscription fee to more SPs and this fee could be higher due to the network effect. However, if the damage caused by malicious traffic is high (i.e., $\frac{1}{2}vq_h + \frac{1}{3}vq_l - V > 0$), the certification provider wants to exclude low-type SPs when the proportion of high-type SPs is high enough. Low-type SPs spend more in controlling outbound traffic and can only afford a lower fee compared with high-type SPs. Thus, the certification provider prefers to only serve high-type SPs. When the regulative practice investment is not very efficient (i.e., $\beta > Mvq_h$), the disadvantage for low-type SPs in controlling outbound traffic becomes more severe and demand an even lower subscription fee. Consequently, the certification provider will give up the market for low-type SPs.

2.5 SYSTEM SURPLUS

In the pooling equilibrium, all SPs invest in more efficient security practices, regulative practices, instead of protective practices. We conclude that the pooling equilibrium always generates a higher system surplus than the benchmark case. Proposition 2.3 further shows that the pooling equilibrium is also more efficient than the separating equilibrium and hence it is socially optimal.

Proposition 2.3: *The pooling equilibrium is socially optimal.*

Although blocking the inbound traffic from low-type SPs could be an optimal strategy for SPs (as Condition 3 specifies), it is not socially optimal. The magnitude of damage caused by low-type SPs cannot completely eliminate the benefit that low-type SPs bring to network communications (corresponding to Condition 2). Network effect always dominates the adverse consequence caused by low-type SPs. Therefore, we conclude that a global network should be maintained.

Social optimality can be achieved when the certification provider is a non-profit organization who always maximizes the system surplus. However, a for-profit certification provider may prefer the separating outcome in certain conditions. Proposition 2.4 shows that, though suboptimal, the separating equilibrium can still generate a higher system surplus than the benchmark case.

Proposition 2.4: *There is a* $\tilde{\delta}$ *above which the separating equilibrium generates a higher system surplus than in the benchmark case.*

The network effect, which plays a prominent role in network communications, is unavoidably undermined by the blocking and separation induced by the certification mechanism. However, when the proportion of high-type SPs is high and enough SPs subscribe to certification services, efficiency can still be improved given that regulative practices are widely deployed.

Corollary 2.2: *The certification mechanism induces a higher system surplus when (1)* $\beta > Mvq_h$ *or (2)* $Mvq_h\delta < \beta \le Mvq_h$ *and* $\frac{1}{2}vq_h + \frac{1}{3}vq_l - V < 0$.

When one of the conditions hold, the certification provider always induces the pooling equilibrium which is the socially optimal outcome.

2.6 DISCUSSION AND CONCLUSION

This research examines the Internet architecture and addresses Internet security issues from an economic perspective. We propose a certification mechanism to induce SPs to exert collective effort and improve Internet security. More specifically, the proposed mechanism provides certified SPs incentives to deploy regulative practices. We use a game-theoretic model to examine the efficiency of our mechanism. The results show that our mechanism can increase the system surplus. By providing SPs with appropriate incentives, our mechanism can create a better communication environment over the Internet.

The challenging issue is, *who should be the certification provider*? The certification provider can be a non-profit institution, such as Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a central authority with limited power in the essentially decentralized and neutral global network. However, its functions are restricted to running the addressing system, giving out blocks of unique identifiers to countries and private registries. Commentators have suggested ICANN should play an enhanced role in governing the unregulated Internet. By providing certification services, it introduces a soft regulation to the Internet, characterized by the fact that participation is voluntary, and participants choose their actions based on self-interest. The certification provider can also be a for-profit organization. The previous analysis examines the certification provider's profit and discusses its impact on system surplus.

This paper characterizes the effectiveness of security practices using a single parameter, x, representing the *false negative*[5]. In most control settings, both false negatives and false positives are used to describe the effectiveness of security practices.

[5] A false negative is the polar opposite of a false positive. A false negative occurs when the security protection fails to detect a malicious activity. For example, a virus scanner fails to detect a virus in an infected file or an email filter fails to detect a spam email.

Since regulative practices generally outperform protective practices in reducing errors, the analysis and results considering both false positive and false negative will be similar.

In addition to the subscription fee, certified SPs also incur the overhead when they verify the certification status of incoming packets. The overhead has the similar impact on SPs' payoff as the subscription fee. When the overhead or the subscription fee increases, SPs have less incentive to subscribe to certification services. However, it must be recognized that without the certification mechanism, SPs have to carefully filter all incoming traffic. The increasingly sophisticated attacks make it more difficult and costly to detect malicious activities from incoming traffic. The proposed certification mechanism has the advantage of avoiding the difficulty of handling incoming malicious traffic. SPs can effectively manage the cost by shifting the focus from identifying malicious incoming traffic to verifying the certification status of incoming traffic. Thus, the overhead will not be a barrier to the implementation of the certification mechanism.

Chapter 3: Security Overinvestment and Risk Pooling Arrangement

3.1 INTRODUCTION

Information security has become a major concern for public and private organizations. Studies indicate that security-related spending is growing fast. According to the annual CSI/FBI Computer Crime and Security Survey 2006 (Gordon et al. 2007), firms with annual sales under $10 million spent an average of $1,349 per employee on computer security in 2006, a 210% increase over 2005, and firms with annual sales between 10 million and $99 million spent an average of $461 per employee on computer security, a 327% increase over 2005. In academia, information security has drawn a tremendous amount of attention. Researchers have addressed information security from technical perspectives (e.g., Muralidhar et al. 1999; Sarathy and Muralidhar 2002; Garfinkel et al. 2002), economic perspectives (e.g., Gordon and Loeb 2002; 2006; Gal-Or and Ghose 2005; Cavusoglu et al. 2004; 2005; Kannan and Telang 2005; Ghose and Rajan 2006), and organizational perspectives (e.g. Loch et al. 1992; Straub and Welke 1998; Gattiker and Kelley 1999; Tanaka et al. 2005). A central research question is how firms can manage security expenditure in an effective and efficient way.

Existing literature on information security mainly focuses on the underinvestment issue (e.g., Anderson 2001; Kunreuther and Heal 2003; Ogut et al. 2005), while the overinvestment issue has not received adequate attention. It is worth noticing that firms' security investment may exceed, rather than fall behind, the optimal level in many cases. For instance, the Sarbanes-Oxley Act 2002 (SOX) has dramatically boosted firms' spending on security. However, companies largely find that the costs of compliance exceed the benefits. A study by Oversight (Oversight 2006) indicates that 37% of

financial executives say SOX compliance created a cost burden that suppresses stock prices (up from 33% in 2004). A Symantec study investigates the efficiency of IT risk management programs that firms maintain and the levels of IT risks they experience. The report summarizes that some organizations are addressing IT risks through overinvestment (Symantec 2007). Although firms' security may not be sufficient overall, redundant resource allocation and excessive investment still exist in certain security areas. In this study, we focus on the overinvestment issue.

There are many reasons for the overinvestment in security. First, security investment may create competitive advantages, which drive firms to invest aggressively. For example, Dynes et al. (2005) found that business customers deem security investment to be a qualifier when evaluating partners. Further, the number of security incidents a firm has affects investors' confidence, making it more difficult for the firm to compete with its rivals for future capital investments (Campbell et al. 2003). Therefore, firms may heavily invest in security to maintain the partner relationship in supply chains and/or to secure their financing capabilities in the capital market. Second, the negative externality associated with information security risks may drive firms to invest more (Kobayashi 2005). For example, a highly protected website may divert hackers to other sites. However, individual firms may ignore this negative externality and invest more than the socially desirable level. Third, the regulatory compliance on internal control (Bailey Jr. et al. 1985) may distract managers' attention and result in overinvestment in security. For example, SOX 404 imposes significant personal penalty on corporate executives for incompliance with the internal control requirements. The compliance pressure results in less cost-effective spending (Leech 2004; Ranger 2005).

Researchers and practitioners have long been studying how to motivate firms to invest in information security at the socially optimal level. Many researchers (Varian

2000; Gordon et al. 2003; Ogut et al. 2005b; Kesan et al. 2005) have proposed that firms can use cyberinsurance to manage their information security risks and optimize their security expenditure. Cyberinsurance is a range of first-party and third-party coverage that enables firms to transfer their security risks to the insurance market.[6] With the cyberinsurance market, firms can balance the expenditure between security protection and insurance, and thus reduce the cost-ineffective investment. Therefore, cyberinsurance can be a potential approach to address the overinvestment issue.

This paper finds that even if the cyberinsurance market is mature (i.e., with actuarially fair premium and no agency problem), it cannot eliminate overinvestment. We start with the case that firms overinvest due to competition. That is, when security investments can bring firms some competitive advantages besides loss prevention, firms tend to overinvest. In this case, cyberinsurance cannot alleviate the competitive effect of security investment and firms still have an incentive to overinvest.

Interestingly, we show that firms may prefer a "less mature" risk management solution, which induces the *moral hazard* problem. In the context of insurance, moral hazard refers to the policyholders' reluctance to invest in loss prevention and loss reduction (Pauly 1968). Although moral hazard is not a favorable feature in general (e.g., Shavell 1979), we find that it can effectively mitigate firms' overinvestment incentive. This benefits firms by preventing the "prisoners' dilemma" where all firms heavily invest in security but the advantage of increased investment is competed away. In this paper, we specifically study such a "less mature" risk management solution – the risk pooling arrangement (RPA).

[6] Examples of existing policies include AIG's NetAdvantage, Lloyd's e-Comprehensive, Chubb's CyberSecurity, Hiscox's Hacker Insurance, etc. The coverage of cyberinsurance includes damages in loss/corruption of data, business interruption, liability, cyber extortion, public relations, criminal rewards, cyber-terrorism, and identity theft.

RPA generally refers to the mutual form of insurance organizations in which the policyholders are also the owners. Examples of RPA include group captive insurance companies, risk retention groups, self insurance groups, etc.[7] The mutual form of insurance organizations was widely adopted in the insurance markets for medical malpractice and municipal liability during the late 1980s (Ligon and Thistle 2005). It has also been since used in other lines of insurance, such as employee pension and employee health insurance. From the perspective of practitioners, the primary advantages of RPA over commercial insurance include reduced overhead expense and flexible policy development (Swiss Re 2003).

Compared to a mature commercial cyberinsurance market, RPA is "less mature" in two ways. First, RPA cannot completely eliminate the risks for an individual policyholder. Even though the risk pool can fully cover individual firms' security losses, each individual firm has to bear part of the risk pool's loss through its equity position. Put differently, RPA leaves positive risk retention for individual members. Second, RPA induces the moral hazard problem (Lee and Ligon 2001). Since members of the risk pool share risks with each other, an individual firm's risks are not completely influenced by its own security investment. Therefore, individual firms have an incentive to reduce their investment. This type of moral hazard is also known as "*moral hazard in team*" (Holmstrong 1982).

The analysis in this paper reveals that RPA can outperform a mature cyberinsurance market in addressing the overinvestment issue. When the competition is

[7] Group captives are special insurance companies that are set up by a group of companies to insure their own risks. Many large corporations have their own single-parent captives. From 2000 to 2004, net premiums written in the captive insurance industry grew by 56 percent, reaching more than $50 billion. Risk retention groups (RRG) are insurance institutions in which entities in a common industry join together to provide members with liability insurance. In 2005, RRG's gross written premium reached $2.5 billion. Self-insurance groups are insurance entities in which firms in similar industries or geographic locations pool resources to insure each other's risks. In 2003, gross written premium of self-insurance groups reached $44 billion (Swiss De 2003; Insurance Information Institute 2006).

sufficiently intense, firms can be better off by setting up a risk pool to share risks with each other instead of using the commercial insurers. The moral hazard associated with RPA softens the competition among firms and mitigates their incentive to overinvest. Therefore, firms are willing to use RPA even though it does not fully eliminate their risks. However, as the size of the pool grows, the moral hazard becomes more severe and eventually leads to underinvestment. Consequently, RPA loses its advantage over mature commercial cyberinsurance. In this regard, there exists an upper bound for the pool size. We further show that multiple pools each with limited size will be formed when the number of competing firms is large.

We then examine the case in which firms can use both RPA and commercial insurance. This paper shows that even when firms can access a mature commercial insurance market, they will still setup a risk pool and allocate certain amount of risks to it. Balancing insurance spending between the commercial insurance market and RPA always dominates pure reliance on the commercial insurance market. Moreover, as the number of firms approaches the infinite, we show that firms invest at the socially optimal level and achieve the socially optimal payoffs.

We further extend this model to analyze two relevant scenarios. First, we consider a different type of security overinvestment—the overinvestment caused by the security risks with negative externality. The analysis shows that RPA can also mitigate the overinvestment incentive. Second, we relate our analysis to the research on security underinvestment (e.g., Anderson 2001; Kunreuther and Heal 2003). We show that overinvestment in certain security practices can exacerbate the problem of underinvestment in other security practices. Through mitigating overinvestment, RPA helps firms optimize the allocation of security spending and improve their overall payoffs.

Given the diverse practice of IT risk management solutions, our paper offers an economic rationale for the adoption of RPA. Traditionally, practitioners have recognized that RPA has the advantages of reduced overhead expense and flexible policy development. This paper indicates that RPA can reduce the undesirable security investment, and with limited pool size, RPA can outperform the commercial insurance market. Moreover, this paper provides security managers with guidance on allocating risks between commercial insurance and RPA.

This paper also generates important implications for the social planner regarding the regulation of the insurance industry. Although the capacity limit of the commercial insurance market stimulates the demand for Alternative Risk Transfer (ART) solutions, the development of RPA is still highly subject to regulatory attitudes. Therefore, it is important for the social planner to recognize not only the strength of RPA in security management at the firm level, but also the positive impact of RPA on industry competition and cooperation. Such recognition can help guide the development of appropriate policies for RPA and improve the social welfare overall.

The rest of the paper is organized as follows. Section 3.2 reviews related literature on the economics of information security and insurance. In section 3.3, we outline the model setup and analyze the case with only the commercial insurance market. Section 3.4 analyzes the case with RPA and compares RPA with the commercial insurance market. Section 3.5 examines the case where both RPA and the commercial insurance market can be used. In section 3.6, we discuss the managerial and policy implications of this study and conclude the chapter.

3.2 LITERATURE REVIEW

Prior research on the economics of information security has studied many issues regarding information security investment. Anderson and Moore (2006) discuss how

moral hazard and adverse selection problems distort firms' incentives to invest in information security. Gordon and Loeb (2002) develop an economic model to study the optimal investment in information security. Gordon and Lucyshyn (2003), and Gal-Or and Ghose (2005) examine firms' incentives to share security information and show that information sharing can benefit security investment. Kunreuther and Heal (2003) demonstrate that firms generally underinvest in security protection when their security risks are interdependent. Our paper considers the optimization problem of firms' security investment. However, we focus on addressing firms' distorted incentives to overinvest rather than underinvest.

There is a growing body of literature examining the use of cyberinsurance to address information security. Gordon et al. (2003) and Kesan et al. (2005) generally discuss the advantages of cyberinsurance in information risk management. Ogut et al. (2005a) examine firms' investments in security protection and their use of cyberinsurance in the context of interdependent security risks. All of these studies focus on the commercial cyberinsurance market. This paper differs from these studies in examining ART mechanisms (i.e., RPA) as a complement to the commercial cyberinsurance market.

Prior literature on risk management justifies the existence of the mutual insurance organizations from a variety of perspectives. For example, the mutual form of insurance organization is more efficient when the distribution of risks prevents independent insurers from using the law of large numbers to eliminate risks (e.g., Marshall 1974; Doherty and Dionne 1993). The mutual form of insurance can also address the interest conflicts between insurers and policyholders since policyholders themselves are the owners of a mutual insurer (Mayers and Smith 1981; Mayers 1988; Cummins and Weiss 1999). Moreover, mutual insurers may coexist with independent insurers as a result of the adverse selection of risk-averse policyholders (e.g., Ligon and Thistle 2005). This paper

complements the above studies by illustrating the advantages of mutual insurance organizations from a new perspective. That is, the moral hazard problem induced by mutual insurance organizations can be strategically leveraged to mitigate the undesirable competition among policyholders.

The moral hazard problem has been examined in the context of the conventional insurance market (e.g., Shavell 1979) and RPA (e.g., Lee and Ligon 2001). Shavell (1979) shows that partial insurance coverage can be used to address the moral hazard problem. Lee and Ligon (2001) illustrate that that moral hazard problem exists in RPA because the sharing of risks among pool members decreases individual members' incentive to invest in loss prevention. They show that the moral hazard problem becomes severe when there are a large number of members; hence, the size of the risk pool should be limited. All of these studies focus on the negative side of moral hazard in the insurance market. In contrast, this paper illustrates the benefit generated by the moral hazard associated with RPA.

3.3 MODEL

We consider n risk-averse firms. Each firm has an initial wealth A. All firms have an identical utility function $U(.)$, where $U(.)$ satisfies that $U'(.)>0$, $U''(.)<0$ (i.e., $U(.)$ is concave), and $U'''(.)\geq 0$. We ignore the higher-order utility effect (i.e., $U^{[4]}(.)$ and higher derivatives are equal to zero). Firms' breach probabilities depend on firms' security investment. Specifically, we assume that firm i's breach probability is $\mu(x_i)$, where x_i denotes firm i's security investment. $\mu(.)$ is a decreasing and convex function: $\mu'(.)<0.\ \mu''(.)>0$. Moreover, $\mu(0)\leq 1$. We also assume that a firm loses L in a security breach.

More security investment not only results in a lower breach probability, but also brings a firm some competitive advantages over its competitors. For example, more

security investment may ease potential business partners' concern over security and thus ensure business relationships; and more security investment can increase investors' confidence about a firm's cash flow and thus reduce its cost of raising capital from the financial market. Specifically, we assume that, given firm i's security investment x_i and its competitors' security investments x_{-i}, firm i gains $C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right)$, where C represents the competition intensity.[8] In other words, if firm i's security investment is higher (lower) than the average security investment of its competitors, firm i gains (loses) a positive amount of capital: $C>0$. We also assume $C<1$ to avoid the degenerate solution that firms never invest. Firm i's expected utility can be represented as [9]

$$\mu(x_i)U\left(A - L + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - x_i\right) + (1-\mu(x_i))U\left(A + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - x_i\right)$$

For notational simplicity, we use μ_i to denote $\mu(x_i)$.

Suppose firms can buy insurance from commercial insurers. In this paper, we consider the case that the commercial insurance market is mature. The perfect competition in the commercial insurance market leaves all surplus to the insured firms, and commercial insurers always earn zero profit. It is also assumed that firms' security investments are observable. Therefore, when firm i buys coverage I_i, the insurance premium is[10] $P_i = \mu_i I_i$. Firm i's expected utility can be represented as

$$\Pi_i = \mu_i U\left(A - L + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) + I_i - \mu_i I_i - x_i\right) + (1-\mu_i)U\left(A + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - \mu_i I_i - x_i\right)$$

[8] The linear functional form is used here mainly for the ease of exposition. However, the insight derived from this model is not dependent on the assumption of this functional form.

[9] Note that in this model, the security investment can bring ex ante competitive advantage, i.e., the competitive advantage is not dependent on the probabilistic event of security breach. However, the insight in this model can also be generalized to the situation where the security investment can bring ex post competitive advantage. For example, more security investment may ease the investors' concern when security breach occurs and thus decrease the magnitude of loss.

[10] Note that we assume that the firm's security investment cannot be contractible in the insurance market. That is, the commercial insurer cannot specify the level of security investment in the insurance contract and enforce it. The non-contractibility can be attributed to the non-verifiability of the security investment. We assume that firms purchase insurance after their investments are observed by insurers. Given the intense competition in the insurance market, firms can always obtain a fair premium.

3.3.1 Only the Commercial Insurance Market

Existing insurance literature (e.g., Shavell 1979) indicates that it is optimal for firms to buy full insurance in the mature insurance market, i.e., $I_i=L$. With this result, firm i's optimal security investment can be determined using the first-order condition (FOC),

$$U'(.)(-\mu_i' L + C - 1) = 0$$

In the symmetric case where $x_i=x_{-i}$, firm i's optimal security investment x_i satisfies that

$$\mu_i' = -\frac{1-C}{L}$$

Lemma 3.1 *In presence of competition, firms overinvest in security.*

Proof: In this first best case, the FOC is $U'(.)(-\mu_i' L - 1) = 0$. Firm i's optimal security investment x_i satisfies that $\mu_i' = -\frac{1}{L} < -\frac{1-C}{L}$. Since $\mu'' > 0_i$, firms overinvest in security when $C > 0$. Q.E.D.

Without competition, the only purpose of security investment is to reduce the insurance premium. In the presence of competition, firms tend to invest more in security to gain the competitive advantage. Each individual firm's advantage will be competed away as all firms increase their security investment. The security investments are more than necessary from the perspective of a social planner. Dynes et al. (2005) find that although firms increase their security investment, few executives felt that such investment in their industry led to increased revenue. The insurance market is insufficient to resolve the overinvestment issue since insurance cannot mitigate the excess incentive of investment caused by the competition.

3.3.2 The Risk Pooling Arrangement (RPA)

In this section, we consider the case where n firms can form a risk pool and share the security loss with each other. An example is that firms may jointly setup a group captive insurance company. The group captive issues insurance to each firm. Since the

group captive is jointly funded by insured companies, the aggregate loss of the group captive is shared by the insureds through their equity position.[11] In particular, if the risk pool covers firm i's loss of an amount q, each of the other firms compensates firm i an amount of q/n once firm i suffers a loss. The compensation is altogether $(n\text{-}1)q/n$. In this section, we consider the following two-stage game. In stage 1, n firms cooperatively choose the amount of loss q covered by the risk pool. It is assumed that $q \le L$. In stage 2, firms choose their security investment x_i (i=1…n) non-cooperatively.

We study a symmetric case. Let x_{-i} denote the security investment of firms other than firm i and $\mu_{-i} = \mu(x_{-i})$ denote the corresponding breach probability. With the risk pooling arrangement, the expected utility of firm i with RPA is

$$\begin{aligned} &\mu_i \sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right) U\left(A - L + \frac{(n-1-k)}{n} q + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - x_i\right) \\ &+ (1-\mu_i) \sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right) U\left(A - \frac{k}{n} q + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - x_i\right) \end{aligned} \tag{3.1}$$

where $b\left(k;(n-1),\mu_{-i}\right) = \sum_{k=0}^{n-1} \frac{(n-1)!}{k!(n-1-k)!} \mu_{-i}^k \left(1-\mu_{-i}^k\right)^{n-1-k}$ denotes the binomial probability that k out of n-1 firms have a security breach.

Lemma 3.2 *In the symmetric case, $q = L$. That is, when firms form a risk pool, they use the risk pool to cover all the risks.*

Lemma 3.2 is consistent with the result in the literature (Lee and Ligon 2001), i.e., without a commercial insurance market, firms set up a risk pool to cover all of their risks. Since firms are risk-averse, they are always willing to transfer more risks to others. Consequently, the mutual insurer issues a full-coverage policy to each firm. As an equity holder of the risk pool, each firm not only retains a share of its own loss but also shoulder a share of any other firm's loss equal to L/n. When k firms suffer security breaches,

[11] Note that the insurance premium paid to the risk pool is suppressed from the model. The rationale is that the premium income of the risk pool will be returned to the member firms as the equity return.

resulting in the mutual insurer incurring an aggregate loss of kL, each firm eventually bears an equity loss of kL/n. Proposition 3.1 characterizes how RPA affects firms' security investment.

Proposition 3.1 *In the symmetric equilibrium, firms invest less in security when using RPA than when using commercial insurance. Furthermore, firms' investments decrease as the number of firms in the risk pool increases.*

Proposition 1 indicates that RPA induces the member firms to invest less. Firms invest less due to the moral hazard problem. When a firm's security loss is determined by the aggregate investment, it has less incentive to invest. This is also called *moral hazard in team* (Holmstrom 1982). As the size of the risk pool increases, the moral hazard problem becomes more severe, and firms further decrease their security investment.[12] In this way, RPA can mitigate firms' overinvestment incentive. This capability of RPA may render it preferable to the commercial insurance market.

3.3.3 The Comparison between RPA and Commercial Insurance

We examine when RPA leads to a better outcome for insured firms than a competitive insurance market. In a symmetric equilibrium, we denote x_P (x_C) and μ_P (μ_C) as the equilibrium investment and breach probability, respectively, when firms use RPA (commercial insurance). We compare a firm's expected utility using RPA (in Equation 3.2) with a firm's expected utility using commercial insurance (in Equation 3.3),

$$\Pi_P(n) = \sum_{k=0}^{n-1} b\left(k;(n-1),\mu_P\right)\left[\mu_P U\left(A - \frac{1+k}{n}L - x_P\right) + (1-\mu_P)U\left(A - \frac{k}{n}L - x_P\right)\right] \quad (3.2)$$

$$\Pi_C = U\left(A - \mu_C L - x_C\right) \quad (3.3)$$

Since it is impossible to compare Equation (3.2) and Equation (3.3) analytically, we rely on the numerical analysis to illustrate the insights. The numerical analysis has

[12] Lee and Ligon (2001) present a formal proof on this feature. They show that as long as one ignores the higher-than-fourth derivative of the utility function, the firms' equilibrium security investment is always strictly decreasing in the number of the risk pool members.

been adopted in prior insurance research (e.g., Asmussen and Rubinstein 1999). We use the following specifications. The breach probability function is $\mu(x)=e^{-x}$. This functional form is consistent with the assumption that $\mu'(x)<0$ and $\mu''(x)>0$. The firm's utility function is $U(x)=-x(20-x)$. This functional form is consistent with the assumption that $U'(x)>0$, $U''(x)<0$, $U'''(x)\geq 0$. The initial wealth A is 8 and the loss L is 6. The competition intensity C is 0.7. Figure 3.1 compares the firm's expected utility using RPA with that using commercial insurance. In Figure 3.1, the "*" line represents the firm's expected utility using RPA and the "+" line represents firms' expected utility using commercial insurance.

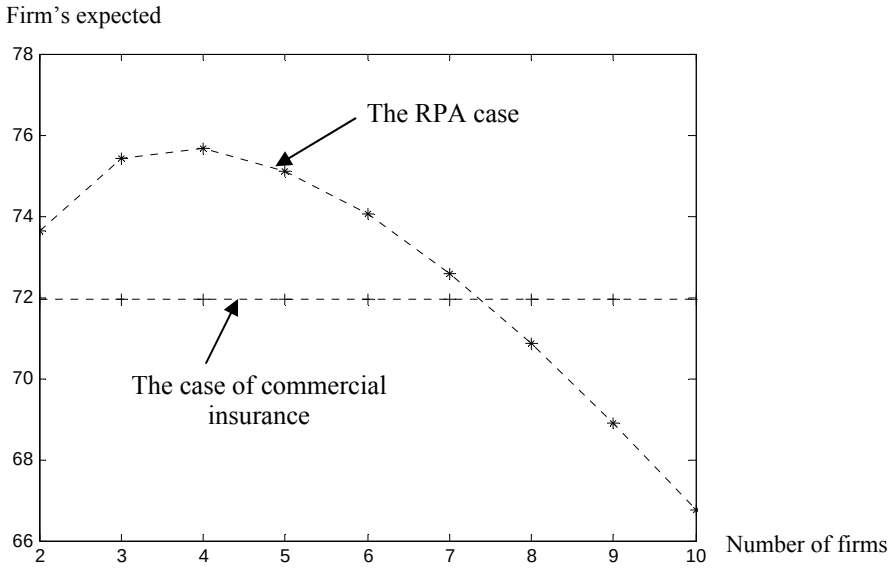


Figure 3.1: The Firm's Expected Utility in the Symmetric Case

As Figure 3.1 shows, when the number of firms is small (i.e., $n\leq 7$), RPA yields higher expected utility than the commercial insurance market. However, when the number of firms is large (i.e., $n>7$), RPA yields lower expected utility than the commercial insurance market. Figure 3.2 and Figure 3.3 together illustrate why RPA can dominate the commercial insurance market. Figure 3.2 compares the firm's security

investment in these two cases. The "*" line represents firms' security investment using RPA; the "+" line represents firms' security investment using commercial insurance; and the "○" line represents the security investment at the socially optimal level. As Figure 3.2 shows, the security investment in the commercial insurance case is higher than the socially optimal level. The security investment in the RPA case is lower than that in the commercial insurance case. This implies that the competition among firms in their security investment is softened, and thus explains why RPA generates a higher expected utility for firms.

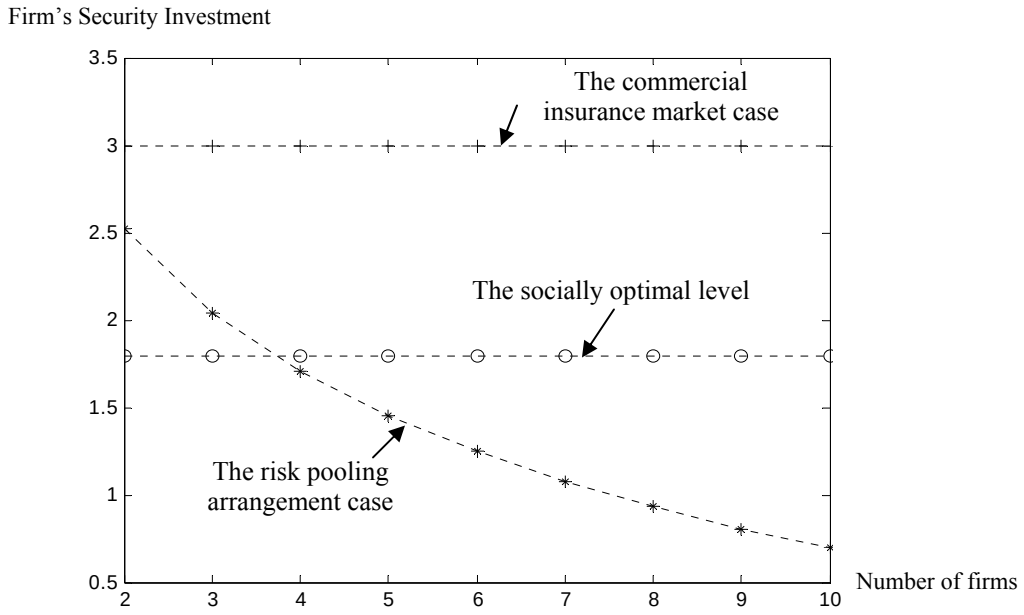


Figure 3.2: The Firm's Security Investment

Note that when $n \geq 4$, the security investment in the RPA case is lower than the socially optimal level. This means that RPA leads to underinvestment. The reason is that when more firms are in the risk pool, each firm free-rides more on other firms, and the moral hazard problem becomes more severe. When firms invest less than the socially

optimal level, their expected utilities start to decrease. When n>7, the moral hazard problem is so severe that RPA is no longer better than the commercial insurance market.

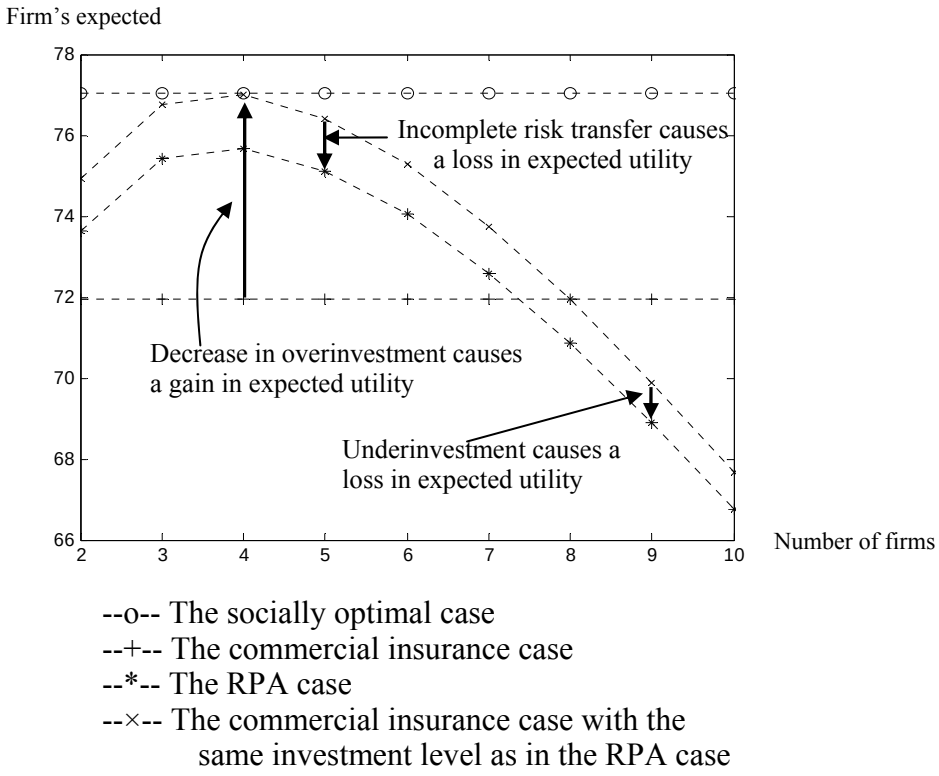


Figure 3.3: The Comparison of the Firm's Expected Utilities

Figure 3.3 further separates two countervailing forces of RPA, i.e., the incomplete risk transfer and the decreased security investment. In Figure 3.3, the "×" line represents a firm's expected utility if it uses commercial insurance but invests at the same level as it does when using RPA. The "+" line represents a firm's expected utility if it uses commercial insurance. Therefore, the difference between the "×" line and the "+" line reflects the difference in a firm's expected utility caused by the difference in security investment (not by the type of insurance, since the firm uses commercial insurance in both cases). Note that the decrease of security investment leads to a gain (a loss) in the

firm's expected utility in the range where $n \leq 8$ ($n > 8$). The "*" line represents the expected utility of firms if they use RPA. Therefore, the decrease from the "×" line to the "*" line reflects the loss in a firm's expected utility caused by incomplete risk transfer (the security investment levels in these two cases are equal). Note when $n \leq 7$ ($n > 7$), the gain from the lower security investment exceeds (does not exceed) the loss from incomplete risk transfer, and thus RPA is better (worse) than the commercial insurance market. In this regard, the size of the risk pool should be bounded.

The separation of two countervailing forces of RPA enables us to further investigate when RPA outperforms the commercial insurance market. Figure 4 illustrates that when competition is not intense enough (i.e., C=0.5), RPA never outperforms the commercial insurance market. With less intense competition, firms' overinvestment incentive is not large. When firms use RPA, the loss caused by the incomplete risk transfer always exceeds the gain caused by the decreased security investment. As a result, firms' expected utilities are always lower when using RPA.

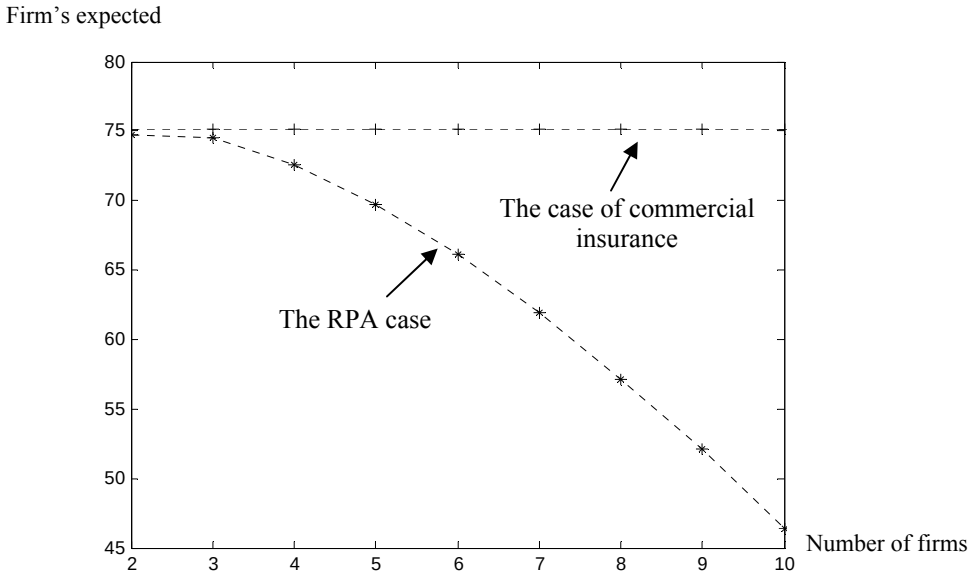


Figure 3.4: The Firm's Expected Utility When Competition is Not Intense

3.3.3 The Use of Multiple Risk Pools

Proposition 3.1 shows that firms' incentive to invest within a single risk pool decreases when the pool size increases. Consequently, using a large single risk pool may make firms worse off than using commercial insurance. When the number of firms is too large and the moral hazard problem is severe, firms need to control the size of the risk pool. Instead of setting up a single large pool, they can form multiple pools. We consider the following process of forming multiple risk pools. In the first stage, firms cooperatively decide how to set up pools (i.e., negotiate the pool size and the number of pools). In the second stage, firms non-cooperatively determine their security investments. Proposition 3.2 indicates that firms may form multiple pools when n is large enough. Let $m^* = \arg\max_m \Pi_P(m)$, where $\Pi_P(.)$ is defined in (3.2).

Proposition 3.2 *Suppose that the total number of firms, n, is sufficiently large and can be divided by m*. If* $\Pi_P(m^*) > \Pi_C$*, then firms set up multiple pools with a size of m*.*

Proposition 3.2 indicates the possibility of forming multiple pools. Later, we compare this case with the case in which firms can use RPA and also access the commercial insurance market. We show that when firms can use both RPA and commercial insurance, the industry of risk pooling tends to consolidate and firms tend to form only a single pool.

3.4 A HYBRID MODEL OF INSURANCE

The previous section shows that the moral hazard problem associated with RPA can resolve the overinvestment issue, but may also result in underinvestment. In this section, we consider the case where firms can use both RPA and commercial insurance to cover their risks. The sequence of the game is as follows. In stage 1, n firms cooperatively choose the amount of loss q covered by the risk pool. In stage 2, given q, firms noncooperatively choose their security investment x_i (i=1..n) and purchase

insurance with coverage I_i (i=1..n) in the commercial insurance market. Again, it is assumed that the commercial insurance market is mature. When firms can use both the risk pool and commercial insurance, firm i's expected utility is

$$\Pi_i = \mu_i \sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right) U\left(A - L + \frac{(n-1-k)}{n} q + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) + I_i - \mu_i I_i - x_i\right)$$
$$+ (1-\mu_{-i}) \sum_{k=0}^{n-1} b\left(k;(n-1),\mu\right) U\left(A - \frac{k}{n} q + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - \mu_i I_i - x_i\right)$$

Lemma 3.3 *When firms use both RPA and commercial insurance, I_i=L-q if q<L. That is, if the risk pool does not provide full coverage, firms use commercial insurance to cover all the residual risks.*

Lemma 3.3 characterizes the complementary relationship between RPA and commercial insurance. If firms do not want to retain all the risks within the risk pool, they will use commercial insurance to cover the residual risks. Thus, firm i's expected utility is

$$\Pi_i = \mu_i \sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right) U\left(A - \frac{(k+1)}{n} q + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - \mu_i (L-q) - x_i\right)$$
$$+ (1-\mu_i) \sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right) U\left(A - \frac{k}{n} q + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - \mu_i (L-q) - x_i\right)$$

Note that the mature commercial insurance market can completely absorb firms' risks. In contrast, firms retain part of the risks within the risk pool. Therefore, if firms want to be exposed to a lower level of risk within the risk pool, they can decrease their coverage in the risk pool and transfer residual risks to the commercial insurance market. The next question is: do firms always have an incentive to adopt RPA as a complement to the commercial insurance market?

Proposition 3.3 W*hen the competition effect of security investment exists (i.e., C>0), firms always have an incentive to set up a risk pool and allocate a positive amount of risks to the pool, i.e., q>0*

Proposition 3.3 generates an important implication. That is, as long as competition drives firms to overinvest in security, firms always have an incentive to set up a risk pool as a complement to commercial insurance. To understand this incentive, we derive the marginal effect of q on firm i's expected utility when q=0,

$$\frac{\partial \Pi_i}{\partial q}|_{q=0} = U'\left(A-\mu\left(x_i\right)L-x_i\right)\mu - U'\left(A-\mu\left(x_i\right)L-x_i\right)\left(\frac{1}{n}\mu_i + \frac{n-1}{n}\mu_{-i}\right) - U'\left(A-\mu\left(x_i\right)L-x_i\right)C\frac{\partial x_{-i}}{\partial q} \tag{3.4}$$

The first term of (3.4) represents the marginal benefit that firms obtain from the reduced insurance premium. In other words, when the coverage of the risk pool q increases, the insurance coverage I decreases and firms pay a lower premium μI to commercial insurers. The second term of (3.4) represents the marginal loss that firms incur from the increased risk exposure. In particular, $\frac{1}{n}\mu_i$ represents the marginal loss from an increase in firm i's own security breach probability, and $\frac{n-1}{n}\mu_{-i}$ represents the marginal loss from an increase in firm i's expected compensation to other firms. The third term of (3.4) represents the marginal impact of increased risk pool coverage on competition. Appendix shows that $\frac{\partial x_{-i}}{\partial q}|_{q=0} < 0$. That is, the rival firms invest less in security when q increases. It is worth remarking that the third term of (3.4) is positive, which means that RPA mitigates the adverse consequence of competition. As the first two terms cancel out in a symmetric equilibrium, the overall marginal impact of q on the firm's expected utility is positive (i.e., $\frac{\partial \Pi_i}{\partial q}|_{q=0} > 0$), and thus firms always have an incentive to set up a risk pool.

Proposition 3.4. *When firms can use both RPA and commercial insurance, they only form a single risk pool.*

The comparison between Proposition 3.2 and Proposition 3.4 generates another important implication. The combined use of commercial insurance and RPA leads to the

consolidation of risk pools. When firms only use RPA, the moral hazard problem restricts the size of the risk pool. Therefore, the consolidation of risk pools is difficult. When a mature commercial insurance market is available, firms can control the degree of moral hazard by allocating more risks to the commercial insurance market (i.e., decreasing the coverage of the risk pool). As a consequence, there will be no excessive moral hazard in a single risk pool and one risk pool is enough.

Next, we consider how firms allocate their risks between RPA and the commercial insurance market. We first illustrate a set of simulation results to show the amount of risk allocated to the risk pool (i.e., q) when n increases. Second, we analytically show an interesting result that firms' security investments and expected utilities approach the socially optimal levels when n approaches the infinite.

We still use the breach probability function $\mu(x)=e^{-x}$ and the utility function $U(x)=-x(20-x)$. Figure 3.5 illustrates the optimal amount of loss that firms would like to share in the risk pool. Generally speaking, the amount of loss shared in the risk pool decreases as the size of the risk pool increases (except for the range from n=2 to n=3). The reason is that when there are more members in a risk pool, the moral

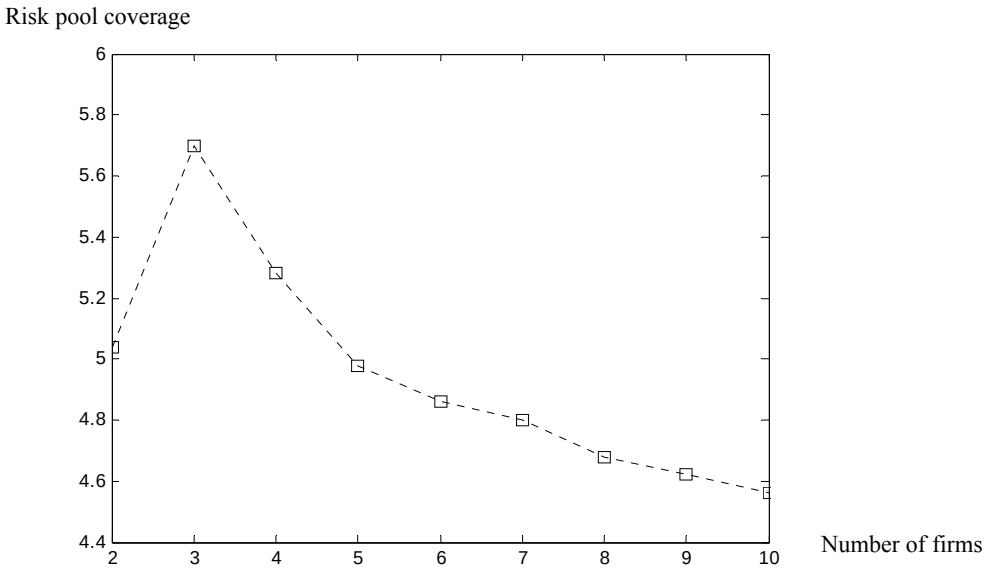


Figure 3.5: The Amount of Loss Covered by the Risk Pool

hazard problem is more severe and firms have less incentive to invest in security. As a consequence, when the risk pool becomes large, firms can choose to buy more insurance from the commercial insurance market and retain fewer risks in the risk pool. Note that firms share fewer risks when n=2 than when n=3. The lower level of coverage is due to the nature of the incomplete risk transfer associated with RPA. When n=2, the number of firms sharing risks is not large enough. If a small risk pool (with only two members) covers a large amount of risk, the amount of risk each member has to retain is large. Therefore, firms tend to decrease their coverage in the risk pool in order to reduce the risk retention.

Figure 3.6 shows firms' security investment in the case with both RPA and commercial insurance. As the number of firms increases, the security investment (the line with mark "□") keeps decreasing but never drops below the socially optimal level. In particular, the security investment approaches the socially optimal level from above. Unlike the case with only RPA, the hybrid model does not lead to security

underinvestment. The results imply that firms can alleviate the moral hazard problem associated with RPA by reducing their coverage in the risk pool and buying insurance from commercial insurers.

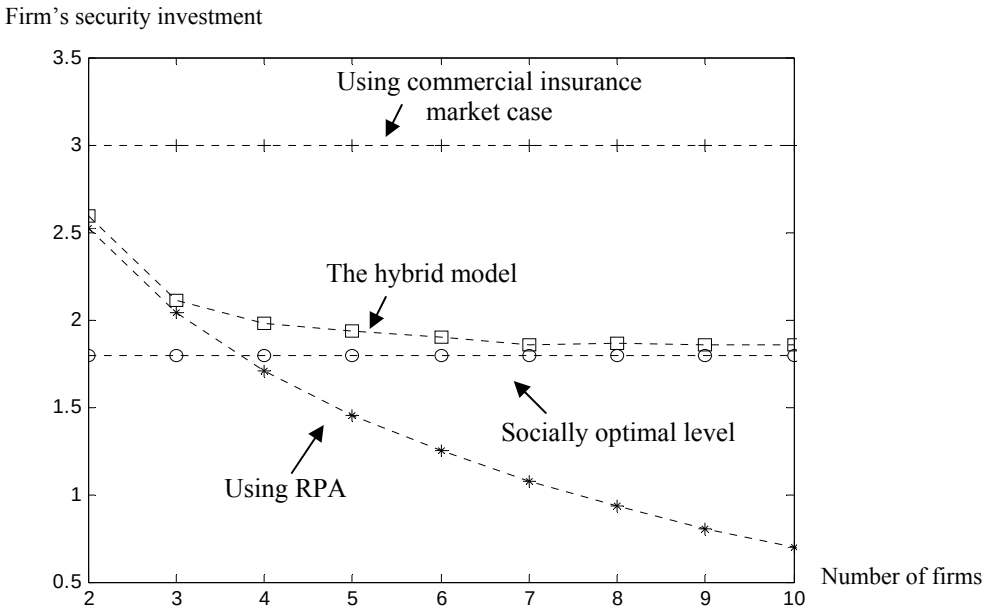


Figure 3.6: The Comparison between Firm's Security Investments in Different

Figure 3.7 compares the firm's expected utility in the hybrid model (the dot line with mark "□") with those in other cases. Note that in the hybrid model, the firm's expected utility increases and approaches the socially optimal level as *n* becomes large. In the case with only RPA, however, the firm's expected utility eventually decreases. A hybrid model can effectively leverage the moral hazard problem associated with RPA to mitigate firms' overinvestment incentive, without generating underinvestment.

Proposition 3.5 *When $n \to \infty$, firms' security investments and expected utilities approach the socially optimal levels.*

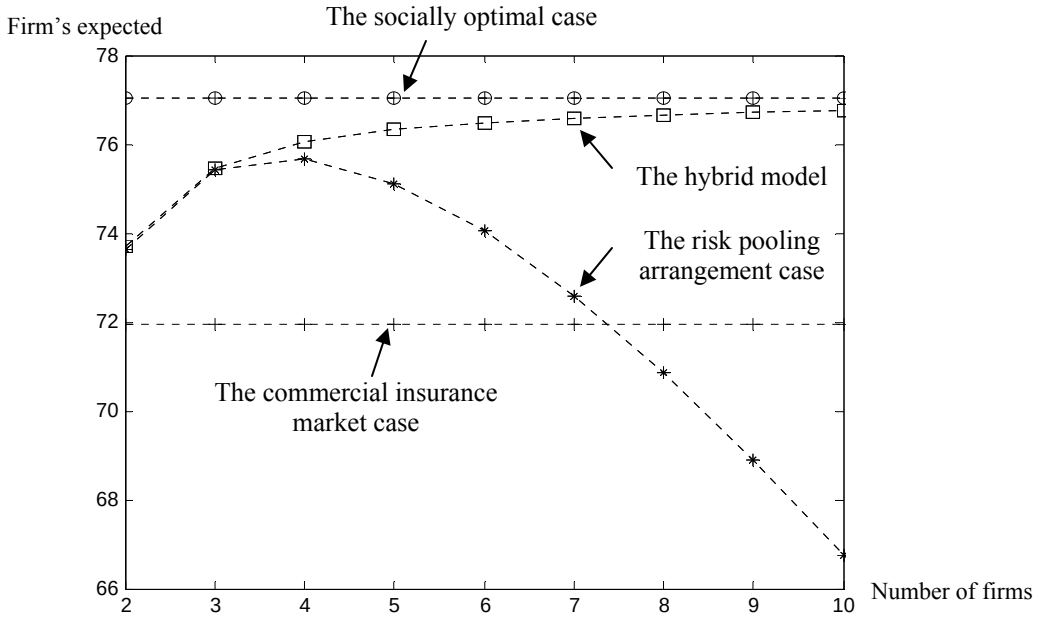


Figure 3.7: The Firm's Expected Utilities in the Hybrid Model

To understand Proposition 3.5, note that when n approaches the infinite, in a symmetric equilibrium, the law of large numbers implies that the expected number of firms with a security breach approaches $n\mu$. Therefore, the expected out-of-pocket compensation that a firm affords in the risk pool is $(n\mu \times q)/n = \mu q$, and a firm's expected utility approaches

$$U_i\left(A - \mu q - \mu_i\left(L - q\right) - x_i\right) \tag{3.5}$$

Expression (3.5) implies that in the extreme case where n approaches the infinite, firms essentially obtain a "full insurance equivalence" by paying a "total insurance premium" of $\mu q + \mu_i(L-q)$. Note that the premium $\mu_i(L-q)$ is paid to commercial insurers. μq can be understood as a "premium equivalence" paid within the risk pool. "Premium equivalence" is an aggregate compensation that firm i pays other firms suffering security losses, in exchange for a compensation from other firms when firm i itself suffers a security loss. Firms' security investment can only reduce the premium $\mu_i(L-q)$ paid to the

commercial insurer, but has no impact on the "premium equivalence" μq paid within the risk pool. The reason is that the "premium equivalence" of firm i is affected by other firms' security investments. Therefore, by adjusting q and allocating more risks to the risk pool, firms can effectively reduce the overinvestment incentive driven by competition. Moreover, a sufficiently large risk pool provides a "full insurance equivalence" and complete risk transfer. Firms can resolve the security overinvestment problem at no cost and achieve the socially optimal outcome.

3.5 EXTENSIONS

In this section, we extend our model to consider two relevant issues. First, we consider the overinvestment caused by the negative externality of security. Second, we relate our analysis of security overinvestment to the case of security underinvestment.

3.5.1 Negative Externality of Security Investment

The model so far concerns the security overinvestment driven by competition. However, the current model setup can be extended to study other types of security overinvestment, for example, the overinvestment caused by the negative externality of security risks. When there is a common pool of malicious hackers, for instance, it is very likely that the security investment by one firm will drive malicious hackers to target other firms and thus generate negative externality on other firms. In other words, the security investment increases the probability of security breaches on other firms while reducing the investing firm's own security risks.

Suppose that firm i's breach probability is $\mu\left(x_i + \left(x_i - \frac{\sum x_{-i}}{n-1}\right)\right)$. Note that firm i's breach probability is increasing in other firms' investment x_{-i}. This captures the adverse impact of other firms' investments on firm i's breach probability. Again, assume that $\mu'<$

0, $\mu''>0$, i.e., μ is convex. Thus, firm i's expected utility in the case with only commercial insurance can be represented as

$$\prod_i = \mu_i U\left(A - L + I_i - \mu_i I_i - x_i\right) + \left(1 - \mu_i\right) U\left(A - \mu_i I_i - x_i\right) \tag{3.6}$$

where $\mu_i = \mu\left(x_i + \left(x_i - \frac{\sum x_{-i}}{n-1}\right)\right)$. Appendix proves that firms will overinvest in this case. This is because firms tend to ignore the negative externality of their investments on other firms' security. Again, the commercial insurance market is insufficient to mitigate the overinvestment, since commercial insurance does not alter the negative externality of an individual firm's investment.

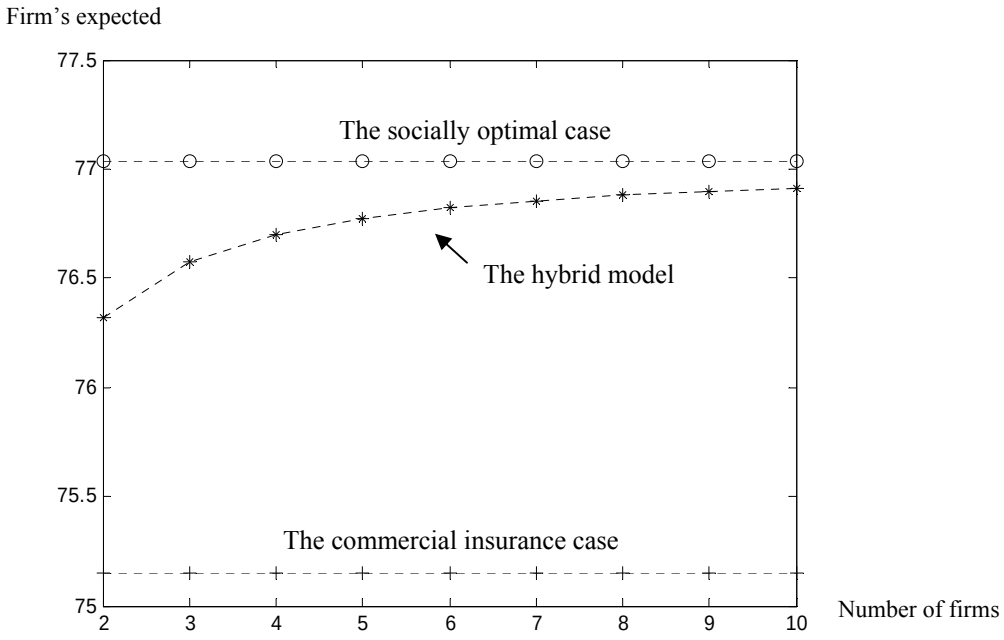


Figure 3.8: The Firm's Expected Utilities with Negative Externality

Similarly, if firms adopt RPA, they will decrease their security investment due to the moral hazard problem. We illustrate this intuition using a numerical analysis. Again, assume that the breach probability function is $\mu(x)=e^{-x}$, and the utility function is $U(x)=-$

x(20-x). Figure 3.8 illustrates how the hybrid model with both RPA and commercial insurance benefits firms. In Figure 3.8, the firm's expected utility in the case with both RPA and commercial insurance is always higher than that in the case with only commercial insurance. Moreover, as n increases, the firm's expected utility in the case with the hybrid model approaches that in the socially optimal case.

3.5.2 Security Underinvestment

Although the main issue examined in this paper is security overinvestment, our work can relate to the general consideration of the security underinvestment issue (i.e., firms lack incentive to invest sufficiently in security protection). It is worth remarking that although firms may underinvest at the aggregate level, they may still overinvest in certain security areas. When firms face security budget constraints, the overinvestment in certain security practices may exacerbate the underinvestment in other security practices. Empirical studies (e.g., Rowe and Gallaher 2006) indicate that in reality, many organizations actually face a fairly fixed budget in security and they can only maximize the overall level of security subject to a predetermined level of resources.

We extend our model to consider a scenario with multiple types of security risks. Suppose that firms can invest in two different types of security practices, x and y. The investment x has negative spillovers and the investment y has positive spillovers. $\mu(x_i)$ and $\eta\left(y_i + \frac{\Sigma_{-i} y_{-i}}{n-1}\right)$ capture the impact of security investments x and y on the firm's breach probability, respectively. We denote $\mu_i = \mu(x_i)$ and $\eta_i = \eta\left(y_i + \frac{\Sigma_{-i} y_{-i}}{n-1}\right)$. It is assumed that μ_i'<0, η_i'<0, μ_i">0, η_i">0. Then, firm i's expected utility is given as

$$\begin{aligned}\prod_i = {} & \mu_i\eta_i U\left(A - L_x - L_y + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) + I_{xi} + I_{yi} - \mu_i I_{xi} - \eta_i I_{yi} - x_i - y_i\right) \\ & + \mu_i(1-\eta_i)U\left(A - L_x + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) + I_{xi} - \mu_i I_{xi} - \eta_i I_{yi} - x_i - y_i\right) \\ & + (1-\mu_i)\eta_i U\left(A - L_y + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) + I_{yi} - \mu_i I_{xi} - \eta_i I_{yi} - x_i - y_i\right) \\ & + (1-\mu_i)(1-\eta_i)U\left(A + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - \mu_i I_{xi} - \eta_i I_{yi} - x_i - y_i\right)\end{aligned} \tag{3.7}$$

$$\text{s.t. } x_i + y_i \le B \tag{3.8}$$

The first (fourth) term in (3.7) represents the case when both (neither) a security breach associated with x and (or) a security breach associated with y occur (s). The second (third) term in (3.7) represents the case where only the security breach associated with x (y) occurs. Similar to the base model, the term $C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right)$ reflects the competitive effect of security investment x. The functional form $\mu\left(y_i + \frac{\sum_{-i} y_{-i}}{n-1}\right)$ reflects the positive externality of investment y. The more other firms invest in y, the less likely that firm i has a security breach. For example, if other firms invest more to prevent their computers from being hacked and taken as zombies, the probability that firm i suffers DDoS attack will be lower. Unlike the investment x, the investment y does not lead to any competitive advantage. For example, firms' investment in preventing their internal users from sending out viruses and email spam may not directly benefit the firms themselves.

Expression (3.8) represents the firm's budget constraint. In this analysis we focus on the relevant case where the budget constraint (3.8) is always binding. Therefore, firm i needs to balance its spending on different types of security investments.

Proposition 3.6 *In the symmetric equilibrium, when the budget constraint is binding, (a) firms overinvest in x and underinvest in y; (b) a firm's investment in y is decreasing in C. Firms invest less in y when C>0 than in the case when C=0.*

Note that when the budget constraint is binding, firm i's investments x_i and y_i satisfy $\frac{\partial \Pi_i}{\partial x_i} = \frac{\partial \Pi_i}{\partial y_i}$, i.e.,

$$U'(.)\left(-\mu_i' L + C - 1\right) = U'(.)\left(-\eta_i' L - 1\right) \tag{3.9}$$

In the first-best case, however, firm i's investments x_i and y_i should satisfy

$$U'(.)\left(-\mu_i' L - 1\right) = U'(.)\left(-\eta_i' L\left(1 + \frac{n-1}{n-1}\right) - 1\right) \tag{3.10}$$

The comparison between (3.9) and (3.10) indicates that firm i underinvests in y due to the interdependent nature of security risks (Kunreuther and Heal 2003; Ogut et al. 2005a; Gordon and Lucyshyn 2003; Varian 2004; Powell 2005). In other words, firm i ignores the impact of its investment y_i on reducing other firms' breach probabilities. Furthermore, compared to the C=0 case (i.e., the investment x has no competitive effect), the C>0 case (i.e., investment x has a positive competitive impact) leads to a smaller investment in y. The competition drives firms to allocate more resources to investment x, which exacerbates the problem of underinvestment in y.

Again, we use a numerical analysis to illustrate this result. Assuming μ(x)=η(x)=e-x, U(x)=-x(20-x), A=8, L=4, C=0.7, and the security investment budget is equal to 1.5, Figure 9 shows that firms' expected utilities are higher in the hybrid case.

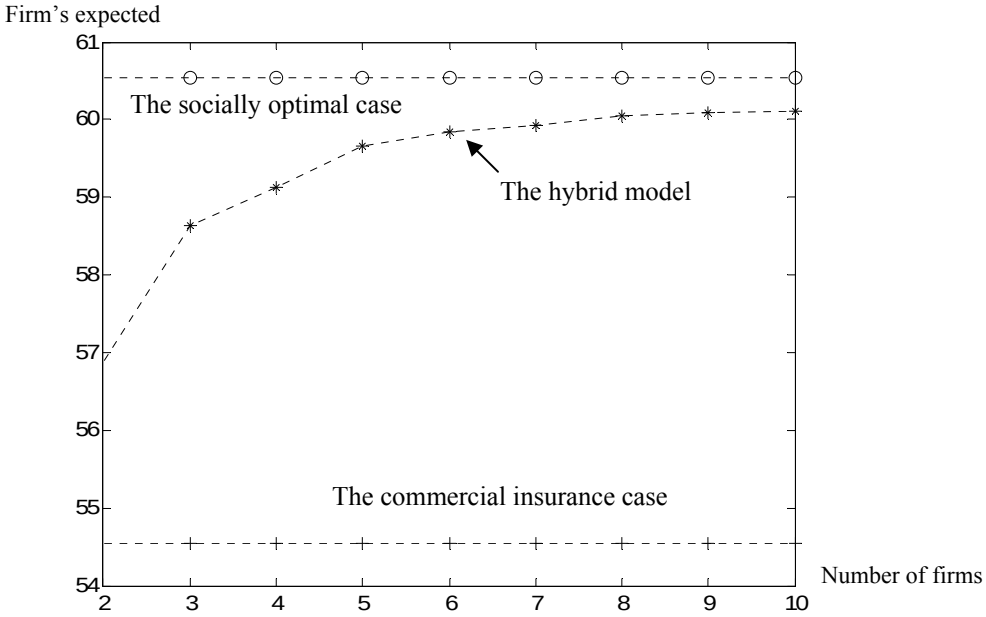


Figure 3.9: Firm's Expected Utilities Considering Security Underinvestment

3.6 DISCUSSION AND CONCLUSION

Compared with security underinvestment, security overinvestment is an under-researched issue. However, previous research emphasizes (Powell 2005) that addressing security overinvestment can be as important as addressing security underinvestment. Firms need to rationalize as well as optimize their security spending. In this paper we consider several potential reasons that can drive firms to overinvest in security, and we study a risk management approach, i.e., the risk pooling arrangement, as a solution to the overinvestment problem. The key insight is that RPA allows firms to leverage the moral hazard in team, a traditionally undesirable phenomenon, to mitigate the overinvestment incentive. This study of using RPA to resolve security overinvestment not only generates implications for security management, but also provides a new understanding of the role of mutual insurance. In this section, we discuss the managerial and policy implications generated by this analysis and provide directions for future research.

3.6.1 Managerial Implications

Security overinvestment can be caused by destructive competition, negative network externality, or managerial discretionary investment. Identifying and resolving security overinvestment can help firms rationalize their security spending and better manage competitive relationships. The appropriate use of a risk management solution, such as RPA, to resolve security overinvestment requires firms to effectively assess the characteristics of specific risks they are facing. For example, firms need to assess whether there are certain types of security risks that are likely to affect their competitive advantage and induce a rat race among competitors. Are certain types of security risks likely to generate negative externality to other competitors, customers, and suppliers? Are certain types of security risks (e.g., compliance-related security risks) likely to be of special concern for the managers and result in discretionary investment? To manage different types of security risks, the RPA may need different types of professional expertise in risk assessment, insurance policy development, incident handling, etc. The effective use of RPA can generate benefits for firms from both the outside and the inside. From the outside, RPA may help alleviate destructive competition among firms. The mitigation of overinvestment caused by negative network externality can also lead to a higher social surplus. Inside the firm, the accessibility of RPA can help managers prioritize security expenditures and better manage security risks.

This study also illustrates the benefit of using both RPA and commercial insurance. Firms need to recognize that these two risk management approaches are complements to, rather than substitutes for, each other. A traditional advantage of using RPA is the flexibility of mutual insurers to develop and issue more specialized insurance policies to its members. Firms can use RPA to cover those risks that are not covered by the commercial insurance market or are not suitable to be covered by the commercial

insurance market. For example, for those security problems with interdependent risks (Kunreuther and Heal 2003), RPA is not an optimal choice, since it may exaggerate the security underinvestment problem. Instead, firms can acquire policies from the commercial insurance market to cover them. Therefore, firms need to carefully study the characteristics of security risks and choose appropriate lines of insurance from different sources.

3.6.2 Policy Implications

This paper also generates important policy implications for the social planner regarding regulation of insurance industry. In general, the insurance industry is highly regulated, and the development of RPA is subject to these regulatory attitudes. For example, in many jurisdictions, certain lines of insurance can only be underwritten by an admitted commercial insurer but not by a mutual insurer. Other factors affecting the adoption of RPA include restrictions on the risk pool's underwriting terms, the deductibility of insurance premiums for corporate taxation purposes, and the risk pool's access to the reinsurance market. However, considering the potential of RPA to address the issue of security overinvestment and mitigate destructive competition, it is worthwhile for the social planner to reexamine and improve existing regulatory policies on mutual insurance to encourage the development of risk pooling arrangements.

3.6.3 Future Directions

This study can be extended in many directions. First, future research can consider the situation with heterogeneous firms. For example, the impacts of security investment on competitive advantages can be different for firms of different sizes. Large firms are more likely to form a RPA to mitigate intense competition. Moreover, the heterogeneity among firms may lead to the formation of different mutual organizations. Thus, an

analysis of heterogeneous firms can generate rich implications on the coexistence of miscellaneous mutual insurance organizations.

The second potential direction is to incorporate more organizational characteristics of RPA and further examine the impact of RPA on firms' security investments. Prior literature suggests that mutual insurance organizations are generally inferior in controlling the managerial discretion (e.g., Mayers and Smith 11981; Cummins and Weiss 1999). Therefore, mutual organizations are not suitable to provide certain lines of insurance that require a large amount of managerial discretion in pricing and underwriting. However, how the managerial discretion of the insurer affects the policyholder's security investment is not clear. Future research on how the mutual form of insurance impacts security investments may benefit by incorporating the consideration of managerial discretion.

The third potential direction for future research is to examine the competition between mutual insurance companies and other forms of insurance organizations: for example, how commercial insurers may develop more appealing policies in response to the competitive threats from the mutual insurers. Such research will improve the understanding of the interaction between different risk management solutions.

From the practitioner's point of view, it is worthwhile to consider which lines of insurance are appropriate for RPA and mutual organizations, and which lines of insurance are appropriate for the commercial insurance market. Studies in this direction can also benefit the social planner in developing policies to boost the growth of RPA and other ART solutions.

Chapter 4: How Fast to Patch? An Economic Analysis on the Information Role of Vendors' Patching Strategies

4.1 INTRODUCTION

The classic "lemon market" issue is common in the software market (Akerlof 1970). The complexity of software makes it difficult for consumers to learn of the software quality in a short period of time. Consequently, consumers' purchasing decisions are largely affected by the reputation of software products. Traditionally, reputation is developed and diffused through word-of-mouth, which has limited reach (Banerjee and Fudenberg 2004; Ellison and Fudenberg 1995). However, recent growth of the Internet accelerates information dissemination and expedites reputation building. Experts and consumers share their comments and opinions through various websites (e.g., CNET) and discussion forums (e.g., slashdot) on a global scale. Thus, maintaining and enhancing reputation naturally becomes one of the most important factors that vendors consider when making strategic decisions, including those regarding patch development and release.

Patching after software release is an integrated phase to the software development cycle. Although software vendors make significant investments, including effort and capital to improve the software development process, it is impossible to develop software without any vulnerability. Patching vulnerabilities improves the security level of a software product and hence influences its reputation. Given the increasing role that patching plays in the software market, strategic aspects of patching strategies need to be studied.

The reputation of a software product fluctuates following vulnerability and patch announcements. Publishing vulnerabilities increases security risks and hence degrades the

quality of the affected software. Vendors suffer a loss in reputation in the software market. By patching vulnerabilities, they improve the quality of the software and ease consumers' concerns about security risks, salvaging their damaged reputation. The earlier patches are released, the sooner the software's reputation is rebuilt. We refer to such a reputation effect of patching strategies as *the salvage effect of patching strategies*.

Patching, in addition to salvaging the reputation, has the potential to enhance the vendor-customer relationship. van Doorn and Verhoef (2007) find that critical incidents cause an update of customers' satisfaction regarding the providers. They suggest that firms should understand the impact of critical incidents on their customer relationship and distinguish the appropriate incidents which can be used as instruments to intensify their customer relationship. The incidents of vulnerability disclosure create opportunities for vendors to enhance customer satisfaction and boost their reputation. In particular, vendors may use patching strategies, a remedy to critical incidents, to eliminate the quality uncertainty and improve the reputation of their software.

Patching strategies can be used to eliminate information asymmetry because of the correlation between the software quality and the patching cost. It is very likely that the patching cost is negatively correlated to the software quality. That is, the better the quality of a software product, the less costly it is for the vendor to repair vulnerabilities quickly. A well-designed software product normally has better structure and is relatively easier to maintain (e.g., Unix). It is also possible that the patching cost is positively correlated to the software quality. That is, the better the quality of a software product, the more costly it is for the vendor to repair it quickly. For a software product with intricate functionality that customers appreciate, it may take more time and effort to repair its vulnerabilities (e.g., Microsoft Windows or Microsoft Office). The existence of a correlation enables vendors to leverage patching strategies to reveal hidden information,

the inherent quality of their software, to consumers and reestablish the reputation of their software. We refer to such a reputation effect of patching strategies as *the signaling effect of patching strategies*.

In this paper, we investigate the salvage effect and the signaling effect of patching strategies using a game-theoretic model. We consider a group of software vendors, each of which is licensing a software product to consumers in a finite time horizon. The software products can be of high-quality or low-quality. After the software is released, vulnerabilities associated with the software may be identified and vendors can repair vulnerabilities by developing patches. It is time-consuming and costly to develop a patch. And the more a vendor invests, the more quickly a patch can be released. We assume that the vulnerabilities of software with varying quality can be repaired at different costs. The quality and the patching cost are only known by vendors.

The reputation of a software product is the consumers' expectation of its quality and security level. Specifically, the reputation of a software product is higher if it is more likely that the software is of high-quality. Since vulnerabilities reduce the security level of a software product, the reputation of the software decreases if a vulnerability is disclosed. Reputation is also updated following the announcement of a patch. A patch can help vendors rebuild or even further improve the reputation of the software. However, it is also likely that patch release causes a reputation slump, as it signals low quality.

We use a signaling game to analyze the role of patching strategies (Lin et al 2005). Here, vendors are senders and consumers are receivers. In traditional signaling games, signals are always sent at the beginning of the game, and the specifications of actions by senders transfer valuable information. In our study, signals are sent out in the intermediate stage of the game. The timing of patch release becomes the signal since it is not equally costly and time-consuming for vendors to develop patches. Considering the

dynamics of the signaling process, we define a new belief profile for receivers. That is, receivers' beliefs at any time are determined by whether they have received any signals so far; hence the update of receivers' beliefs takes place over time. Using this belief profile, we are able to identify two types of separating outcomes in which vendors of software with different quality release patches for vulnerabilities at different times.

We first consider the case in which a vendor's repairing cost is negatively correlated to the quality of the software, that is, it is less costly to repair high-quality software than low-quality software. We identify *a normal separating equilibrium* in which vendors of high-quality software patch vulnerabilities faster than vendors of low-quality software. The salvage effect motivates all vendors to patch vulnerabilities as early as possible. Since it is less costly for vendors of high-quality software to release patches quickly, they can choose a release time earlier enough to prevent low-quality vendors from mimicking. Vendors of low-quality software cannot catch up with vendors of high-quality software and thus choose to release their patches at a later time. Therefore, vendors of high-quality software can leverage the patching release time to signal the quality of their software and obtain a premium in the software market. The signal effect strengthens the incentives for vendors with high-quality software to release patches quickly.

When it is more costly to patch high-quality software than low-quality software, we identify *an atypical separating equilibrium* in which vendors of low-quality software repair vulnerabilities faster than vendors of high-quality software. Vendors of low-quality software do not postpone the release time to mimic vendors of high-quality software because the loss in reputation for vendors of low-quality software from unpatched vulnerabilities exceeds the benefit from misrepresenting their products. The salvage effect dominates the signaling effect for vendors of low-quality software. Consequently,

they repair vulnerabilities earlier to salvage their declined reputation. For vendors of high-quality software, the release time must be late enough to intimidate those of low-quality software from mimicking. Although the salvage effect drives vendors of high-quality software to patch vulnerabilities quickly, the signaling effect weakens such incentives.

As software security becomes a major concern for organizations and individuals, issues of software vulnerability disclosure and patch release have attracted tremendous attention in academia and industry (Arora and Telang 2005; Arora et al. 2005; Arora et al. 2006b, 2006c; August and Tunca 2006a, 2006b; Cavusoglu et al. 2004, 2007; Arora et al. 2007; Choi et al. 2007). To the best of our knowledge, this study is the first one to consider the information role of patch strategies in a dynamic setting. We show that patching strategies can be leveraged to eliminate quality uncertainty. This study deepens the understanding of vendors' strategic patching decisions.

The remainder of the paper is organized as follows. In section 4.2, we review the literature on software vulnerability disclosure and patch release, and information asymmetry. In section 4.3, we outline the model setup. Section 4.4 analyzes the model and presents important results. Finally we conclude the paper.

4.2 LITERATURE REVIEW

Currently software vulnerabilities are disclosed though many sources, such as CERT/CC (Computer Security Incident Response Team/Coordination Center), iDefence, the Bugtraq mailing list, and Secunia. Researchers believe that disclosure causes a loss to vendors and hence expedites the process of patching development and release, and there is a stream of literature exploring various issues of software vulnerability disclosure and patch release. Cavusoglu et al. (2004) and Telang and Wattal (2005) have confirmed that vendors incur a significant loss from vulnerability disclosure. Using an event study, they

both find that vulnerability announcements or disclosures have a negative impact on the market value of the affected vendors. Arora et al. (2005) empirically show that the instant disclosure policy leads to earlier patch delivery. Arora et al. (2006b) empirically examine the competition effect of vulnerability disclosure and patch release, and find that an increase in the number of competitors lowers expected patching time. Malicious hackers' behavior has been studied as well. Arora et al. (2006c) indicate that hackers are able to infer software flaws from released patches and devise targeted attacks. Patching an already known vulnerability decreases the number of attacks, and patching an unknown vulnerability, surprisingly, increases the number of attacks.

There is a contentious debate on whether and how to disclose software vulnerabilities. Proponents of vulnerability disclosure claim that vulnerability disclosure enables users to take precautions, and pushes software vendors to release patches quickly. Opponents argue that vulnerability disclosure, especially without a patch, will expose users to security risks as crackers (black-hat hackers) can easily identify and exploit the vulnerabilities. Hence, researchers have been searching for the optimal disclosure policy. Arora et al. (2007) show that vendors always choose to patch less expeditiously than the socially optimal level, and the social planner can optimally shrink the protected period to push vendors to deliver patches in a timely manner. Cavusoglu et al. (2007) consider the characteristics of the vulnerability, cost structure of users, and vendor's incentives to develop a patch, and identify conditions under which full vendor disclosure, immediate public disclosure, or hybrid disclosure are socially optimal.

In addition to examining disclosure policies from the perspective of a social planner, researchers have also studied the incentives of independent third parties, users, and software vendors to publish vulnerabilities. Camp and Wolfram (2000) propose a market for vulnerabilities to enhance information security. Kannan and Telang (2005)

compare a CERT-type disclosure mechanism with a market-based disclosure mechanism that offers monetary rewards for finding vulnerabilities (e.g., iDefense). They demonstrate that the latter, if not regulated, always underperforms the former. Nizovtsev and Thursby (2006) investigate the rationality of an individual user's decision to disclose security information and indicate that full public disclosure of vulnerabilities can be socially optimal. Choi et al (2007) analyze vendors' strategic decisions on vulnerability disclosure and quality provision. Although researchers have called for more responsible disclosure procedures and proposed various disclosure policies, it is difficult to control or regulate the disclosure process given the unbounded freedom of the Internet. In this paper, we focus on the case where vulnerabilities are published instantly.

The connection between vendors' marketing strategies and patching strategies has been examined analytically. Arora et al. (2006a) show that a vendor has incentives to release a buggier product first and patch it later. August and Tunca (2006a) consider users' patching costs and negative network security externalities, and derive the optimal patching policies from the perspectives of a social planner and a software vendor. August and Tunca (2006b) explore the impact of patch policies on software piracy. They identify conditions under which software vendors should restrict unlicensed users from applying security patches. Our paper focuses on the information role of patching strategies. In particular, we illustrate how vendors can leverage patching strategies to eliminate information asymmetry.

Reputation has been recognized as a valuable asset which generates higher future sales and profitability (Wilson 1985). It becomes an important factor in vendors' decision making processes. Weigelt and Camerer (1988) review game-theoretic models on reputation-building and apply them in various corporate environments. Werbel and Wortman (2000)'s study suggests that companies may strategically use corporate

philanthropy to remedy negative social reputation. However, Rhee and Haunschild (2006) found that reputation could be a disadvantage. They empirically test how firms' reputation affects market reactions to product defects and find that highly reputed firms are punished more heavily for their product recalls. Recently online reputation systems have been widely used in the electronic trading environment, such as online auction sites (e.g., eBay and eLance), online shopping search engines (e.g., BizRate and Pricegrabber), and online forum (e.g., Slashdot). The Internet accelerates information dissemination and magnifies the reputation effect to a global scale. This paper studies vendors' patching strategies and investigates two reputation effects, the salvage effect and the signaling effect, in a dynamic setting.

Our work also relates to the literature on information asymmetry. Akerlof (1970) indicates that when information is asymmetric between buyers and sellers in the marketplace, low-quality products may drive high-quality products out of the market. Signaling games have been widely adopted to study adverse selection issues (Spence 1973; Cho and Kreps 1987; Lin et al 2005; Mailath 1987; Zhao et al. 2006). All of the models above share the common characteristics that players with private information send out informative signals at the beginning of the game. In our paper, signals are sent at the intermediate stage of the game. Specifically the timing of actions is the signal.

4.3 MODEL

We consider a group of software vendors who are licensing software products to consumers in a finite horizon T. Vendors can be one of two types, {high,low}. Vendors differ in the quality of software products that they are licensing. Specifically, the quality of the software offered by a high-type vendor is higher than that by a low-type vendor. We use r_i to denote the software quality and $r_h > r_l$. A vendor's type (the quality of its software product) is only known by the vendor itself, but the distribution of types is

common knowledge. We assume $\Pr(r = r_h) = \delta$ and $\Pr(r = r_l) = 1 - \delta$. The expected quality of the software is $r = \delta r_h + (1-\delta) r_l$.

At the beginning of the game, a vulnerability that is associated with all of the software is discovered and published. Malicious hackers may devise attacks targeting the vulnerability, and the security risk for all of the software will increase. Consequently, the quality of the software will drop. $\hat{r}_i$ is used to denote the quality of a software product with an unpatched vulnerability and $\hat{r}_i < r_i$. The expected quality of the software with an unpatched vulnerability is $\hat{r} = \delta \hat{r}_h + (1-\delta)\hat{r}_l$. It is assumed that $r_h > r_l > \hat{r}_h > \hat{r}_l$ given that the vulnerability is critical.

Vendors can repair the vulnerability at a cost. They make a one-time decision on when to release patches. s is used to denote the release time. We assume that the patch release time is deterministic. A vendor with type i has to invest $C_i(s)$ in order to release the patch at time $s \in [0, T]$. In order to release a patch early, vendors must heavily invest in the patch development. We assume $C_i(s)$ is decreasing and convex: $C_i'(s) < 0, C_i''(s) > 0$. s also characterizes the patching speed. The smaller s is, the faster the vendor repairs the vulnerability. Without loss of generality, we assume $C_i(s) = \frac{k_i}{s}$. It is assumed that the patch can completely repair the vulnerability. Thus, the quality of a software product after patching is r_i.

We assume that there is a constant flow of new customers with the normalized size 1 at any time. Since consumers do not know the quality of the software, their willingness to pay (WTP) is determined by the reputation of the software. For simplicity, we assume that the WTP is equal to the reputation. We define the reputation of a software product as its expected quality. If consumers do not know the quality of software products, the reputation of a software product without any vulnerability is r and of a

software product with an unpatched vulnerability is $\hat{r}$. When consumers know the quality of software products, the reputation of a software product is its quality.

4.4 ANALYSIS AND RESULTS

4.4.1 Base Analysis

We first analyze how the reputation affects the patch release time. We denote the reputation of a software product after a vulnerability is disclosed but before a patch is released as r_1 and the reputation after a patch is released as r_2. The profit of a vendor with type i, $i \in \{h,l\}$, can be represented as:

$$\int_0^s r_1\,dt + \int_s^T r_2\,dt - C_i(s) = r_2 T - (r_2 - r_1)s - C_i(s)$$

FOC is

$$r_2 - r_1 = -C_i'(s)$$

Let $C_i(s) = \frac{k_i}{s}$ and $T = 1$.

$$s_i^b = \sqrt{\frac{k_i}{r_2 - r_1}} \tag{4.1}$$

$$\pi_i^b = r_2 - 2\sqrt{k_i(r_2 - r_1)} \tag{4.2}$$

The reputation of the affected software declines after a vulnerability is disclosed. Consumers are concerned about security risks and less willing to pay for the vulnerable software. Venders have an incentive to repair the vulnerability to rebuild their reputation and increase their profitability. Vendors' patching decisions are determined by the patching cost and the difference between r_2 and r_1. In particular, the more costly for a vendor to patch a vulnerability, the later the vendor releases a patch. The more the reputation can be increased by patching, the earlier the vendor releases a patch.

From equation, (4.1) and (4.2), we can obtain the release time and the profit for a vendor under two information structures, complete information and partially incomplete information.

Complete Information: If consumers always know the quality of the software, $r_1 = \hat{r}_i$ and $r_2 = r_i$, $i \in \{h,l\}$. The release time and profit of a vendor with type i are as follows.

$$s_i^c = \sqrt{\frac{k_i}{r_i - \hat{r}_i}}$$

$$\pi_i^c = r_i - 2\sqrt{k_i(r_i - \hat{r}_i)}$$

Partially Incomplete Information: If consumers know the quality of the software only after the vendor releases a patch, $r_1 = \hat{r}$ and $r_2 = r_i$, $i \in \{h,l\}$. The release time and profit of a vendor with type i are as follows.

$$s_i^p = \sqrt{\frac{k_i}{r_i - \hat{r}}}$$

$$\pi_i^p = r_i - 2\sqrt{k_i(r_i - \hat{r})}$$

4.4.2 Asymmetric Information

When consumers do not know the quality of a software product, their WTP is determined by the reputation of the software. Since high-type vendors and low-type vendors initially share the same reputation, they have the same instantaneous revenue at the early stage of the game. It is not difficult to see that high-type vendors lose and low-type vendors benefit from information asymmetry. Vendors' heterogeneous costs to repair vulnerabilities enable them to disclose valuable information through their patching strategies. In this paper, we are interested in equilibria in which high-type vendors and low-type vendors choose different release times. Put differently, vendors of different types repair vulnerabilities at different speeds.

Different from traditional signaling games where informative actions are taken and signals are sent at the beginning of the game, the signal in this paper is generated in the intermediate stage. In fact, the timing of actions is actually the signal. The reputation of a software product at any time t is determined by the signal-whether a patch has been released by t. We use A_t to represent the signal. $A_t = 1$ represents the event that a patch has been released by the time t and $A_t = 0$ represents the event that no patch has been released by the time t. $\Pr_t(h \mid A_t)$ denotes consumers' belief that a vendor is high-type at time t given the signal A_t. The corresponding reputation of the software product is $\Pr_t(h \mid A_t)\hat{r}_h + (1 - \Pr_t(h \mid A_t))\hat{r}_l$ if $A_t = 0$ or $\Pr_t(h \mid A_t)r_h + (1 - \Pr_t(h \mid A_t))r_l$ if $A_t = 1$. s^- represents the time which is infinitely close to s. In this study, we define two types of separating equilibria.

Definition 1: *We define a pure-strategy normal separating equilibrium as* $\left\{(s_h, s_l), s_h < s_l, \Pr_{t\in[0,\, s_h)}(h \mid A_t = 0) = \delta, \Pr_{t\in[0,\, s_h]}(h \mid A_t = 1) = 1, \Pr_{t\in[s_h,\, T]}(h \mid A_{s_h} = 0) = 0\right\}$.

In a pure-strategy normal separating equilibrium, high-type vendors release patches earlier than low-type vendors: $s_h < s_l$. At any time t before s_h, if no patch has yet been released by a vendor, consumers believe that the vendor is of high-type with probability δ. At any time t no later than s_h, if a vendor has released a patch, consumers believe that it is of high-type. At any time t no earlier than s_h, if no patch has been released by a vendor by the time s_h, consumers believe that the vendor is of low type. The belief update has the characteristic that the earlier a vendor releases a patch, the more likely it is of high-type. The reputation of a software product evolves over time as Figure 4.1 shows. Figure 4.1 (a) illustrates how the reputation of the software product evolves if a patch is released before s_h. Figure 4.1(b) illustrates the evolution of the reputation if a patch is released after s_h.

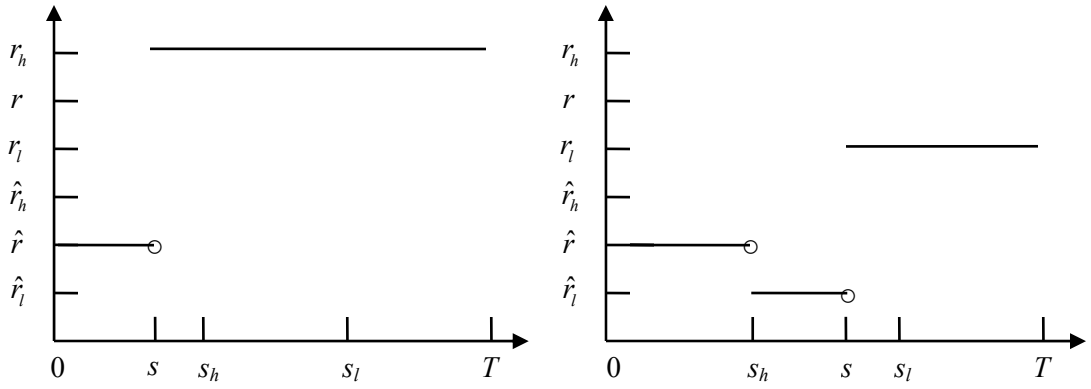


Figure 4.1 Vendors' Reputation in a Pure-Strategy Normal Separating Equilibrium

Definition 2: *We define a pure-strategy atypical separating equilibrium as* $\left\{(s_l, s_h), s_l < s_h, \Pr_{t\in[0,s_l')}(h \mid A_t = 0) = \delta, \Pr_{t\in[s_l',s_h)}(h \mid A_t = 0) = 1, \Pr_{t\in[0,s_h)}(h \mid A_t = 1) = 0, \right.$ $\left. \Pr_{t\in[s_h,T]}\left(h \mid A_{(s_h)^-} = 0\right) = 1\right\}$.

In a pure-strategy atypical equilibrium, low-type vendors release patches earlier than high-type vendors: $s_l < s_h$. At any time t before s_l', if no patch has been released, consumers believe that the vendor is of high-type with probability δ. At any time t before s_h, if a vendor has released a patch, consumers believe that it is of low-type. At any time no earlier than s_l' but before s_h, if no patch has yet been released, consumers believe that the vendor is of high-type. At any time no earlier than s_h, if a vendor has not yet released a patch by the time t, which is infinitely close to s_h, consumers believe that the vendor is of high-type. Different from the normal separating equilibrium, the later a vendors releases a patch, the more likely that it is of high-type. The reputation of a software product evolves over time as Figure 4.2 shows. Figure 4.2(a) illustrates how the reputation of the software product evolves if a patch is released before s_l'. Figure 4.2(b)

illustrates the evolution of the reputation if a patch is released between $s_l^{'}$ and s_h. Figure 4.2(c) illustrates the evolution of the reputation if a patch is released after s_h.

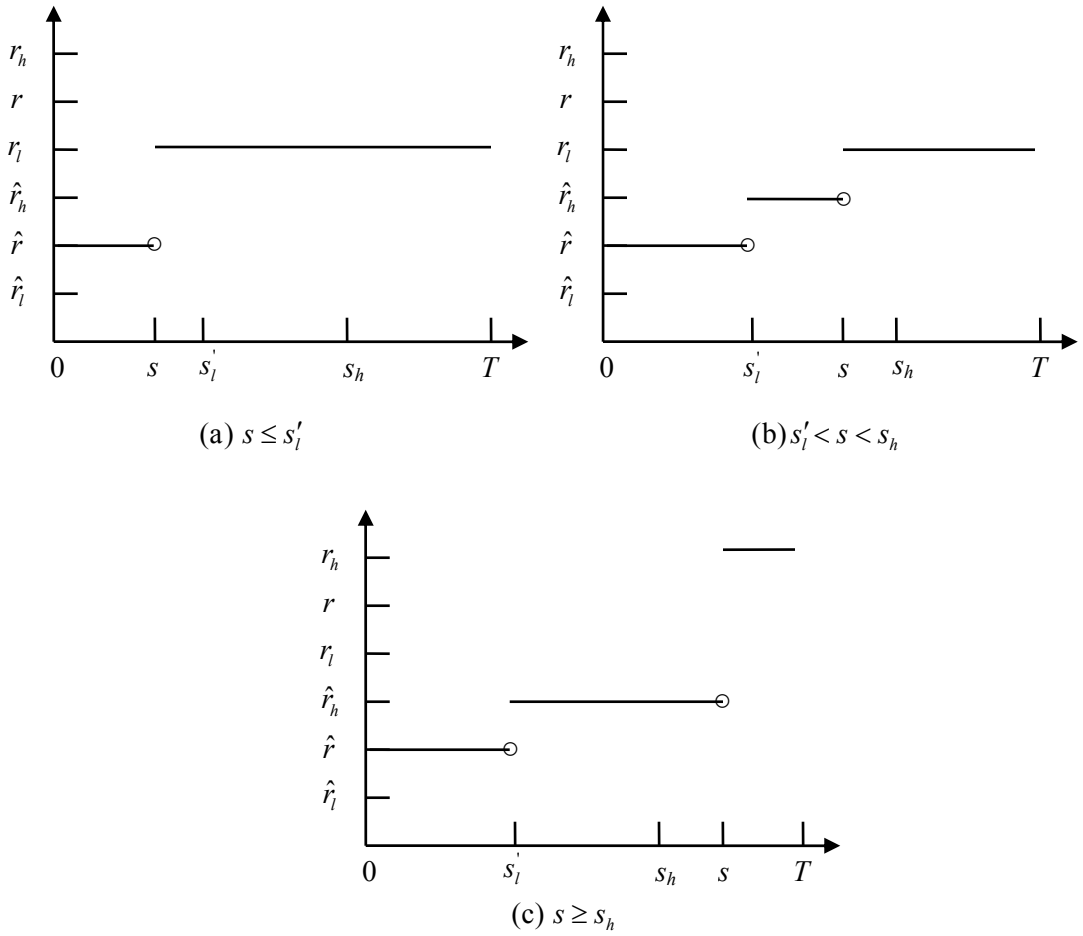


Figure 4.2 Vendors' Reputation in a Pure-Strategy Atypical Separating Equilibrium

4.4.3 Normal Separating Equilibrium

We first consider the case in which high-type vendors have a lower patching cost than low-type vendors. That is, $k_h < k_l$. Suppose that there is a normal separating equilibrium,

$$\left\{\left(s_h, s_l\right), s_h < s_l, \Pr_{t\in[0,s_h)}\left(h \mid A_t = 0\right) = \delta, \Pr_{t\in[0,s_h]}\left(h \mid A_t = 1\right) = 1, \Pr_{t\in[s_h,T]}\left(h \mid A_{s_h^n} = 0\right) = 0\right\}. \quad \text{A}$$

low-type vendor's profit function can be represented as

$$\int_0^{s_h} \hat{r}dt + \int_{s_h}^{s} \hat{r}_l dt + \int_s^T r_l dt - C_l\left(s\right) \tag{4.3}$$

$$= \hat{r}s_h - \hat{r}_l s_h + r_l - \left(r_l - \hat{r}_l\right)s - \frac{k_l}{s}$$

At any time before the equilibrium release time for high-type vendors, s_h, the reputation of a software product is $\hat{r}$, which is the expected quality of the software with an unpatched vulnerability. The first integration in (4.3) represents the total revenue that a low-type vendor makes before s_h. At any time after s_h, the type of the vendor has been revealed as low-type. Before the vendor releases a patch, the reputation of the software is $\hat{r}_l$, and the second integration represents the vendor's total revenue between s_h and s. After the vendor releases a patch, the reputation of the software is recovered to r_l, and the third integration represents the vendor's total revenue after s. And the last term is the patching cost.

Using FOC, we can obtain the equilibrium release time and the profit for a low-type vendor:

$$s_l = s_l^c = \sqrt{\frac{k_l}{r_l - \hat{r}_l}}$$

$$\pi_l = \left(\hat{r} - \hat{r}_l\right)s_h + r_l - 2\sqrt{k_l\left(r_l - \hat{r}_l\right)} \tag{4.4}$$

In the normal separating equilibrium, low-type vendors choose the release time that they will choose in the complete information case. However, they make a higher profit than they do in the complete information case. The first two terms of equation (4.4) can be rewritten as $\delta\left(\hat{r}_h - \hat{r}_l\right)s_h$, which is greater than zero. This result is different from the traditional signaling game, in which low-type players obtain the same payoffs as they do in the complete information case. The surplus comes from the fact that it takes time

for high-type vendors to produce signals. In the dynamic setting, signals are sent in the intermediate stage of the game. Low-type vendors benefit from information asymmetry at the early stage of the game.

A high-type vendor's profit function can be represented as

$$\int_0^{s_h} \hat{r}dt + \int_{s_h}^{T} r_h dt - C_h(s_h) \tag{4.5}$$
$$= r_h - (r_h - \hat{r})s_h - \frac{k_h}{s_h}$$

Before a high-type vendor releases a patch, the reputation of its software is $\hat{r}$, and the first integration of (4.5) is the vendor's total revenue before s_h. After it releases a patch, the reputation of its software is r_h, and the second integration is its total revenue after s_h. The last term is the patching cost. Proposition 4.1 characterizes the pure-strategy normal separating equilibrium.

Proposition 4.1

1. *A pure-strategy normal separating equilibrium exists if*
$$\sqrt{r_h - r_l}\left(\sqrt{(r_h - r_l) + 4\sqrt{k_l}\left(\sqrt{r_l - \hat{r}_l} - \sqrt{k_l}\right)} - \sqrt{(r_h - r_l) + 4\sqrt{k_h}\left(\sqrt{r_l - \hat{r}_l} - \sqrt{k_h}\right)}\right)$$
$$\leq 2\sqrt{r_l - \hat{r}_l}\left(\sqrt{k_l} - \sqrt{k_h}\right)$$

2. $\{(s_h, s_l), s_h < s_l, \Pr_{t\in[0,s_h)}(h \mid A_t = 0) = \delta, \Pr_{t\in[0,s_h]}(h \mid A_t = 1) = 1, \Pr_{t\in[s_h,T]}(h \mid A_{s_h^n} = 0) = 0\}$
is the pure-strategy normal separating equilibrium.

$s_l = s_l^c = \sqrt{\frac{k_h}{r_l - \hat{r}_l}}$.

If $s_h^p = \sqrt{\frac{k_h}{r_h - \hat{r}}} \in \left[s_{hl}^{n*}, \min\{s_h^{n*}, s_{hl}^{n**}\}\right]$, $s_h = s_h^p$. If $s_h^p > \min\{s_h^{n*}, s_{hl}^{n**}\}$,

$s_h = \min\{s_h^{n*}, s_{hl}^{n**}\}$.

$s_h^{n*} = \frac{r_h - r_l + 2\sqrt{k_l(r_l - \hat{r}_l)} - \sqrt{\left(r_h - r_l + 2\sqrt{k_l(r_l - \hat{r}_l)}\right)^2 - 4k_l(r_h - \hat{r}_l)}}{2(r_h - \hat{r}_l)}$.

$s_{hl}^{n*} = \frac{r_h - r_l + 2\sqrt{k_h(r_l - \hat{r}_l)} - \sqrt{\left(r_h - r_l + 2\sqrt{k_h(r_l - \hat{r}_l)}\right)^2 - 4k_h(r_h - \hat{r}_l)}}{2(r_h - \hat{r}_l)}$.

$s_{hl}^{n**} = \frac{r_h - r_l + 2\sqrt{k_h(r_l - \hat{r}_l)} + \sqrt{\left(r_h - r_l + 2\sqrt{k_h(r_l - \hat{r}_l)}\right)^2 - 4k_h(r_h - \hat{r}_l)}}{2(r_h - \hat{r}_l)}$.

Proposition 4.1 gives the condition under which a pure-strategy normal separating equilibrium exists. In the normal separating equilibrium, high-type vendors always choose to release a patch earlier than low-type vendors. The analysis shows that high-type vendors' release time must be earlier than s_h^{n*} to prevent low-type vendors from mimicking. In addition, it must fall in the range $\left[s_{hl}^{n*}, s_{hl}^{n**}\right]$ to guarantee that high-type vendors have incentive to differentiate themselves from low-type vendors. Thus, the equilibrium release time for high-type vendors must be in the range $\left[s_{hl}^{n*}, \min\{s_h^{n*}, s_{hl}^{n**}\}\right]$. Overall, the sufficient and necessary condition for the existence of a normal separating equilibrium is $s_{hl}^{n*} < s_h^{n*}$.

The earlier a vendor releases a patch, the more likely the vendor is of high-type. If the optimal release time for high-type vendors in the partially incomplete information case, s_h^p, is early enough to prevent low-type vendors from mimicking, high-type vendors will choose it as the equilibrium release time. Otherwise, high-type vendors will choose the marginal release time, $\min\{s_h^{n*}, s_{hl}^{n**}\}$. In the normal separating equilibrium, low-type vendors' types are completely revealed after the equilibrium patch release time for high-type vendors. Therefore, low-type vendors choose the patch release time that they will choose in the complete information case, s_l^c.

The salvage effect motivates vendors to release patches in a timely manner for their reputation and profitability. The signaling effect provides high-type vendors additional incentives to patch the vulnerability quickly. The low patching cost enables high-type vendors to release patches for the vulnerability earlier and signal their types. Although the signaling effect drives low-type vendors to mimic high-type vendors, it is not worthwhile for them to do so because of its high patching cost. Low-type vendors patch the vulnerability to salvage their damaged reputation.

4.4.4 Atypical Separating Equilibrium

We then consider the case in which low-type vendors' patching cost is lower than that of high-type vendors. That is, $k_l < k_h$. We are interested in the existence of an atypical separating equilibrium in which low-type vendors choose to release patches earlier than high-type vendors. Suppose that there is a pure-strategy atypical separating equilibrium

$$\left\{(s_l, s_h), s_l < s_h, \Pr_{t\in[0,s_l')}(h \mid A_t = 0) = \delta, \Pr_{t\in[s_l', s_h)}(h \mid A_t = 0) = 1, \Pr_{t\in[0,s_h)}(h \mid A_t = 1) = 0,\right.$$

$$\left.\Pr_{t\in[s_h,T]}\left(h \mid A_{(s_h)^-} = 0\right) = 1\right\}.$$

A low-type vendors' profit function can be represented as

$$\begin{aligned} &\int_0^s \hat{r}dt + \int_s^T r_l dt - C_l(s) \\ &= r_l - (r_l - \hat{r})s - C_l(s) \end{aligned} \tag{4.6}$$

The structure of (4.6) is similar to that of (4.5). Before a low-type vendor releases a patch, the reputation of its software product is $\hat{r}$, and the first integration of (4.6) represents the vendor's total revenue before s. After it releases a patch, the reputation of its software becomes r_l, and the second integration is its total revenue after s. The last term is the patching cost.

A high-type vendor's profit function can be represented as

$$\begin{aligned} &\int_0^{s_l'} \hat{r}dt + \int_{s_l'}^{s_h} \hat{r}_h dt + \int_{s_h}^T r_h dt - C_h(s_h) \\ &= r_h - (\hat{r}_h - \hat{r})s_l' - (r_h - \hat{r}_h)s_h - \frac{k_h}{s_h} \end{aligned} \tag{4.7}$$

The structure of (4.7) is similar to that of (4.3). Before the marginal time s_l', the reputation of its software product is $\hat{r}$, and the first integration of (4.7) represents the vendor's total revenue before s_l'. After s_l' but before its equilibrium release time s_h, the reputation of its software becomes $\hat{r}_h$ and the second integration represents the vendor's total revenue during that period. After the equilibrium release time s_h, the reputation of

its software becomes r_h. And the third integration represents the vendor's total revenue after s_h.

Using the profit functions we define above, we examine the incentives for high-type and low-type vendors. Our result shows that there is no pure-strategy atypical separating equilibrium.

Proposition 4.2*: There is no pure-strategy atypical separating equilibrium.*

Next we search for a mixed-strategy equilibrium. We define a mixed-strategy separating equilibrium in Definition 3.

Definition 3*: We define a mixed-strategy atypical separating equilibrium as*

$$\left\{(\sigma_l, s_h), \sigma_l \in \left[s_l^{'}, s_l^{''}\right], s_l^{''} < s_h, \Pr_{t\in\left[0,s_l^{'}\right)}\left(h \mid A_t = 0\right) = \delta, \Pr_{t\in\left[s_l^{'}, s_l^{''}\right]}\left(h \mid A_t = 0\right) = \delta(t),\right.$$

$$\left.\Pr_{t\in\left(s_l^{''}, s_h\right\}}\left(h \mid A_t = 0\right) = 1, \Pr_{t\in[0,s_h)}\left(h \mid A_t = 1\right) = 0, \Pr_{t\in[s_h,T]}\left(h \mid A_{(s_h)^-} = 0\right) = 1\right\}.$$

Low-type vendors choose the release time following the distribution function σ_l on $\left[s_l^{'}, s_l^{''}\right]$. At any time in the range $\left[s_l^{'}, s_l^{''}\right]$, if a vendor has not yet released a patch, consumers believe that it is of high-type with probability $\delta(t)$. The reputation of a software product evolves over time as Figure 4.3 shows. Figure 4.3(a) illustrates how the reputation of the software product evolves if a patch is released before $s_l^{'}$. Figure 4.2(b) illustrates the evolution of the reputation if a patch is released between $s_l^{'}$ and $s_l^{"}$. Figure 4.2(c) illustrates the evolution of the reputation if a patch is released between $s_l^{"}$ and s_h. Figure 4.2(d) illustrates the evolution of the reputation if a patch is released after s_h.

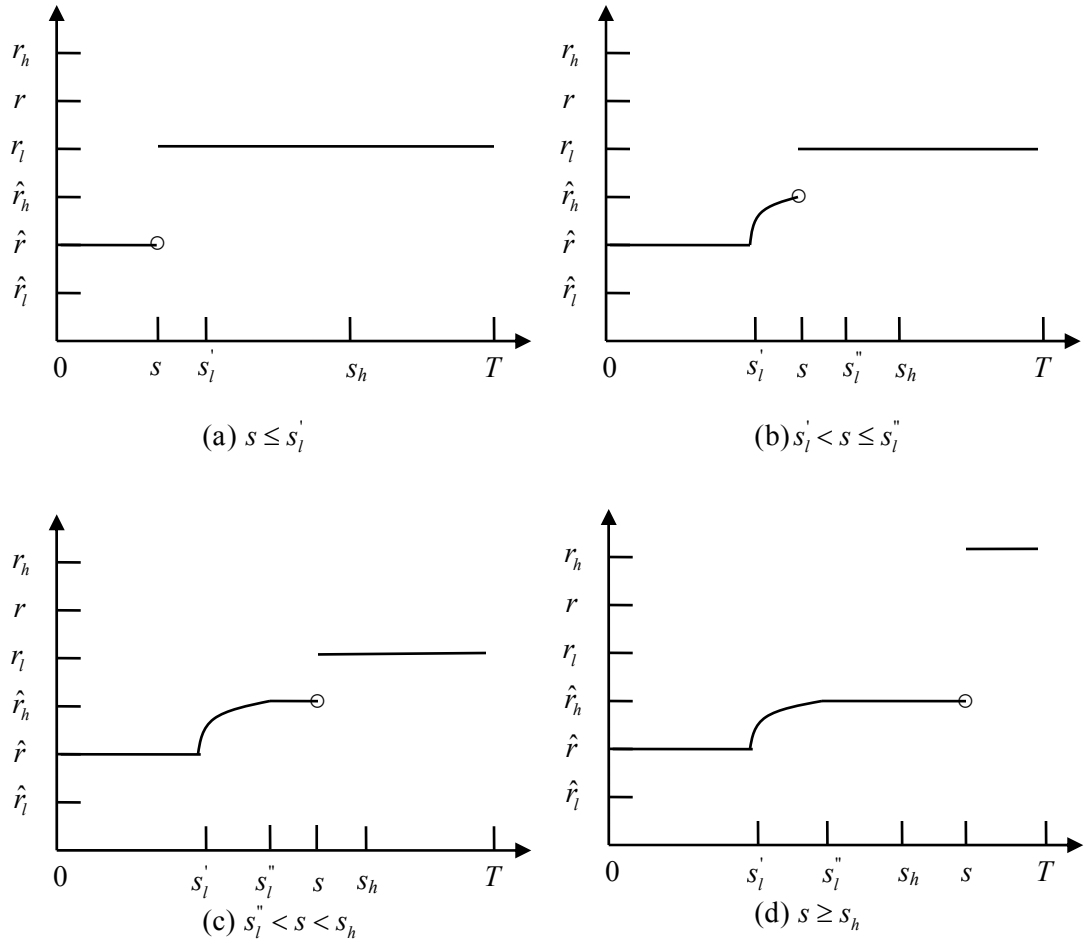


Figure 4.3 Vendors' Reputation in a Mixed-Strategy Atypical Separating Equilibrium

Since delaying patch release increases consumers' expectation of the vendor being of high-quality, $\delta(t)$ is an increasing function of t. It is worth noticing that high-type vendors will never randomize the release time in the separating equilibrium. An early release will reduce customers' expectation of the software quality and will also incur a higher cost.

In a mixed-strategy equilibrium, low-type vendors make an equal profit on $\left[s_l^{'}, s_l^{''}\right]$. The profit function for a low-type vendor can be represented as

$$\int_0^{s_t^{'}} \hat{r} d\tau + \int_{s_t^{'}}^{t} r(\tau) d\tau + \int_t^1 r_l d\tau - \frac{k_l}{t} = Const, t \in \left[s_l^{'}, s_l^{''}\right]$$

where $r(t)=\delta(t)\hat{r}_h+(1-\delta(t))\hat{r}_l$.

For a high-type vendor, its profit function can be represented as
$\int_0^{s_l'}\hat{r}dt+\int_{s_l'}^{s_l''}r(t)dt+\int_{s_l''}^{s_h}\hat{r}_h dt+\int_{s_h}^{T}r_h dt-C_h(s_h)$

Proposition 4.3 characterizes the mixed-strategy separating equilibrium.

Proposition 4.3:

1. *A mixed-strategy atypical separating equilibrium exists if*
$$\sqrt{r_h-r_l}\left(\sqrt{r_h-r_l+4\sqrt{k_l(r_l-\hat{r}_h)}-4k_l}-\sqrt{r_h-r_l+4\sqrt{k_h(r_l-\hat{r}_h)}-4k_h}\right)$$
$$<2\sqrt{r_l-\hat{r}_h}\left(\sqrt{k_h}-\sqrt{k_l}\right)$$

   and
$$\sqrt{\frac{k_h}{r_l-\hat{r}}}>\sqrt{\frac{k_l}{r_l-\hat{r}_h}}$$

2. $\left\{\sigma_l,s_h,\sigma_l\in\left[s_l',s_l''\right],\Pr_{t\in[0,s_l')}(h\mid A_t=0)=\delta,\Pr_{t\in\left[s_l',s_l''\right]}(h\mid A_t=0)=\frac{r_l-\hat{r}_l}{\hat{r}_h-\hat{r}_l}-\frac{k_l}{(\hat{r}_h-\hat{r}_l)t^2},\right.$
$\left.\Pr_{t\in(s_l'',s_h)}(h\mid A_t=0)=1,\Pr_{t\in[0,s_h)}(h\mid A_t=1)=0,\Pr_{t\in[s_h,1]}\left(h\mid A_{(s_h)^-}=0\right)=1\right\}$ *is the mixed-strategy atypical separating equilibrium.*

   $\sigma_l=\frac{1}{1-\delta}-\frac{\delta(\hat{r}_h-\hat{r}_l)}{(1-\delta)\left(r_l-\hat{r}_l-\frac{k_l}{t^2}\right)}$, $s_l'=s_l^p=\sqrt{\frac{k_l}{r_l-\hat{r}}}$, $s_l''=s_{lh}=\sqrt{\frac{k_l}{r_l-\hat{r}_h}}$,

   If $s_h^c=\sqrt{\frac{k_h}{r_h-\hat{r}_h}}\in\left[\max\left\{s_h^{a**},s_{hl}^{a*}\right\},s_{hl}^{a**}\right]$. $s_h=s_h^c$. *If* $s_h^c<\max\left\{s_h^{a**},s_{hl}^{a*}\right\}$,
   $s_h=\max\left\{s_h^{a**},s_{hl}^{a*}\right\}$.

   $s_h^{a**}=\frac{r_h-r_l+2\sqrt{k_l(r_l-\hat{r}_h)}+\sqrt{\left(r_h-r_l+2\sqrt{k_l(r_l-\hat{r}_h)}\right)^2-4k_l(r_h-\hat{r}_h)}}{2(r_h-\hat{r}_h)}$.

   $s_{hl}^{a*}=\frac{r_h-r_l+2\sqrt{k_h(r_l-\hat{r})}-\sqrt{\left(r_h-r_l+2\sqrt{k_h(r_l-\hat{r})}\right)^2-4k_h(r_h-\hat{r})}}{2(r_h-\hat{r})}$.

   $s_{hl}^{a**}=\frac{r_h-r_l+2\sqrt{k_h(r_l-\hat{r})}+\sqrt{\left(r_h-r_l+2\sqrt{k_h(r_l-\hat{r})}\right)^2-4k_h(r_h-\hat{r})}}{2(r_h-\hat{r})}$.

Proposition 4.3 shows the condition under which a mixed-strategy atypical separating equilibrium exists. In the mixed-strategy atypical separating equilibrium, low-

type vendors release patches earlier than high-type vendors. Different from the normal separating equilibrium, high-type vendors' release time must be *later* than the marginal release time, s_h^{a**}, to prevent low-type vendors from mimicking. If $\sqrt{\frac{k_h}{r_l-\hat{r}}} > \sqrt{\frac{k_l}{r_l-\hat{r}_h}}$, any release time for high-type vendors in the range $\left[s_{hl}^{a*}, s_{hl}^{a**}\right]$ can ensure that high-type vendors have an incentive to signal their types. Therefore, the equilibrium release time for high-type vendors must fall in the range $\left[\max\left\{s_h^{a**}, s_{hl}^{a*}\right\}, s_{hl}^{a**}\right]$. The existence of an atypical separating equilibrium requires $s_h^{a**} < s_{hl}^{a**}$.

The later a vendor releases a patch, the more likely it is of high-type. The reputation of the software product is weakly increasing. If high-type vendors' release time in the complete information case, s_h^c, is late enough to prevent low-type vendors from mimicking, high-type vendors will choose it as the equilibrium release time. Otherwise, high-type vendors will choose the marginal release time, $\max\left\{s_h^{a**}, s_{hl}^{a*}\right\}$. In equilibrium, a low-type vendor will choose the release time following the distribution σ_l over $\left[s_l^p, s_{lh}\right]$. Consumers' belief, $\Pr_{t\in\left[s_l^p, s_{lh}\right]}\left(h \mid A_t = 1\right) = \frac{r_l-\hat{r}_l}{\hat{r}_h-\hat{r}_l} - \frac{k_l}{(\hat{r}_h-\hat{r}_l)t^2}$, guarantees that low-type vendors make the same profit over $\left[s_l^p, s_{lh}\right]$. Low-type vendors' strategies, $\sigma_l = \frac{1}{1-\delta} - \frac{\delta(\hat{r}_h-\hat{r}_l)}{(1-\delta)\left(r_l-\hat{r}_l-\frac{k_l}{t^2}\right)}$, ensure that consumers' belief update consistent with Bayes' rule. Vendors can be completely separated because the upper bound of the support of σ_l, s_{lh}, is smaller than s_h.

Since low-type vendors have a lower patching cost than high-type vendors, it is easier for low-type vendors to delay the patch release. Considering the signaling effect of patching strategies, it is natural to expect that low-type vendors have incentives to misrepresent their software quality by mimicking high-type vendors. However, low-type vendors suffer a loss in sales in the presence of unpatched vulnerabilities. Thus, they choose to patch vulnerabilities as soon as possible because of the salvage effect of patching strategies.

Example 1: Assume that $r_h = 1$, $r_l = \frac{1}{2}$, $\delta = \frac{1}{2}$, $\hat{r}_h = \frac{1}{2}$, $\hat{r}_l = \frac{1}{4}$, $k_h = \frac{1}{16}$ and $k_l = \frac{1}{4}$. The sufficient and necessary condition in Proposition 1 holds. Thus, there is a normal separating equilibrium. In particular, $s_l^c = 1$, $s_h^p = \sqrt{\frac{1}{10}} = 0.316$, $s_{hl}^{n*} = \frac{1}{2} - \sqrt{\frac{1}{6}} = 0.093$, $s_h^{n*} = \frac{1}{3}$, $s_{hl}^{n**} = \frac{1}{2} + \sqrt{\frac{1}{6}} = 0.908$, Since $\sqrt{\frac{1}{10}} \in \left[\frac{1}{2} - \sqrt{\frac{1}{6}}, \min\{\frac{1}{3}, \frac{1}{2} + \sqrt{\frac{1}{6}}\}\right]$, $\sqrt{\frac{1}{10}}$ is the equilibrium release time for high-type vendors and 1 is the equilibrium release time for low-type vendors.

Example 2: Assume that $r_h = 1$, $r_l = \frac{1}{2}$, $\delta = \frac{1}{2}$, $\hat{r}_h = \frac{1}{4}$, $\hat{r}_l = \frac{1}{8}$, $k_h = \frac{1}{4}$, $k_l = \frac{1}{8}$. The conditions in Proposition 2 hold, there is a mixed-strategy atypical separating equilibrium. In particular, $s_l^p = \sqrt{\frac{2}{5}}$. $s_{lh} = \sqrt{\frac{1}{2}}$, $s_h^c = \sqrt{\frac{1}{3}} = 0.5547$, $s_h^{a**} = \frac{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}} + \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}} - \frac{3}{8}}}{\frac{3}{2}} = 0.9656$, $s_{hl}^{a*} = \frac{\frac{1}{2} + \frac{\sqrt{5}}{4} - \sqrt{\left(\frac{1}{2} + \frac{\sqrt{5}}{4}\right)^2 - \frac{13}{16}}}{\frac{3}{2}} = 0.4099$, $s_{hl}^{a**} = \frac{\frac{1}{2} + \frac{\sqrt{5}}{4} + \sqrt{\left(\frac{1}{2} + \frac{\sqrt{5}}{4}\right)^2 - \frac{13}{16}}}{\frac{3}{2}} = 1.614$. $\sigma_l = 2 - \frac{1}{3 - \frac{1}{t^2}}$. Since $\sqrt{\frac{1}{3}} < \max\left\{\frac{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}} + \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}} - \frac{3}{8}}}{\frac{3}{2}}, \frac{\frac{1}{2} + \frac{\sqrt{5}}{4} - \sqrt{\left(\frac{1}{2} + \frac{\sqrt{5}}{4}\right)^2 - \frac{13}{16}}}{\frac{3}{2}}\right\}, \frac{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}} + \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}} - \frac{3}{8}}}{\frac{3}{2}}$ is the equilibrium release time for high-type vendors and $\sqrt{\frac{2}{5}}$ is the equilibrium release time for low-type vendors.

4.5 DISCUSSION AND CONCLUSION

Patching vulnerabilities after software release is an important stage in the software development circle. While quality uncertainty is a fundamental issue in the software market, and patching behavior is closely connected to the software quality, the strategic aspects of the patching decisions need to be understood. In this paper, we explore the information role of patching strategies. We show that vendors can leverage the patch release time to signal the quality of their software considering two distinct reputation effects, the salvage effect and the signaling effect. We find both the salvage effect and the signaling effect can drive a separating outcome.

We define and identify two types of separating equilibria. In the normal separating equilibrium, high-type vendors patch vulnerabilities more quickly than low-type vendors. High-type vendors prefer to differentiate themselves from low-type vendors in addition to rebuilding the reputation for their software products. The signal effect strengthens the salvage effect in providing incentives for vendors to patch quickly. In the atypical separating equilibrium, low-type vendors patch vulnerabilities more quickly than high-type vendors. The salvage effect provides vendors incentives to patch earlier, whereas the signaling effect drives them to delay the patch release. The signaling effect weakens the salvage effect. Low-type vendors release patches earlier because the salvage effect dominates the signaling effect.

This paper investigates a special form of signals. Specifically, the patch release time is an informative signal. Different from previous literature in which the signal is sent at the beginning of the game, the signal in this study is the timing of actions. The update of belief takes place over time. We define a new belief profile and identify the corresponding separating equilibria.

To simplify the analysis and derive tractable results, this model has some restrictions. For example, hackers are exogenous, users are homogenous, and consumers' patching decisions are exogenous. A more complex model accounting for these aspects would change the specifics of the analysis but not the basic insights provided by the model. We also abstract from the choice of software quality and patch quality. This allows us to focus on strategic issues of timing decisions.

Future research directions naturally include an empirical study, including estimating the correlation between the software quality and the patching cost, identifying the reputation determinants, and testing the existence of the separation. It is also valuable to extend our approach to other relevant scenarios and gain insight into repairing and

reputation building. Besides the software industry, rework and warranties are commonly observed in other industries. We will extend our analysis to manufacturing sectors, such as automobiles and consumer electronics, considering their distinct features. A potentially interesting direction is to explore the tradeoff between reworking in the production process and repairing in the after-sale stage, taking account of the reputation effects.

Appendix

APPENDIX FOR CHAPTER 2

Proof of Lemma 2.1

Proof: Since certified SPs choose the blocking strategy before they choose the pricing and investment strategies, we first analyze certified SPs' pricing and investment strategies in each blocking strategy, then derive the blocking strategy.

(1) Blocking Case: certified SPs completely block the traffic from non-certified SPs

A customer's expected willingness to pay to certified SP i is

$$u_{sk} = 2VNn\delta + VNn(1-\delta) - n\sum_{j\in CP}(v-s)(1-x_{jk}))q_j$$

The subscript *k* represents that case certified SPs completely block the inbound traffic from non-certified SPs. From Condition 4, $u_{sk} = 2VNn\delta + VNn(1-\delta) = VNn + VNn\delta$. The price a certified SP can charge is $p_{sk} = u_{sk}$. Certified SP i 's profit is

$$\pi_{sk} = p_{sk}n - v(1-x_{ik})q_i\delta Nn^2 - C_2(x_{ik}) - t.$$

Certified SP's optimization problem is $\underset{x_{sk}}{Max}\ p_{sk}n - v(1-x_{ik})q_i\delta Nn^2 - \frac{1}{2}\beta x_{ik}^2 - t$.

Using FOC, we can derive the optimal investment for certified SPs.

$x_{sk}(q_i) = \min\left\{1,\ \frac{1}{\beta}Mvq_i\delta\right\}$. A certified SP i 's profit is

$$\begin{aligned}\pi_s^* &= VNn^2\delta + VNn^2 - v(1-x_{sb})\delta Nn^2 q_i - C_2(x_{sb}) - t \\ &= MV\delta + MV - \left(1-\min\left\{1,\ \frac{1}{\beta}Mv\delta q_i\right\}\right)Mv\delta q_i - \frac{1}{2}\beta\left(\min\left\{1,\ \frac{1}{\beta}Mv\delta q_i\right\}\right)^2 - t\end{aligned}$$

(2) Filtering Case: certified SPs selectively filter the traffic from non-certified SPs

A customer's expected willingness to pay to certified SP *i* is

$$u_{sf} = 2VNn\delta + 2VNn(1-\delta) - n\sum_{j\in CP}(v-s)(1-x_{sf}))q_j - n\sum_{k\notin CP}v(1-y_{sf}))q_k \qquad \text{(A2.1)}$$

The subscript f represents the case that certified SPs selectively filter the traffic from non-certified SPs. y_{sk} denotes the level of effectiveness of certified SPs' protective

practices. From Condition 4 and given that only high-type SPs get certified in the separating outcome, (A2.1) can be written as $u_{sf} = 2VNn - \left(1 - y_{sf}\right) vN\left(1-\delta\right) nq_l$. The price a certified SP can charge is $p_{sf} = u_{sf}$. Certified SP i's profit is

$$\pi_{sf} = p_{sf} n - v\left(1 - x_{sf}\right) q_i \delta N n^2 - C_1\left(y_{sf}\right) - C_2\left(x_{sf}\right) - t .$$

Certified SP's optimization problem is

$\underset{x_{sf}}{Max}\left(2VNn - \left(1-y_{sf}\right)vN\left(1-\delta\right)nq_l\right)n - v\left(1-x_i\right)q_i\delta Nn^2 - \frac{1}{2}\alpha y_{sf}^2 - \frac{1}{2}\beta x_{sf}^2 - t$. Using FOC,

$x_{sf}^*(q_i) = \min\left\{1,\ \frac{1}{\beta}Mvq_i\delta\right\}$, $y_{sf}^* = \frac{1}{\alpha}Mvq_l\left(1-\delta\right)$. A certified SP i's profit is

$$\pi_{sf} = 2MV - Mvq_i\delta\left(1 - \min\left\{1,\ \frac{1}{\beta}Mvq_i\delta\right\}\right) - \frac{1}{2}\beta\left(\min\left\{1,\ \frac{1}{\beta}Mvq_i\delta\right\}\right)^2 - Mvq_l\left(1-\delta\right) + \frac{1}{2\alpha}\left(Mvq_l\left(1-\delta\right)\right)^2 - t$$

Certified SPs' profit difference between when they selectively filter traffic from non-certified SPs and when they completely block traffic from non-certified SPs.

$$\pi_{sf} - \pi_{sk} = \left(\begin{array}{c} 2MV - Mvq_i\delta\left(1 - \min\left\{1,\ \frac{1}{\beta}Mvq_i\delta\right\}\right) - \frac{1}{2}\beta\left(\min\left\{1,\ \frac{1}{\beta}Mvq_i\delta\right\}\right)^2 \\ -Mvq_l\left(1-\delta\right) + \frac{1}{2\alpha}\left(Mvq_l\left(1-\delta\right)\right)^2 - t \end{array}\right)$$

$$-\left(2MV\delta + MV\left(1-\delta\right) - Mvq_i\delta\left(1 - \min\left\{1,\ \frac{1}{\beta}Mvq_i\delta\right\}\right) - \frac{1}{2}\beta\left(\min\left\{1,\ \frac{1}{\beta}Mvq_i\delta\right\}\right)^2 - t\right)$$

$$\begin{aligned} \pi_{sf} - \pi_{sk} &= MV\left(1-\delta\right) - Mvq_l\left(1-\delta\right) + \frac{1}{2\alpha}\left(Mvq_l\left(1-\delta\right)\right)^2 \\ &< MV\left(1-\delta\right) - Mvq_l\left(1-\delta\right) + \frac{1}{2\alpha}\left(Mvq_l\right)^2\left(1-\delta\right) \\ &= \left(MV - Mvq_l + \frac{1}{2\alpha}\left(Mvq_l\right)^2\right)\left(1-\delta\right) \end{aligned}$$

From Condition 4, $\pi_{sf} - \pi_{sk} < 0$. Certified SPs make a higher profit when they completely block the inbound traffic from non-certified SPs. Thus, certified SPs will block the traffic from non-certified SPs.

Proof of Lemma 2.2

Proof: A customer's willingness to pay to a non-certified SP is

$$\begin{aligned} \hat{u}_s &= \left(V\delta + 2V\left(1-\delta\right)\right)Nn - \left(1-\hat{y}_{sf}\right)Nnv\left(1-\delta\right)q_l - Nnv\delta\left(1 - \min\left\{1,\ \frac{1}{\beta}Mvq_h\delta\right\}\right)q_h \\ &= VNn + V\left(1-\delta\right)Nn - \left(1-\hat{y}_{sf}\right)Nnv\left(1-\delta\right)q_l - Nnv\delta q_h + Nnv\delta q_h \min\left\{1,\ \frac{1}{\beta}Mvq_h\delta\right\} \end{aligned}$$

Since regulative practices are more effective than protective practices, non-certified SPs cannot further clean inbound malicious traffic given that certified SPs have screened the outgoing traffic. Thus, protective practices can only effectively filter the traffic from non-certified SPs, $Nnv(1-\delta)q_l$.

The price non-certified SPs can charge is $\hat{p}_s = \hat{u}_s$. Non-certified SP profit is $\hat{\pi}_s = MV + MV(1-\delta) - (1-\hat{y}_s)Mvq_l(1-\delta) - Mv\delta q_h + Mv\delta q_h \min\left\{1, \frac{1}{\beta}Mvq_h\delta\right\} - \frac{1}{2}\alpha(\hat{y}_s)^2$. Using FOC, $\hat{y}_s = \min\left\{1, \frac{1}{\alpha}Mvq_l(1-\delta)\right\}$. And from Condition 2, $\hat{y}_s = \frac{1}{\alpha}Mvq_l(1-\delta)$. Thus, a non-certified SP's profit is

$$\hat{\pi}_s = VM + MV(1-\delta) - MvE[q] + \frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2 + Mv\delta q_h \min\left\{1, \frac{1}{\beta}Mvq_h\delta\right\}$$

Proof of Lemma 2.3

Proof: The separating outcome requires $\begin{cases}\pi_s(q_h) \geq \hat{\pi}_s(q_h) & \text{(IC for high-type ISPs)}\\ \hat{\pi}_s(q_l) > \pi_s(q_l) & \text{(IC for low-type ISPs)}\end{cases}$

Here $\hat{\pi}_s(q_h)$ is the profit a high-type SPs can make if it is non-certified and $\pi_s(q_l)$ is the profit a low-type SPs can make if it is certified. If a high-type SPs deviates and does not subscribe to the CS

$$\hat{\pi}_s(q_h) = V(N\delta-1)n^2 + 2V(N(1-\delta)+1)n^2 - MvE[q] + \frac{1}{2\alpha}\left(n^2vq_l(N(1-\delta)+1)\right)^2 + n^2vq_h(N\delta-1)\min\left\{1, \frac{1}{\beta}n^2vq_h(N\delta-1)\right\}$$

Since $N >> 1$, we can simply $\hat{\pi}_s(q_h)$ as follows.

$$\hat{\pi}_s(q_h) = VM + MV(1-\delta) - MvE[q] + \frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2 + Mv\delta q_h \min\left\{1, \frac{1}{\beta}Mvq_h\delta\right\}$$

If a low-type SP deviates and subscribes to CS, its profit is.

$$\pi_s(q_l) = MV\delta + MV - \left(1-\min\left\{1, \frac{1}{\beta}Mvq_l\delta\right\}\right)Mvq_l\delta - \frac{1}{2}\beta\left(\min\left\{1, \frac{1}{\beta}Mvq_l\delta\right\}\right)^2 - t$$

If $\beta \geq Mvq_l\delta$,

$$\begin{pmatrix} MV(2\delta-1) + Mvq_l(1-2\delta) \\ +Mvq_h\delta - \frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2 \\ +\frac{1}{2\beta}\left(Mvq_l\delta\right)^2 - \frac{1}{\beta}\left(Mvq_h\delta\right)^2 \end{pmatrix} < t \leq \begin{pmatrix} MV(2\delta-1) + Mvq_l(1-\delta) \\ -\frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2 - \frac{1}{2\beta}\left(Mvq_h\delta\right)^2 \end{pmatrix}$$

If $Mvq_h\delta \leq \beta < Mvq_l\delta$,

$$\begin{pmatrix} MV(2\delta-1)+MvE[q]-\frac{1}{2}\beta \\ -\frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2-\frac{1}{\beta}\left(Mvq_h\delta\right)^2 \end{pmatrix} < t \le \begin{pmatrix} MV(2\delta-1)+Mvq_l(1-\delta) \\ -\frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2-\frac{1}{2\beta}\left(Mvq_h\delta\right)^2 \end{pmatrix}$$

If $\beta < Mvq_h\delta$, $\begin{pmatrix} MV(2\delta-1)+Mvq_l(1-\delta) \\ -\frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2-\frac{1}{2}\beta \end{pmatrix} < t \le \begin{pmatrix} MV(2\delta-1)+Mvq_l(1-\delta) \\ -\frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2-\frac{1}{2}\beta \end{pmatrix}$

No t satisfies both incentive constraints. Thus, when $\beta < Mvq_h\delta$, there is no separating outcome.

Overall, when $\beta \ge Mvq_h\delta$, there is a range of t all of which support separating outcome. The optimal fee for the certification provider to induce the separating outcome is $MV(2\delta-1)+Mvq_l(1-\delta)-\frac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2-\frac{1}{2\beta}\left(Mvq_h\delta\right)^2$.

Proof of Lemma 2.4

Proof: A customer's willingness to pay to certificated SP $u_p = 2VNn-(v-s)\left((1-x_{ph})q_h\delta+(1-x_{pl})q_l(1-\delta)\right)Nn$. Again, Let $v=s$, $u_p = 2VNn$. The price a SP can charge is $p^p = u^p$. Certificate SP's ($q_i = q_l$ or q_h) profit is

$$\pi_p(q_i)=\left(p^p-v\left(1-x_p(q_i)\right)q_iNn\right)n-C_2\left(x_p(q_i)\right)-t=2VM-Mv\left(1-x_p(q_i)\right)q_i-\frac{1}{2}\beta\left(x_p(q_i)\right)^2-t$$

Using FOC, $x_{ci}^p=\min\left\{1,\ \frac{1}{\beta}Mvq_i\right\},\ i\in\{h,\ l\}$. And a SP's profit is

$$\pi_p(q_i)=2VM-Mv\left(1-\min\left\{1,\ \frac{1}{\beta}Mvq_i\right\}\right)q_i-\frac{1}{2}\beta\left(\min\left\{1,\ \frac{1}{\beta}Mvq_i\right\}\right)^2-t,\ \ i\in[h,\ l]$$

(1) If a SP deviates and certified SPs completely block the traffic from non-certified SPs

A customer's expected willingness to pay to certified SP *i* is $u_{pk}=V(2N-1)n-n\sum_{j\in CP}(v-s)\left(1-x_{pk}(q_j)\right)q_j$. From Condition 4, $u_{pk}=(2N-1)nV$. The price a certified SP can charge is $p_{pk}=u_{pk}$.

Certified SP i 's profit is $\pi_{pk}(q_i)=p_{pk}n-v\left(1-x_{pk}(q_i)\right)q_i(N-1)n^2-C_2\left(x_{pk}\right)-t$. Using FOC, $x_{pk}(q_i)=\min\left\{1,\ \frac{1}{\beta}(N-1)n^2vq_i\right\}$. A certified SP *i* 's profit is

$$\pi_{pk}(q_i)=(2N-1)n^2V-(N-1)n^2vq_i\left(1-\min\left\{1,\ \frac{1}{\beta}(N-1)n^2vq_i\right\}\right)-\frac{1}{2}\beta\left(\min\left\{1,\ \frac{1}{\beta}(N-1)n^2vq_i\right\}\right)^2$$

(2) If a SP deviates and certified SPs accept and filter the traffic from non-certified SPs

A customer's expected willingness to pay to certified SP *i* is $u_{pf} = V(2N-1)n + Vn - n\sum_{j\in CP}(v-s)\left(1-x_{pf}(q_j)\right)q_j - nv\left(1-y_{pf}\right)q_l$. From Condition 4, $u_{pf} = 2NnV - nv\left(1-y_{pf}\right)q_l$. The price a certified SP can charge is $p_{pf} = u_{pf}$

Certified SP *i* 's profit is $\pi_{pf}(q_i) = p_{pf}n - v\left(1-x_{pf}(q_i)\right)q_i(N-1)n^2 - C_1\left(y_{pf}\right) - C_2\left(x_{pf}\right) - t$. Using FOC, $x_{pf}(q_i) = \min\left\{1,\ \frac{1}{\beta}(N-1)n^2vq_i\right\}$, $y_{pf} = \frac{1}{\alpha}n^2vq_l$

A certified SP *i* 's profit is

$$\pi_{pf}(q_i) = (2N+1)n^2V - (N-1)n^2vq_i\left(1-\min\left\{1,\ \tfrac{1}{\beta}(N-1)n^2vq_i\right\}\right) - \tfrac{1}{2}\beta\left(\min\left\{1,\ \tfrac{1}{\beta}(N-1)n^2vq_i\right\}\right)^2 - n^2vq_l + \tfrac{1}{2}\left(n^2vq_l\right)^2 - t$$

Certified SPs' profit difference between when they completely block traffic from non-certified SPs and when they selectively filter traffic from non-certified SPs.

$$\pi_{pf} - \pi_{pk} = \begin{pmatrix} (2N+1)n^2V - (N-1)n^2vq_i\left(1-\min\left\{1,\ \tfrac{1}{\beta}(N-1)n^2vq_i\right\}\right) \\ -\tfrac{1}{2}\beta\left(\min\left\{1,\ \tfrac{1}{\beta}(N-1)n^2vq_i\right\}\right)^2 - n^2vq_l + \tfrac{1}{2\alpha}\left(n^2vq_l\right)^2 - t \end{pmatrix} - \begin{pmatrix} (2N-1)n^2V - (N-1)n^2vq_i\left(1-\min\left\{1,\ \tfrac{1}{\beta}(N-1)n^2vq_i\right\}\right) \\ -\tfrac{1}{2}\beta\left(\min\left\{1,\ \tfrac{1}{\beta}(N-1)n^2vq_i\right\}\right)^2 - t \end{pmatrix}$$

$$\pi_{pf} - \pi_{pk} = n^2V - n^2vq_l + \tfrac{1}{2\alpha}\left(n^2vq_l\right)^2 = \tfrac{1}{N}\left(MV - Mvq_l + \tfrac{1}{N}\tfrac{1}{2\alpha}\left(Mvq_l\right)^2\right) < \tfrac{1}{N}\left(MV - Mvq_l + \tfrac{1}{2\alpha}\left(Mvq_l\right)^2\right)$$

From Condition 4, $\pi_{pf} - \pi_{pk} < 0$. Certified SPs make a higher profit when they completely block the traffic from non-certified SPs. Thus, certified SPs will block the traffic from non-certified SPs.

Proof of Lemma 2.5

Proof: The pooling outcome requires $\begin{cases} \pi_p(q_h) \geq \hat{\pi}_p(q_h) & \text{IC for high-type ISPs} \\ \hat{\pi}_p(q_l) \geq \pi_p(q_l) & \text{IC for low-type ISPs} \end{cases}$

A high-type certified SP earns higher profit than a low-type certified SP. The profit earned by a non-certified SP is independent of its type. Therefore, if a low-type SP subscribes to certification services, a high-type SP also subscribes to it. Thus, the incentive constraint for high-type SPs does not bind. In this proof, we only consider the incentive constraint for low-type SPs.

A customer's willingness to pay to a non-certified SP is

$$\hat{u}_p = V(N-1)n + 2nV - nv\begin{pmatrix} \left(1-\min\left\{1,\ \frac{1}{\beta}Mvq_l\right\}\right)\left(N(1-\delta)-1\right)q_l \\ +\left(1-\min\left\{1,\ \frac{1}{\beta}Mvq_h\right\}\right)q_h N\delta \end{pmatrix} + \left(1-\hat{y}_p\right)nvq_l$$

The price that a non-certified SP can charge is $\hat{p}_p = \hat{u}_p$. The non-certified SP's profit is

$$\hat{\pi}_p = MV - n^2V + 2nV - n^2v\begin{pmatrix} \left(1-\min\left\{1,\ \frac{1}{\beta}Mvq_l\right\}\right)q_l\left(N(1-\delta)-1\right) \\ +\left(1-\min\left\{1,\ \frac{1}{\beta}Mvq_h\right\}\right)q_h N\delta \end{pmatrix} + \left(1-\hat{y}_p\right)n^2vq_l - \frac{1}{2}\alpha\left(\hat{y}_p\right)^2$$

$\hat{y}_p = \frac{1}{\alpha}n^2vq_l$

$$\hat{\pi}_p = MV - n^2v\begin{pmatrix} \left(1-\min\left\{1,\ \frac{1}{\beta}Mvq_l\right\}\right)q_l N(1-\delta) \\ +\left(1-\min\left\{1,\ \frac{1}{\beta}Mvq_h\right\}\right)q_h N\delta \end{pmatrix}$$

The optimal fee for the certification provider is the maximal fee the certification provider can charge in each case. Thus,

$$\begin{cases} t \geq VM + Mvq_h\delta - Mvq_l\delta + \frac{1}{2\beta}\left(Mvq_l\right)^2 - \frac{1}{\beta}\left(Mvq_l\right)^2(1-\delta) - \frac{1}{\beta}\left(Mvq_h\right)^2\delta & \text{if } \beta \geq Mvq_l \\ t \geq VM - \frac{1}{2}\beta + Mvq_h\delta - \frac{1}{\beta}\left(Mvq_h\right)^2\delta & \text{if } Mvq_h \leq \beta < Mvq_l \\ t \geq VM - \frac{1}{2}\beta & \text{if } \beta < Mvq_h \end{cases}$$

Proof of Proposition 2.2

Proof: Define $\Delta_i = \pi_{si} - \pi_{pi}$, $i \in \{1,\ 2,\ 3\}$.

(1) When $\beta > Mvq_l$

The certification provider's profit in the separating outcome and the pooling outcome are as follows:

$$\pi_{s1} = \left(MV(2\delta - 1) + Mvq_l(1-\delta) - \tfrac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2 - \tfrac{1}{2\beta}\left(Mvq_h\delta\right)^2 \right)\delta$$

$$\pi_{p1} = VM + Mvq_h\delta - Mvq_l\delta + \tfrac{1}{2\beta}\left(Mvq_l\right)^2 - \tfrac{1}{\beta}\left(Mvq_l\right)^2(1-\delta) - \tfrac{1}{\beta}\left(Mvq_h\right)^2\delta$$

$$\Delta_1 = \pi_{s1} - \pi_{p1} = \begin{pmatrix} \left(MV(2\delta - 1) + Mvq_l(1-\delta) - \tfrac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2 - \tfrac{1}{2\beta}\left(Mvq_h\delta\right)^2 \right)\delta \\ -\left(VM + Mvq_h\delta - Mvq_l\delta + \tfrac{1}{2\beta}\left(Mvq_l\right)^2 - \tfrac{1}{\beta}\left(Mvq_l\right)^2(1-\delta) - \tfrac{1}{\beta}\left(Mvq_h\right)^2\delta \right) \end{pmatrix}$$

When $\delta \to 0$,

$$\Delta_1 = \begin{pmatrix} \left(-MV + Mvq_l - \tfrac{1}{2\alpha}\left(Mvq_l\right)^2 \right)\delta \\ -\left(VM + \tfrac{1}{2\beta}\left(Mvq_l\right)^2 - \tfrac{1}{\beta}\left(Mvq_l\right)^2 \right) \end{pmatrix} = \tfrac{1}{2\beta}\left(Mvq_l\right)^2 - MV < M\left(\tfrac{1}{2}vq_l - V\right)$$

When $\delta \to 1$, $\Delta_1 = Mv\left(q_l - q_h\right)\left(1 - \tfrac{1}{2\beta}Mv\left(q_h + q_l\right)\right) > 0$

When δ is large enough, the certification provider has a higher profit in the separating equilibrium. When δ is small, the certification provider prefers the pooling equilibrium.

(2) When $Mvq_h < \beta \le Mvq_l$

In the separating outcome, the certification provider's profit is

$$\pi_{2s} = \left(MV(2\delta - 1) + Mvq_l(1-\delta) - \tfrac{1}{2\alpha}\left(Mvq_l(1-\delta)\right)^2 - \tfrac{1}{2\beta}\left(Mvq_h\delta\right)^2 \right)\delta$$

The certification provider's profit in the pooling outcome, is

$$\pi_{2p} = VM - \tfrac{1}{2}\beta + Mvq_h\delta - \tfrac{1}{\beta}\left(Mvq_h\right)^2\delta$$

$$\Delta_2 = \pi_{2s} - \pi_{2p} = -\begin{pmatrix} \tfrac{1}{2\beta}\left(Mvq_h\right)^2\delta^3 + \tfrac{1}{2\alpha}\left(Mvq_l\right)^2\delta^3 - 2MV\delta^2 - \tfrac{1}{\alpha}\left(Mvq_l\right)^2\delta^2 + Mvq_l\delta^2 \\ +\tfrac{1}{2\alpha}\left(Mvq_l\right)^2\delta + MV\delta - Mvq_l\delta + Mvq_h\delta - \tfrac{1}{\beta}\left(Mvq_h\right)^2\delta + MV - \tfrac{1}{2}\beta \end{pmatrix}$$

When $\delta \to 0$, $\Delta_2 = -MV + \tfrac{1}{2}\beta < 0$

When $\delta \to 1$, $\Delta_2 = \frac{1}{2}\beta - Mvq_h + \frac{1}{2\beta}\left(Mvq_h\right)^2 > 0$

When δ is large enough, the certification provider will induce the separating equilibrium if possible. When δ is small, the certification provider prefers the pooling equilibrium.

(3) When $Mv\delta q_h < \beta \le Mvq_h$

In the separating outcome, the certification provider's profit is

$$\pi_{3s} = \left(MV\left(2\delta - 1\right) + Mvq_l\left(1-\delta\right) - \frac{1}{2\alpha}\left(Mvq_l\left(1-\delta\right)\right)^2 - \frac{1}{2\beta}\left(Mvq_h\delta\right)^2\right)\delta$$

The certification provider's profit in the pooling outcome, is $\pi_{3p} = VM - \frac{1}{2}\beta$

$$\Delta_3 = \pi_{2s} - \pi_{2p} = -\left(\begin{array}{c}\frac{1}{2\beta}\left(Mvq_h\right)^2\delta^3 + \frac{1}{2\alpha}\left(Mvq_l\right)^2\delta^3 - 2MV\delta^2 - \frac{1}{\alpha}\left(Mvq_l\right)^2\delta^2 + Mvq_l\delta^2 \\ + \frac{1}{2\alpha}\left(Mvq_l\right)^2\delta + MV\delta - Mvq_l\delta + MV - \frac{1}{2}\beta\end{array}\right)$$

When $\delta \to 0$, $\Delta_3 = -MV + \frac{1}{2}\beta < 0$

When $\delta \to 1$,

$$\begin{aligned}\Delta_3 &= -\left(\begin{array}{c}\frac{1}{2\beta}\left(Mvq_h\right)^2\left(1-\varepsilon\right)^3 + \frac{1}{2\alpha}\left(Mvq_l\right)^2\left(1-\varepsilon\right)^3 - 2MV\left(1-\varepsilon\right)^2 - \frac{1}{\alpha}\left(Mvq_l\right)^2\left(1-\varepsilon\right)^2 \\ + Mvq_l\left(1-\varepsilon\right)^2 + \frac{1}{2\alpha}\left(Mvq_l\right)^2\left(1-\varepsilon\right) + MV\left(1-\varepsilon\right) - Mvq_l\left(1-\varepsilon\right) + MV - \frac{1}{2}\beta\end{array}\right) \\ &= 3M\left(\frac{1}{2}vq_h + \frac{1}{3}vq_l - V\right)\varepsilon\end{aligned}$$

If $\frac{1}{2}vq_h + \frac{1}{3}vq_l - V > 0$, when δ is large enough, the certification provider induces the separating equilibrium; when δ is small, the certification provider prefers the pooling equilibrium. If $\frac{1}{2}vq_h + \frac{1}{3}vq_l - V < 0$, the certification provider always makes higher profit in the pooling equilibrium than in the separating equilibrium.

Proof of Proposition 2.3

Proof: The system surplus in the separating equilibrium is

$$S_s = \left(\begin{array}{c}\left(MV\delta + MV - \left(1 - \min\left\{1,\ \frac{1}{\beta}Mv\delta q_h\right\}\right)Mv\delta q_h - \frac{1}{2}\beta\left(\min\left\{1,\ \frac{1}{\beta}Mv\delta q_h\right\}\right)^2\right)\delta N \\ + \left(VM + MV\left(1-\delta\right) - MvE\left[q\right] + \frac{1}{2\alpha}\left(Mvq_l\left(1-\delta\right)\right)^2 + Mv\delta q_h \min\left\{1,\ \frac{1}{\beta}Mvq_h\delta\right\}\right)\left(1-\delta\right)N\end{array}\right)$$

Let $\beta > Mv\delta q_h$

$$S_s = \begin{pmatrix} \left(MV\delta + MV - Mv\delta q_h + \frac{1}{2\beta}\left(Mv\delta q_h\right)^2\right)\delta N \\ +\left(VM + MV\left(1-\delta\right) - MvE\left[q\right] + \frac{1}{2\alpha}\left(Mvq_l\left(1-\delta\right)\right)^2 + \frac{1}{\beta}\left(Mvq_h\delta\right)^2\right)\left(1-\delta\right)N \end{pmatrix}$$

The system surplus in the benchmark case is

$$S_b = 2V(Nn)^2 - (Nn)^2 vE\left[q\right] + \frac{N}{2\alpha}\left(MvE\left[q\right]\right)^2$$

Define $D_i = S_s - S_b$

$$D_1 = S_s - S_b = \begin{pmatrix} \left(MV\delta + MV - Mv\delta q_h + \frac{1}{2\beta}\left(Mv\delta q_h\right)^2\right)\delta N \\ +\left(VM + MV\left(1-\delta\right) - MvE\left[q\right] + \frac{1}{2\alpha}\left(Mvq_l\left(1-\delta\right)\right)^2 + \frac{1}{\beta}\left(Mvq_h\delta\right)^2\right)\left(1-\delta\right)N \end{pmatrix}$$

$$-\left(2V(Nn)^2 - (Nn)^2 vE\left[q\right] + \frac{N}{2\alpha}\left(MvE\left[q\right]\right)^2\right)$$

When $\delta \to \varepsilon$, $D_1 = -\left(2MV - Mvq_l + \frac{1}{2\alpha}\left(Mvq_l\right)^2 + \frac{1}{\alpha}\left(Mv\right)^2 q_h q_l\right)N\varepsilon < 0$

When $\delta \to 1$, $D_1 = \frac{1}{2\beta}\left(Mvq_h\right)^2 N - \frac{1}{2\alpha}\left(Mvq_h\right)^2 N > 0$

When $\delta > \tilde{\delta}$, the separating equilibrium generates a higher system surplus.

Proof of Proposition 2.4

Proof: The system surplus of the separating equilibrium is

$$S_s = \begin{pmatrix} \left(MV\delta + MV - Mv\delta q_h + \frac{1}{2\beta}\left(Mv\delta q_h\right)^2\right)\delta N \\ +\left(VM + MV\left(1-\delta\right) - MvE\left[q\right] + \frac{1}{2\alpha}\left(Mvq_l\left(1-\delta\right)\right)^2 + \frac{1}{\beta}\left(Mvq_h\delta\right)^2\right)\left(1-\delta\right)N \end{pmatrix}$$

The system surplus in the pooling outcome is

$$S_p = 2V(Nn)^2 - (Nn)^2 vE\left[q\right] + \frac{N}{2\beta}\left(MvE\left[q\right]\right)^2$$

Define $D = S_s - S_p$, $i \in \{1,\ 2\}$

$$D = S_s - S_p = -\begin{pmatrix} \frac{1}{2\alpha}\left(Mvq_l\right)^2\delta^3 + \frac{1}{2\beta}\left(Mvq_h\right)^2\delta^3 + Mvq_l\delta^2 - \frac{1}{\beta}\left(Mv\right)^2 q_h q_l\delta^2 \\ -2MV\delta^2 - \frac{3}{2\alpha}\left(Mvq_l\right)^2\delta^2 + \frac{1}{2\beta}\left(Mvq_l\right)^2\delta^2 - \frac{1}{2\beta}\left(Mvq_h\right)^2\delta^2 \\ +\frac{1}{\beta}\left(Mv\right)^2 q_h q_l\delta - \frac{1}{\beta}\left(Mvq_l\right)^2\delta + 2MV\delta + \frac{3}{2\alpha}\left(Mvq_l\right)^2\delta \\ -Mvq_l\delta + \frac{1}{2\beta}\left(Mvq_l\right)^2 - \frac{1}{2\alpha}\left(Mvq_l\right)^2 \end{pmatrix}$$

When $\delta \to 0$, $D_1 = \frac{1}{2\alpha}\left(Mvq_l\right)^2 - \frac{1}{2\beta}\left(Mvq_l\right)^2 < 0$

When $\delta \to 1$, let $\delta = 1-\varepsilon$,

$$D_1 = \left(\tfrac{1}{2\beta}\left(Mvq_h - Mvq_l\right)^2 - \tfrac{1}{2\beta}\left(Mvq_l\right)^2 + Mvq_l - 2MV\right)\varepsilon < 0$$

Thus, the system surplus in the pooling equilibrium is higher than the system surplus in the separating equilibrium.

APPENDIX FOR CHAPTER 3

Proof of Lemma 3.2

Proof: The first-order condition (FOC) of (1) with respective to x_i is

$$\begin{aligned}
&\mu_i' \sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)\begin{bmatrix} U\left(A-L+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+\frac{(n-1-k)}{n}q-x_i\right) \\ -U\left(A-\frac{k}{n}q+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-x_i\right)\end{bmatrix} \\
&=\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)\begin{bmatrix} \mu_i U'\left(A-L+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+\frac{(n-1-k)}{n}q-x_i\right) \\ +(1-\mu_i)U'\left(A-\frac{k}{n}q+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-x_i\right)\end{bmatrix}(1-C)
\end{aligned} \tag{A3.1}$$

When $q = L$, the FOC w.r.t. x_i can be represented as

$$\begin{aligned}
&\mu_i' \sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)\left[U\left(A-\frac{1+k}{n}q-x_i\right)-U\left(A-\frac{k}{n}q-x_i\right)\right] \\
&=\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)\left[\mu_i U'\left(A-\frac{1+k}{n}q-x_i\right)+(1-\mu_i)U'\left(A-\frac{k}{n}q-x_i\right)\right](1-C)
\end{aligned} \tag{A3.2}$$

Use $\sum_{k=0}^{n-1}\frac{(n-1)!}{k!(n-1-k)!}\mu_{-i}^k\left(1-\mu_{-i}^k\right)^{n-1-k}$ to substitute $b\left(k;(n-1),\mu_{-i}\right)$ in (A3.1) and simplify (A3.1), we have

$$\begin{aligned}
&\mu_i \sum_{k=0}^{n-1}\frac{(n-1)!}{k!(n-1-k)!}\mu^k(1-\mu)^{n-1-k}\frac{(n-1-k)}{n}U\left(A-L+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+\frac{(n-1-k)}{n}q-x_i\right) \\
&=(1-\mu_i)\sum_{k=0}^{n-1}\frac{(n-1)!}{k!(n-1-k)!}\frac{k}{n}U\left(A-\frac{k}{n}q+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-x_i\right)
\end{aligned}$$

$$\mu_i \sum_{k=0}^{n-2} \frac{(n-1)!}{k!(n-2-k)!} \mu^k (1-\mu)^{n-1-k} \frac{1}{n} U\left(A - L + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1} \right) + \frac{(n-1-k)}{n} q - x_i \right)$$

→

$$= (1-\mu_i) \sum_{k=0}^{n-1} \frac{(n-1)!}{k!(n-1-k)!} \frac{k}{n} U\left(A - \frac{k}{n} q + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1} \right) - x_i \right)$$

$$\mu_i \frac{1}{n} \sum_{k=0}^{n-2} \frac{(n-1)!}{k!(n-2-k)!} \mu^k (1-\mu)^{n-1-k} U\left(A - L + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1} \right) + \frac{(n-1-k)}{n} q - x_i \right)$$

→

$$= (1-\mu_i) \frac{1}{n} \sum_{k=0}^{n-2} \frac{(n-1)!}{k!(n-2-k)!} \mu^{k+1} (1-\mu)^{n-2-k} U\left(A - \frac{k+1}{n} q + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1} \right) - x_i \right)$$

In the symmetric case, $\mu(x_i) = \mu$, therefore we have

$$\frac{1}{n} \sum_{k=0}^{n-2} \frac{(n-1)!}{k!(n-2-k)!} \mu^{k+1} (1-\mu)^{n-1-k} U\left(A - L + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1} \right) + \frac{(n-1-k)}{n} q - x_i \right)$$

$$= \frac{1}{n} \sum_{k=0}^{n-2} \frac{(n-1)!}{k!(n-2-k)!} \mu^{k+1} (1-\mu)^{n-1-k} U\left(A - \frac{k+1}{n} q + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1} \right) - x_i \right)$$

When $q = L$, we have

$$\frac{1}{n} \sum_{k=0}^{n-2} \frac{(n-1)!}{k!(n-2-k)!} \mu^{k+1} (1-\mu)^{n-1-k} U\left(A - \frac{1+k}{n} L + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1} \right) - x_i \right)$$

$$= \frac{1}{n} \sum_{k=0}^{n-2} \frac{(n-1)!}{k!(n-2-k)!} \mu^{k+1} (1-\mu)^{n-1-k} U\left(A - \frac{k+1}{n} L + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1} \right) - x_i \right)$$

Therefore, the FOC (A3.1) holds when $q = L$. Thus, $q = L$

Proof of Proposition 3.1

Proof: Given $L=q$ the FOC of (3.1) w.r.t. x_i can be represented as

$$\begin{aligned} &\mu_i' \sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)\left[U\left(A - \frac{1+k}{n} q - x_i \right) - U\left(A - \frac{k}{n} q - x_i \right) \right] \\ &= \sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)\left[\mu(x_i) U'\left(A - \frac{1+k}{n} q - x_i \right) + (1-\mu(x_i)) U'\left(A - \frac{k}{n} q - x_i \right) \right](1-C) \end{aligned} \quad \text{(A3.3)}$$

The left-hand side (LHS) of (A3.3) can be represented as

$$\mu_i' \left[EU\left(A - \frac{1+k}{n} L - x_i \right) - EU\left(A - \frac{k}{n} L - x_i \right) \right]$$

Let $A - x_i = W_i$, let l_1 and l_0 be random variables denoting the expected out-of-pocket money when firm *i* has a loss or no loss, respectively. Thus, $l_1 = \frac{1+k}{n} L$ and

$l_0 = \frac{k}{n}L$. Let l_1^i and l_0^i be the ith moment of l_1 and l_0, respectively. Then, with n members in a risk pool, we have

$$E\left(l_1^1\right) = n^{-1}\left[1+(n-1)\mu_i\right]L$$

$$E\left(l_0^1\right) = n^{-1}(n-1)\mu_i L$$

$$E\left(l_1^2\right) = n^{-2}\left[1+3(n-1)\mu_i+(n-1)(n-2)\mu_i^2\right]L^2$$

$$E\left(l_0^2\right) = n^{-2}\left[(n-1)\mu_i+(n-1)(n-2)\mu_i^2\right]L^2$$

$$E\left(l_1^3\right) = n^{-3}\left[1+7(n-1)\mu_i+6(n-1)(n-2)\mu_i^2+(n-1)(n-2)(n-3)\mu_i^3\right]L^3$$

$$E\left(l_0^3\right) = n^{-3}\left[(n-1)\mu_i+3(n-1)(n-2)\mu_i^2+(n-1)(n-2)(n-3)\mu_i^3\right]L^3$$

Then

$$EU(W-l) = \mu_i E\left[U(W)-l_1^1U'(W)+l_1^2U''(W)/2-l_1^3U'''(W)/6\right]$$
$$+(1-\mu_i)E\left[U(W)-l_0^1U'(W)+l_0^2U''(W)/2-l_0^3U'''(W)/6\right]$$

Using Taylor Expansion, the LHS of the FOC in (A2.1) can be transformed as

$$\mu_i'\left[U'(W)\left(E\left(l_0^1\right)-E\left(l_1^1\right)\right)-U''(W)\left(E\left(l_0^2\right)-E\left(l_1^2\right)\right)/2+U'''(W)\left(E\left(l_0^3\right)-E\left(l_1^3\right)\right)/6\right]$$

Since $\mu' < 0$, $E\left(l_0^2\right)-E\left(l_1^2\right)<0$, $E\left(l_0^3\right)-E\left(l_1^3\right)<0$, $U''(W)<0$, $U'''(W)>0$, The LHS of (A3.3) satisfies that

$$LHS < \mu_i'\left[U'(W)\left(E\left(l_0^1\right)-E\left(l_1^1\right)\right)\right] = -\mu_i'\left[U'(W)L/n\right] < -\mu_i'U'(W)L = -\mu_i'U'(A-x_i)L$$

Also, the right-hand side (RHS) of (A3)

$$\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)\left[\mu_i U'\left(A-\frac{1+k}{n}q-x_i\right)+(1-\mu_i)U'\left(A-\frac{k}{n}q-x_i\right)\right](1-C)$$
$$> U'(A-x_i)(1-C)$$

Therefore, we have

$$-\mu_i'U'(A-x_i)L > LHS = RHS > U'(A-x_i)(1-C)$$

and

$$\mu_i' < -\frac{(1-C)}{L}$$

Thus, the security investment if the case of RPA is less than that in the case of commercial insurance.

Proof of Proposition 3.2

Proof: We first show that when n is sufficiently large, firms do not form a single risk pool. To see that, note when $n \to \infty$, if firms form a single risk pool, each firm's expected utility is

$$\Pi_P(1) = U(A - \mu L - x) \tag{A3.4}$$

where μ is the equilibrium breach probability and x is the equilibrium security investment. The FOC of (A3.4) is $U'(A - \mu L - x)(C - 1) < 0$. Therefore, x=0. In other words, firms do not invest at all. Thus,

$$\Pi_P(1) = U(A - \mu(0)L) < \Pi_C = U(A - \mu(x_C)L - x_C) \tag{A3.5}$$

(A3.5) indicates that when n is sufficiently large, forming a single risk pool does not generate higher expected utilities for firms than using commercial insurance.

Note that when n firms form n/m^* risk pools, in symmetric equilibrium, all firms invest at the same level, regardless of which risk pool they participate in. Therefore, each firm's expected utility is $\Pi_P(m^*)$. Since $\Pi_P(m^*) > \Pi_C$, firms will form multiple risk pools instead of using commercial insurance.

Proof of Lemma 3.3

Proof: The first-derivative of firm i's expected utility w.r.t I_i

$$= \mu_i \sum_{k=0}^{n-1} b(k;(n-1),\mu_{-i}) U'\left(A - L + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) + \frac{(n-1-k)}{n} q + I_i - \mu_i I_i - x_i\right)(1-\mu_i)$$

$$+ (1-\mu_i) \sum_{k=0}^{n-1} b(k;(n-1),\mu_{-i}) U'\left(A - \frac{k}{n} q + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - \mu_i I_i - x_i\right)(-\mu_i)$$

$$= \mu_i(1-\mu_i)\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)\begin{pmatrix} U'\left(A-L+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+\frac{(n-1-k)}{n}q+I_i-\mu_i I_i-x_i\right) \\ -U'\left(A-\frac{k}{n}q+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu_i I_i-x_i\right)\end{pmatrix}$$

The second-derivative of firm *i*'s expected utility w.r.t I_i is

$$\mu_i(1-\mu_i)\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)\times$$

$$\begin{pmatrix} (1-\mu_i)U''\left(A-L+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+\frac{(n-1-k)}{n}q+I_i-\mu_i I_i-x_i\right) \\ +\mu_i U''\left(A-\frac{k}{n}q+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu_i I_i-x_i\right)\end{pmatrix}<0$$

When $I_i \le L-q$, we have $-L+\frac{(n-1-k)}{n}q+I_i<-\frac{k}{n}q$ and

$$U'\left(A-L+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+\frac{(n-1-k)}{n}q+I_i-\mu_i I_i-x_i\right)$$

$$-U'\left(A-\frac{k}{n}q+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu_i I_i-x_i\right)$$

$$>0$$

Therefore, the first-derivative of firm *i*'s expected utility w.r.t I_i is positive, and thus firm *i* will choose $I_i=L-q$.

Proof of Proposition 3.3

Proof: In the symmetric case, the FOC of (3.2) w.r.t. *q*, by the Envelop Theorem,

$$\mu_i\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\frac{(k+1)}{n}q-\mu(x_i)(L-q)-x_i\right)\left(-\frac{(k+1)}{n}+\mu_i-C\frac{\partial x_{-i}}{\partial q}\right)$$

$$+(1-\mu_i)\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\frac{k}{n}q-\mu(x_i)(L-q)-x_i\right)\left(-\frac{k}{n}+\mu_i-C\frac{\partial x_{-i}}{\partial q}\right)$$

$$=0$$

Then when q=0 and $\mu_i=\mu_{-i}=\mu$, the FOC can be represented as

$$\sum_{k=0}^{n-1} b\left(k;(n-1),\mu\right)\left(-\frac{(k+1)}{n}+\mu-\frac{nC}{n-1}\frac{\partial x_{-i}}{\partial q}\right)\mu+\sum_{k=0}^{n-1} b\left(k;(n-1),\mu\right)(1-\mu)\left(-\frac{k}{n}+\mu-C\frac{\partial x_{-i}}{\partial q}\right)$$

$$=\sum_{k=0}^{n-1} b\left(k;(n-1),\mu\right)\left(\frac{n-1}{n}\mu-\frac{k}{n}-C\frac{\partial x_{-i}}{\partial q}\right)$$

$$=\frac{n-1}{n}\mu-C\frac{\partial x_{-i}}{\partial q}-\frac{k}{n}\sum_{k=0}^{n-1} b\left(k;(n-1),\mu\right)$$

$$=\frac{n-1}{n}\mu_i-C\frac{\partial x_{-i}}{\partial q}-\frac{n-1}{n}\mu_{-i}\sum_{k=0}^{n-2} b\left(k;(n-2),\mu\right)$$

$$=\frac{n-1}{n}\left(\mu_i-\mu_{-i}\right)-C\frac{\partial x_{-i}}{\partial q}$$

$$=-C\frac{\partial x_{-i}}{\partial q}$$

Then if $-C\frac{\partial x_{-i}}{\partial q}\Big|_{q=0}>0$, we have $\frac{\partial \Pi_i}{\partial q}|_{q=0}>0$.

Next, we derive $\partial x_{-i}/\partial q$.

Note that given q and I, in the symmetric case, the FOC w.r.t. x_i satisfies that

$$\begin{aligned}0=\frac{\partial \Pi_i}{\partial x_i}&=\mu_i'\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)U\left(A-\frac{(k+1)}{n}q-\mu_i(L-q)-x_i\right)\\&+\mu_i\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\frac{(k+1)}{n}q-\mu_i(L-q)-x_i\right)\left(-\mu_i'(L-q)+C-1\right)\\&-\mu_i'\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)U\left(A-\frac{k}{n}q-\mu_i(L-q)-x_i\right)\\&+(1-\mu_i)\sum_{k=0}^{n-1} b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\frac{k}{n}q-\mu_i(L-q)-x_i\right)\left(-\mu_i'(L-q)+C-1\right)\\&=H\end{aligned}$$

By the Implicit Theorem

$$\frac{\partial x_i}{\partial q}=-\frac{\frac{\partial H}{\partial q}}{\frac{\partial H}{\partial x_i}}$$

$$\frac{\partial H}{\partial q}=\mu_i'\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\frac{(k+1)}{n}q-\mu_i(L-q)-x_i\right)\left(-\frac{(k+1)}{n}+\mu_i\right)$$
$$+\mu_i\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U''\left(A-\frac{(k+1)}{n}q-\mu_i(L-q)-x_i\right)\left(-\mu_i'(L-q)-1+C\right)\times\left(-\frac{(k+1)}{n}+\mu_i\right)$$
$$+\mu_i\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\frac{(k+1)}{n}q-\mu_i(L-q)-x_i\right)\mu_i'$$
$$-\mu'(x_i)\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\frac{k}{n}q-\mu_i(L-q)-x_i\right)\left(-\frac{k}{n}+\mu_i\right)$$
$$+(1-\mu_i)\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U''\left(A-\frac{k}{n}q-\mu_i(L-q)-x_i\right)\left(-\mu_i'(L-q)-1+C\right)\times\left(-\frac{k}{n}+\mu_i\right)$$
$$+(1-\mu_i)\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\frac{k}{n}q-\mu_i(L-q)-x_i\right)\mu_i'$$

Therefore, we have

$$\begin{aligned}\frac{\partial H}{\partial q}|_{q=0}&=\mu_i'\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\mu_iL-x_i\right)\left(-\frac{1}{n}\right)\\&\quad+\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\mu_iL-x_i\right)\mu_i'\\&=\mu_i'U'\left(A-\mu_iL-x_i\right)\left(-\frac{1}{n}\right)+U'\left(A-\mu_iL-x_i\right)\mu_i'\\&=U'\left(A-\mu_iL-x_i\right)\left(\frac{n-1}{n}\right)\mu_i'\end{aligned}$$

Moreover, tedious algebra shows that

$$\begin{aligned}\frac{\partial H}{\partial x}|_{q=0}&=\mu_i''\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U\left(A-\mu_iL-x_i\right)\\&\quad+\mu_i\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\mu_iL-x_i\right)\left(-\mu_i''L\right)\\&\quad-\mu_i''\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U\left(A-\mu_iL-x_i\right)\\&\quad+(1-\mu_i)\sum_{k=0}^{n-1}b\left(k;(n-1),\mu_{-i}\right)U'\left(A-\mu_iL-x_i\right)\left(-\mu_i''L\right)\\&=U'\left(A-\mu_iL-x_i\right)\left(-\mu_i''(L-q)\right)\end{aligned}$$

Therefore,

$$\frac{\partial x_i}{\partial q}|_{q=0} = -\frac{\frac{\partial H}{\partial q}}{\frac{\partial H}{\partial x_i}}|_{q=0} = -\frac{U'\left(A-\mu_i L-x_i\right)\left(\frac{n-1}{n}\right)\mu_i'}{U'\left(A-\mu_i L-x_i\right)\left(-\mu_i'' L\right)} = \frac{\left(n-1\right)\mu_i'}{nL\mu_i''} < 0$$

Thus, $\frac{\partial \Pi_i}{\partial q}|_{q=0} > 0$ and firms have an incentive to choose a q>0, i.e., use RPA.

Proof of Proposition 3.4

Proof: The main logic of the proof for this proposition is as follows. If there exists a case where firms form multiple pools to retain an amount q^m of risks, invest at x^m, and use commercial insurance to cover L- q^m, then we can also find a corresponding case where firms form a single pool to retain an amount $q < q^m$ of risks and invest at the same level x^m. With the same investment level but a single pool, firms are better off since they retain fewer risks within the single pool.

Consider two cases. First, firms form m pools and the size of each pool is $J=n/m$ (suppose that n can be divided by m). Suppose the firm's optimal security investment in this case is x^m, and the amount of loss covered by the risk pool is q^m, where m stands for "multiple pools". Also, denote x^c as the firm's equilibrium security investment when only commercial insurance is used. Therefore, we must have $x^m < x^c$. To see that, let $\Pi_c(x^c)$ denote a firm's expected utility when firms only use commercial insurance and invest at x^c, let $\Pi_c(x^m)$ denote a firm's expected utility when firms only use commercial insurance and invest at x^m, let $\Pi_m(x^m, q^m)$ denote a firm's expected utility when firms use the risk pools to cover q^m and invest at x^m. Therefore, the expected utility of a firm, say firm i, in the case of multiple pools is

$$\Pi_m\left(x^m, q^m\right) = \sum_{k=0}^{J-1} b\left(k;\left(J-1\right),\mu\right)\begin{pmatrix} \mu U\left(A-\frac{k+1}{J}q^m-\mu\left(L-q^m\right)-x^m\right) \\ +\left(1-\mu\right)U\left(A-\frac{k}{J}q^m-\mu\left(L-q^m\right)-x^m\right)\end{pmatrix}$$

Since x^c is higher than optimal investment level (i.e., overinvestment), if $x^m > x^c$, we must have $\Pi_c(x^m) < \Pi_c(x^c)$. Recall that when firms only use commercial insurance, they always buy full insurance. Since when using RPA, firms retain part of risks and do

not have the full insurance, we must have $\Pi_m(x^m, q^m) < \Pi_c(x^m)$. Therefore, if $x^m > x^c$, $\Pi_m(x^m, q^m) < \Pi_c(x^m) < \Pi_c(x^c)$ and firms are worse off by using RPA. In other words, if firms use multiple risk pools in equilibrium, we must have $x^m < x^c$.

Next, let $\Pi_s(x^s, q^m)$ denote a firm's expected utility when firms use a single risk pool to cover q^m (and use commercial insurance to cover $L-q^m$) and invest at the optimal level x^s. In the equilibrium, we must have $x^s < x^m$. This is because the single risk pool has more members to share the risks and therefore, the moral hazard problem is more severe. To see that, note that if firms form a single pool, the expected utility of a firm in the symmetric equilibrium is

$$\Pi_s\left(x^s, q^m\right) = \sum_{k=0}^{n-1} b\left(k;(n-1),\mu\right)\begin{pmatrix} \mu U\left(A - \frac{k+1}{n}q^m - \mu\left(L-q^m\right) - x^s\right) \\ +(1-\mu)U\left(A - \frac{k}{n}q^m - \mu\left(L-q^m\right) - x^s\right)\end{pmatrix}$$

Therefore, x^s satisfies the FOC:

$$\sum_{k=0}^{n-1} b\left(k;(n-1),\mu\right)\begin{pmatrix} \mu' U\left(A - \frac{k+1}{n}q^m - \mu\left(L-q^m\right) - x^s\right) \\ -\mu' U\left(A - \frac{k}{n}q^m - \mu\left(L-q^m\right) - x^s\right) \\ -\mu U'\left(A - \frac{k+1}{n}q^m - \mu\left(L-q^m\right) - x^s\right)\left(\mu'\left(L-q^m\right)+1-C\right) \\ -(1-\mu)U'\left(A - \frac{k}{n}q^m - \mu\left(L-q^m\right) - x^s\right)\left(\mu'\left(L-q^m\right)+1-C\right)\end{pmatrix} = 0$$

Suppose firms invest at x^m, following the same approach as in Lee and Ligon (2001), we ignore the high-order derivatives of $U(.)$ (i.e., higher than 3rd derivative).

$$\sum_{k=0}^{n-1} b\left(k;(n-1),\mu\right)\begin{pmatrix} \mu' U\left(A - \frac{k+1}{n}q^m - \mu\left(L-q^m\right) - x^m\right) \\ -\mu' U\left(A - \frac{k}{n}q^m - \mu\left(L-q^m\right) - x^m\right) \\ -\mu U'\left(A - \frac{k+1}{n}q^m - \mu\left(L-q^m\right) - x^m\right)\left(\mu'\left(L-q^m\right)+1-C\right) \\ -(1-\mu)U'\left(A - \frac{k}{n}q^m - \mu\left(L-q^m\right) - x^m\right)\left(\mu'\left(L-q^m\right)+1-C\right)\end{pmatrix} = 0$$

Let $A - \mu\left(L-q^m\right) - x^m = W$, firm i's expected utility can be represented as

$$\Pi_s\left(x^m, q^m\right) = \mu\sum_{k=0}^{n-1} b\left(k;(n-1),\mu\right)\left[U\left(W - \frac{k+1}{n}q^m\right)\right] + (1-\mu)\sum_{k=0}^{n-1} b\left(k;(n-1),\mu\right)\left[U\left(W - \frac{k}{n}q^m\right)\right]$$

Let l_1 and l_0 be random variables denoting the expected out-of-pocket money when firm i has a loss or no loss, respectively. Let Let $l_1{}^i$ and $l_0{}^i$ be the ith moment of l_1 and l_0, respectively. Then, with n members in a risk pool, we have

$$E\left(l_1^1\right)=n^{-1}\left[1+(n-1)\mu\right]q^m$$
$$E\left(l_0^1\right)=n^{-1}(n-1)\mu q^m$$
$$E\left(l_1^2\right)=n^{-2}\left[1+3(n-1)\mu+(n-1)(n-2)\mu^2\right]\left(q^m\right)^2$$
$$E\left(l_0^2\right)=n^{-2}\left[(n-1)\mu+(n-1)(n-2)\mu^2\right]\left(q^m\right)^2$$
$$E\left(l_1^3\right)=n^{-3}\left[1+7(n-1)\mu+6(n-1)(n-2)\mu^2+(n-1)(n-2)(n-3)\mu^3\right]\left(q^m\right)^3$$
$$E\left(l_0^3\right)=n^{-3}\left[(n-1)\mu+3(n-1)(n-2)\mu^2+(n-1)(n-2)(n-3)\mu^3\right]\left(q^m\right)^3$$

Then

$$E(W-l)=\mu E\left[U(W)-l_1^1U'(W)+l_1^2U''(W)/2-l_1^3U'''(W)/6\right]$$
$$+(1-\mu)E\left[U(W)-l_0^1U'(W)+l_0^2U''(W)/2-l_0^3U'''(W)/6\right]$$

Using Taylor Expansion, the FOC can be transformed as

$$\mu'\left[U'(W)\left(E\left(l_0^1\right)-E\left(l_1^1\right)\right)-U''(W)\left(E\left(l_0^2\right)-E\left(l_1^2\right)\right)/2+U'''(W)\left(E\left(l_0^3\right)-E\left(l_1^3\right)\right)/6\right] \quad \text{(A3.6)}$$
$$=\left[\mu EU\left(W-l_1^1\right)+(1-\mu)EU\left(W-l_0^1\right)\right]\left(\mu'\left(L-q^m\right)+1-C\right)$$

Also, using Taylor Expansion, the RHS of (A3.6) can be transformed as

$$\left[\mu EU\left(W-l_1^1\right)+(1-\mu)EU\left(W-l_0^1\right)\right]\left(\mu'\left(L-q^m\right)+1-C\right)$$
$$=\left[U'(W)-U''(W)\left(\mu E\left(l_1^1\right)+(1-\mu)E\left(l_0^1\right)\right)+U'''(W)\left(\mu E\left(l_1^2\right)+(1-\mu)E\left(l_0^2\right)\right)/2\right]\left(\mu'\left(L-q^m\right)+1-C\right)$$
$$=\left[U'(W)-U''(W)\mu q^m+U'''(W)\left(q^m\right)^2\left(\frac{\mu}{n}+\mu^2-\frac{\mu^2}{n}\right)/2\right]\left(\mu'\left(L-q^m\right)+1-C\right)$$

The LHS of (A3.6) can be transformed as

$$-\mu'\left[\begin{array}{l}U'(W)\left(n^{-1}q^m\right)-U''(W)\left(n^{-2}\left(1+2(n-1)\mu\right)\left(q^m\right)^2\right)/2\\+U'''(W)\left(n^{-3}\left(1+6(n-1)\mu+3(n-1)(n-2)\mu^2\right)\left(q^m\right)^3\right)/6\end{array}\right]$$

Therefore, the FOC can be transformed as

$$-\mu'\begin{bmatrix} U'(W)\left(n^{-1}q^m\right)-U''(W)\left(n^{-2}\left(1+2(n-1)\mu\right)\left(q^m\right)^2\right)/2 \\ +U'''(W)\left(n^{-3}\left(1+6(n-1)\mu+3(n-1)(n-2)\mu^2\right)\left(q^m\right)^3\right)/6 \end{bmatrix} \quad \text{(A3.7)}$$
$$=\left[U'(W)-U''(W)\mu q^m+U'''(W)\left(\frac{\mu}{n}+\mu^2-\frac{\mu^2}{n}\right)/2\right]\left(\mu'\left(L-q^m\right)+1-C\right)$$

For expositional purpose, we represent the FOC in (A3.7) as

$LHS_n = RHS_n$

Similarly, when firms form multiple risk pools with a size of j, the FOC for firm i is

$$-\mu'\begin{bmatrix} U'(W)\left(j^{-1}q^m\right)-U''(W)\left(j^{-2}\left(1+2(j-1)\mu\right)\left(q^m\right)^2\right)/2 \\ +U'''(W)\left(j^{-3}\left(1+6(j-1)\mu+3(j-1)(j-2)\mu^2\right)\left(q^m\right)^3\right)/6 \end{bmatrix} \quad \text{(A3.8)}$$
$$=\left[U'(W)-U''(W)\mu q^m+U'''(W)\left(\frac{\mu}{j}+\mu^2-\frac{\mu^2}{j}\right)/2\right]\left(\mu'\left(L-q^m\right)+1-C\right)$$

For expositional purpose, we represent the FOC in (A3.8) as

$LHS_j = RHS_j$

Note that $\frac{n}{j}LHS_n < LHS_j$ and $RHS_j < \frac{n}{j}RHS_n$. Therefore, when x^m satisfies the FOC $LHS_j = RHS_j$, it will make $LHS_n < RHS_n$. Since x^s satisfies that $LHS_n = RHS_n$, we must have $x^s<x^m$.

By assuming that the utility function $U(.)$ is well-behaved, $x^s(q)$ (i.e., the optimal investment x^s as a function of q) is a continuous function of q. Therefore, there exists a $q<q^m$ such that $x^s(q)=x^m$. In other words, firms can choose a $q<q^m$ to make the investment in a single pool equal to x^m. In this case, firms' investments in a single pool are equal to their investments in multiple pools but firms retain fewer risks in the single pool than in multiple pools. Consequently, firms' expected utilities in the case of a single pool are higher than their utilities in the case of multiple pools.

Proof of Proposition 3.5

Proof: When n approaches to the infinite, the number of firms who have the security breach approaches $n\mu$ (Law of large number). And the expected loss shared by the pool member approaches to μq. The risk pool provides full coverage to all the members and the shared loss is the "premium equivalence" that each pool member pays. We can rewrite the pool member's expected utility as

$$U\left(A-\mu q+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu_i\left(L-q\right)-x_i\right)$$

In the symmetric equilibrium, the expected utility becomes

$$U\left(A+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu L-x\right)$$

The expected utility function has the same form as that in the case of commercial insurance and the maximum profit can be achieved if all firms invest at the optimal.

Next we examine a firm's investment decision. The first-derivative of firm i's expected utility w.r.t x_i, $U'\left(A-\mu_i q+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu_i\left(L-q\right)-x_i\right)\left(C-\mu_i'\left(L-q\right)-1\right)=0$

$$\mu_i'=-\frac{1-C}{L-q}$$

With a single risk pool, firms can always collectively choose a q to induce the optimal security investment where for any firm i, the investment x_i satisfies that $\mu'\left(x_i\right)=-\frac{1}{L}$. To achieve that, q must satisfy that $q=CL$.

Proof of Overinvestment in the Case of Negative Externality

Firm i's expected utility is

$\mu_i U\left(A-L+I_i-\mu_i I_i-x_i\right)+\left(1-\mu_i\right)U\left(A-\mu_i I_i-x_i\right)$ where $\mu_i=\mu\left(x_i+\left(x_i-\frac{\sum x_{-i}}{n-1}\right)\right)$

FOC w.r.t. I, I_i=L. Firm i's expected utility is $U\left(A-\mu_i L-x_i\right)$

FOC w.r.t x_i, $\mu_i'\left(2x_i-\frac{\sum x_{-j}}{n-1}\right)=-\frac{1}{2L}$

In the symmetric case, where $x_i = x_{-i}$, the investment x_i satisfies that $\mu'(x_i) = -\frac{1}{2L}$

Next, consider the socially optimal case. Let x represents the socially optimal investment in the symmetric case. With the full insurance, the total expected utility of all firms is

$$\sum_i U\left(A - \mu_i L - x_i\right) = nU\left(A - \mu L - x\right)$$

FOC w.r.t. x is $U'\left(A - \mu(x)L - x\right)\left(-\mu'(x)L - 1\right) = 0$. Therefore, the socially optimal investment x satisfies that $\mu'(x) = -\frac{1}{L}$

Note that since $-\frac{1}{2L} > -\frac{1}{L}$, we have that $x_i > x$ and the firm I overinvests in x_i.

Proof of Proposition 3.6

Proof:

$$\begin{aligned}
\underset{I_x, I_y}{Max} \prod_i = {} & \mu_i \eta\left(y_i + \frac{\sum_{-i} y_{-i}}{n-1}\right) U\left(A - L_x - L_y + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) + I_{xi} + I_{yi} - \mu_i I_{xi} - \eta_i I_{yi} - x_i - y_i\right) \\
& + \mu_i\left[1 - \eta\left(y_i + \frac{\sum_{-i} y_{-i}}{n-1}\right)\right] U\left(A - L_x + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) + I_{xi} - \mu_i I_{xi} - \eta_i I_{yi} - x_i - y_i\right) \\
& + (1 - \mu_i)\eta\left(y_i + \frac{\sum_{-i} y_{-i}}{n-1}\right) U\left(A - L_y + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) + I_{yi} - \mu_i I_{xi} - \eta_i I_{yi} - x_i - y_i\right) \\
& + (1 - \mu_i)\left[1 - \eta\left(y_i + \frac{\sum_{-i} y_{-i}}{n-1}\right)\right] U\left(A + C\left(x_i - \frac{\sum_{-i} x_{-i}}{n-1}\right) - \mu_i I_{xi} - \eta_i I_{yi} - x_i - y_i\right)
\end{aligned}$$

The first-order condition (FOC) w.r.t. I_{xi} is

$$\mu_i\eta\left(y_i+\frac{\sum_{-i}y_{-i}}{n-1}\right)U'\left(A-L_x-L_y+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+I_{xi}+I_{yi}-\mu_iI_{xi}-\eta_iI_{yi}-x_i-y_i\right)(1-\mu_i)$$
$$+\mu_i\left[1-\eta\left(y_i+\frac{\sum_{-i}y_{-i}}{n-1}\right)\right]U'\left(A-L_x+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+I_{xi}-\mu_iI_{xi}-\eta_iI_{yi}-x_i-y_i\right)(1-\mu_i)$$
$$+(1-\mu_i)\eta\left(y_i+\frac{\sum_{-i}y_{-i}}{n-1}\right)U'\left(A-L_y+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+I_{yi}-\mu_iI_{xi}-\eta_iI_{yi}-x_i-y_i\right)(-\mu_i)$$
$$+(1-\mu_i)\left[1-\eta\left(y_i+\frac{\sum_{-i}y_{-i}}{n-1}\right)\right]U'\left(A+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu_iI_{xi}-\eta_iI_{yi}-x_i-y_i\right)(-\mu_i)$$
$$=0$$

The first-order condition (FOC) w.r.t. I_{yi} is

$$\mu_i\eta\left(y_i+\frac{\sum_{-i}y_{-i}}{n-1}\right)U'\left(A-L_x-L_y+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+I_{xi}+I_{yi}-\mu_iI_{xi}-\eta_iI_{yi}-x_i-y_i\right)(1-\eta_i)$$
$$+\mu_i\left[1-\eta\left(y_i+\frac{\sum_{-i}y_{-i}}{n-1}\right)\right]U'\left(A-L_x+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+I_{xi}-\mu_iI_{xi}-\eta_iI_{yi}-x_i-y_i\right)(-\eta_i)$$
$$+(1-\mu_i)\eta\left(y_i+\frac{\sum_{-i}y_{-i}}{n-1}\right)U'\left(A-L_y+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)+I_{yi}-\mu_iI_{xi}-\eta_iI_{yi}-x_i-y_i\right)(1-\eta_i)$$
$$+(1-\mu_i)\left[1-\eta\left(y_i+\frac{\sum_{-i}y_{-i}}{n-1}\right)\right]U'\left(A+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu_iI_{xi}-\eta_iI_{yi}-x_i-y_i\right)(-\eta_i)$$
$$=0$$

In a symmetric case, $I_{xi}=L_x$ and $I_{yi}=L_y$

$$U\left(A+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu_iL_x-\eta_iL_y-x_i-y_i\right)$$

Given the budget constraint, FOCs with respect to x_i and y_i satisfy,

$$U'\left(A+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu_iL_x-\eta_iL_y-x_i-y_i\right)(C-\mu_i'L_x-1)$$
$$=U'\left(A+C\left(x_i-\frac{\sum_{-i}x_{-i}}{n-1}\right)-\mu_iL_x-\eta_iL_y-x_i-y_i\right)(-\eta_i'L_y-1)$$

That is, $\mu_{iu}'L_x=\eta_{iu}'L_y+C$

where subscript "*u*" represents underinvestment case. Given $\mu''>0$, it is easy to see that x_{iu} increases in *C* and y_{iu} decreases in *C*.

FOCs in the first-best case satisfy,

$\mu'_{io} L_x = 2\eta'_{io} L_y$

where subscript "*o*" represents the first-best case.

Given $\eta'_{iu} L_y + C > 2\eta'_{io} L_y$, we can conclude that $x_{iu} > x_{io}$ and hence $y_{iu} < y_{io}$.

APPENDIX FOR CHAPTER 4

Proof for Proposition 4.1

Proof:: If a low-type vendor mimics a high-type vendor, its profit can be represented as

$$\hat{r} s_h + r_h (1 - s_h) - \frac{k_l}{s_h}$$

The incentive constraint for a low-type vendor can be represented as

$$\hat{r} s_h - \hat{r}_l s_h + r_l - 2\sqrt{k_l (r_l - \hat{r}_l)} > \hat{r} s_h + r_h (1 - s_h) - \frac{k_l}{s_h}$$

$$(r_h - \hat{r}_l) s_h^2 + \left(r_l - r_h - 2\sqrt{k_l (r_l - \hat{r}_l)} \right) s_h + k_l > 0$$

We can derive the marginal release times which prevent the low-type vendor from mimicking as follows.

$$s_h^{n*} = \frac{r_h - r_l + 2\sqrt{k_l (r_l - \hat{r}_l)} - \sqrt{\left(r_h - r_l + 2\sqrt{k_l (r_l - \hat{r}_l)} \right)^2 - 4k_l (r_h - \hat{r}_l)}}{2(r_h - \hat{r}_l)}$$

$$s_h^{n**} = \frac{r_h - r_l + 2\sqrt{k_l (r_l - \hat{r}_l)} + \sqrt{\left(r_h - r_l + 2\sqrt{k_l (r_l - \hat{r}_l)} \right)^2 - 4k_l (r_h - \hat{r}_l)}}{2(r_h - \hat{r}_l)}$$

Thus, the equilibrium release time for a high-type vendor must satisfy

$$s_h < s_h^{n*}$$

Next we consider the incentive constraint of a high-type vendor. If a high-type vendor deviates from its equilibrium release time, its profit can be represented as

$$\pi_{hl}^{n} = \int_0^{s_h} \hat{r} dt + \int_{s_h}^{s} \hat{r}_l dt + \int_s^T r_l dt - C_h(s)$$
$$= \hat{r} s_h - \hat{r}_l s_h + r_l - (r_l - \hat{r}_l) s - \frac{k_h}{s}$$

Using FOC, we can derive the release time and the profit for a high-type vendor if it chooses to deviate as follows.

$$s_{hl}^{n} = \sqrt{\frac{k_h}{r_l - \hat{r}_l}}$$
$$\pi_{hl}^{n} = \hat{r} s_h - \hat{r}_l s_h + r_l - 2\sqrt{k_h (r_l - \hat{r}_l)}$$

The incentive constraint for a high-type vendor can be represented as

$$r_h - (r_h - \hat{r}) s_h - \frac{k_h}{s_h} \geq \hat{r} s_h - \hat{r}_l s_h + r_l - 2\sqrt{k_h (r_l - \hat{r}_l)}$$
$$(r_h - \hat{r}_l) s_h^2 - \left(r_h - r_l + 2\sqrt{k_h (r_l - \hat{r}_l)}\right) s_h + k_h \leq 0$$

We can derive the marginal release times as

$$s_{hl}^{n*} = \frac{r_h - r_l + 2\sqrt{k_h (r_l - \hat{r}_l)} - \sqrt{\left(r_h - r_l + 2\sqrt{k_h (r_l - \hat{r}_l)}\right)^2 - 4k_h (r_h - \hat{r}_l)}}{2(r_h - \hat{r}_l)}$$
$$s_{hl}^{n**} = \frac{r_h - r_l + 2\sqrt{k_h (r_l - \hat{r}_l)} + \sqrt{\left(r_h - r_l + 2\sqrt{k_h (r_l - \hat{r}_l)}\right)^2 - 4k_h (r_h - \hat{r}_l)}}{2(r_h - \hat{r}_l)}$$
$$s_{hl}^{n*} \leq s_h \leq s_{hl}^{n**}$$

Thus, the equilibrium release time for high-type vendors should satisfy $s_h \in \left[s_{hl}^{n*}, \min\{s_h^{n*}, s_{hl}^{n**}\} \right]$. The sufficient and necessary condition under which a normal separating equilibrium exists is $s_{hl}^{n*} \leq s_h^{n*}$. That is,

$$\sqrt{r_h - r_l}\left(\sqrt{(r_h - r_l) + 4\sqrt{k_l}\left(\sqrt{r_l - \hat{r}_l} - \sqrt{k_l}\right)} - \sqrt{(r_h - r_l) + 4\sqrt{k_h}\left(\sqrt{r_l - \hat{r}_l} - \sqrt{k_h}\right)}\right)$$
$$\leq 2\sqrt{r_l - \hat{r}_l}\left(\sqrt{k_l} - \sqrt{k_h}\right)$$

If $s_h^p \in \left[s_{hl}^{n*}, \min\{s_h^{n*}, s_{hl}^{n**}\} \right]$,

$\left\{ \left(s_h^p, s_l^c \right), s_h^p < s_l^c, \Pr_{t \in \left[0, s_h^p\right)} \left(h \mid A_t = 0 \right) = \delta, \Pr_{t \in \left[0, s_h^p\right]} \left(h \mid A_t = 1 \right) = 1, \Pr_{t \in \left[s_h^p, T \right]} \left(h \mid A_{s_h} = 0 \right) = 0 \right\}$ is the normal separating equilibrium.

If $s_h^p > \min\{s_h^{n*}, s_{hl}^{n**}\}$,

$\left\{ \left(s_h^n, s_l^c \right), s_h^n < s_l^c, \Pr_{t \in \left[0, s_h^n\right)} \left(h \mid A_t = 0 \right) = \delta, \Pr_{t \in \left[0, s_h^n\right]} \left(h \mid A_t = 1 \right) = 1, \Pr_{t \in \left[s_h^n, T \right]} \left(h \mid A_{s_h} = 0 \right) = 0 \right\}$ is the normal separating equilibrium where $s_h^n = \min\{s_h^*, s_{hl}^{**}\}$

Proof of Proposition 4.2

Proof: Suppose that $s_l^{'} = s_l^p$. That is, the marginal belief is equal to the release time for a low-type vendor in the partially incomplete information case. We can derive the equilibrium release time and the profit for a low-type vendor as follows.

$$s_l = s_l^p = \sqrt{\frac{k_l}{r_l - \hat{r}}}$$

$$\pi_l = \pi_l^p = r_l - 2\sqrt{k_l \left(r_l - \hat{r} \right)}$$

Since low-type vendors reveal their type right after they release patches, its release time and profit are exactly the same as that in the partially incomplete information case.

If a low-type vendor delays the release time, its profit can be represented as

$$\max \int_0^{s_l^p} \hat{r} dt + \int_{s_l^p}^{s} \hat{r}_h dt + \int_s^T r_l dt - C_l(s)$$

$$= r_l - r_l s + \hat{r}_h \left(s - s_l^p \right) + \hat{r} s_l^p - \frac{k_l}{s}$$

Using FOC, we can obtain the equilibrium release time and the profit for a low-type vendor who deviates from the equilibrium path.

$$s_{lh} = \sqrt{\frac{k_l}{r_l - \hat{r}_h}}$$

$$\pi_{lh} = r_l - \frac{\hat{r}_h - \hat{r}}{r_l - \hat{r}}\sqrt{k_l\left(r_l - \hat{r}\right)} - 2\sqrt{k_l\left(r_l - \hat{r}_h\right)}$$

The incentive constraint should satisfied

$$r_l - 2\sqrt{k_l\left(r_l - \hat{r}\right)} > r_l - \frac{\hat{r}_h - \hat{r}}{r_l - \hat{r}}\sqrt{k_l\left(r_l - \hat{r}\right)} - 2\sqrt{k_l\left(r_l - \hat{r}_h\right)}$$

$$0 > \left(r_l - \hat{r}_h - \left(r_l - \hat{r}\right)\right)^2 \qquad \text{(A4.1)}$$

which is impossible to hold. The belief and vendors' strategies are not consistent.

Suppose that $s_l^{'} \in \left[0, s_l\right)$, a low-type vendor's profit by choosing any release time in the range $\left[0, s_l^{'}\right)$ is less than π_l. If the vendor choose the release time s_{lh}, its profit is higher than π_{lh}. From (A4.1), $\pi_{lh} > \pi_l$. The vendor will not release patch at any time within $\left[0, s_l\right)$. The belief and vendors' strategies are not consistent.

Suppose that $s_l^{'} \in \left[s_{lh}, s_h\right)$. The vendor obtains the maximal profit at $s_l^{'}$ in the range $\left[s_l^{'}, s_h\right)$. But the profit is lower than what it can get by choosing s_l. The belief and vendors' strategy are not consistent.

Overall, we conclude that there is no pure strategy equilibrium.

Proof of Proposition 4.3

Proof:: Suppose that the equilibrium release time for low-type vendors follows the distribute $\sigma_l\left(t\right)$ on $\left[s_l^{'}, s_l^{''}\right]$. $\sigma_l\left(t\right) = \Pr\left(s_l \le t\right)$. Given $\sigma_l\left(t\right)$, we can derive consumers' belief at any time, $\delta\left(t\right) = \Pr\left(h \mid A_t = 0\right)$, using Bayes' rule. $\delta\left(s_l^{'}\right) = \delta$ and $\delta\left(s_l^{''}\right) = 1$

From $\delta\left(t\right)$, we can obtain the distribution of the release time σ_l. For notation simplicity, we use a to represent $A_t = 0$

$$\begin{aligned}\delta(t) &= \Pr(h \mid a) \\ &= \frac{\Pr(a \mid h)\Pr(h)}{\Pr(a)} \\ &= \frac{\Pr(a \mid h)\Pr(h)}{\Pr(a \mid h)\Pr(h) + \Pr(a \mid l)\Pr(l)}\end{aligned}$$

Given $\Pr(a \mid h) = 1$. $\Pr(a \mid l) = 1 - \sigma_l(t)$. $\Pr(h) = \delta$. $\Pr(l) = 1 - \delta$.

$$\delta(t) = \frac{\delta}{\delta + (1 - \sigma_l(t))(1 - \delta)} \tag{A4.2}$$

And the instantaneous reputation can be represented as

$$r(t) = \delta(t)\hat{r}_h + (1 - \delta(t))\hat{r}_l \tag{A4.3}$$

Next we derive the reputation function which leads to a equal profit for low-type vendors on $[s_l', s_l'']$. If it chooses the release time t, a low-type vendor's profit function can be represented as

$$\int_0^{s_l'} \hat{r} d\tau + \int_{s_l'}^{t} r(\tau) d\tau + \int_t^1 r_l d\tau - \frac{k_l}{t} = Const \tag{A4.4}$$

Differentiate (A4.4) w.r.t. t

$$r(t) - r_l + \frac{k_l}{t^2} = 0$$

$$r(t) = r_l - \frac{k_l}{t^2} \tag{A4.5}$$

From (A4.3)

$$\delta(t)\hat{r}_h + (1 - \delta(t))\hat{r}_l = r_l - \frac{k_l}{t^2}$$

$$\delta(t) = \frac{r_l - \hat{r}_l}{\hat{r}_h - \hat{r}_l} - \frac{k_l}{(\hat{r}_h - \hat{r}_l)t^2}$$

At $t = s_l'$, $\delta(t)$ should be δ,

$$\delta = \frac{r_l - \hat{r}_l}{\hat{r}_h - \hat{r}_l} - \frac{k_l}{(\hat{r}_h - \hat{r}_l)t^2}$$

$$s_l^{'} = s_l^p = \sqrt{\frac{k_l}{r_l - \hat{r}}}$$

At $t = s_l^{''}$, $\delta(t)$ should be 1,

$$1 = \frac{r_l - \hat{r}_l}{\hat{r}_h - \hat{r}_l} - \frac{k_l}{(\hat{r}_h - \hat{r}_l)t^2}$$

$$s_l^{''} = s_{lh} = \sqrt{\frac{k_l}{r_l - \hat{r}_h}}$$

From (A4.2)

$$\sigma_l(t) = \frac{\delta(t) - \delta}{(1-\delta)\delta(t)}$$

$$= \frac{1}{1-\delta} - \frac{\delta}{(1-\delta)\delta(t)}$$

$$= \frac{1}{1-\delta} - \frac{\delta(\hat{r}_h - \hat{r}_l)}{(1-\delta)\left(r_l - \hat{r}_l - \frac{k_l}{t^2}\right)}$$

$\sigma_l(t)$ satisfies $\sigma_l\left(s_l^p\right) = 0$ and $\sigma(s_{lh}) = 1$.

Therefore, we suppose the belief profile as

$$\mu = \left\{ \Pr_{t \in [0, s_l^p)}(h \mid A_t = 0) = \delta, \Pr_{t \in [s_l^p, s_{lh}]}(h \mid A_t = 0) = \frac{r_l - \hat{r}_l}{\hat{r}_h - \hat{r}_l} - \frac{k_l}{(\hat{r}_h - \hat{r}_l)t^2}, \Pr_{t \in (s_{lh}, s_h)}(h \mid A_t = 0) = 1, \right.$$

$$\left. \Pr_{t \in [0, s_h)}(h \mid A_t = 1) = 0, \Pr_{t \in [s_h, 1]}\left(h \mid A_{(s_h)^-} = 0\right) = 1 \right\}$$

The low-type vendor's profit is $r_l - 2\sqrt{k_l(r_l - \hat{r})}$

Following the analysis in proof for proposition 2, we can also obtain that the low-type vendor will not deviate to any time in the range $\left[0, s_l^p\right)$ or (s_{lh}, s_h).

And a high-type vendor's equilibrium profit can be represented as

$$\pi_h = \int_0^{s_l^p} \hat{r}dt + \int_{s_l^p}^{s_{lh}} r(t)\,dt + \int_{s_{lh}}^{s_h} \hat{r}_h dt + \int_{s_h}^{T} r_h dt - C_h(s_h)$$

$$= \int_0^{s_l^p} \hat{r}dt + \int_{s_l^p}^{s_{lh}} \left(r_l - \frac{k_l}{t^2}\right)dt + \int_{s_{lh}}^{s_h} \hat{r}_h dt + \int_{s_h}^{T} r_h dt - C_h(s_h)$$

$$= \hat{r}s_l^p + r_l\left(s_{lh} - s_l^p\right) + \frac{k_l}{s_{lh}} - \frac{k_l}{s_l^p} + \hat{r}_h\left(s_h - s_{lh}\right) + r_h\left(1 - s_h\right) - \frac{k_h}{s_h}$$

$$= 2\sqrt{k_l\left(r_l - \hat{r}_h\right)} - 2\sqrt{k_l\left(r_l - \hat{r}\right)} + r_h + \left(\hat{r}_h - r_h\right)s_h - \frac{k_h}{s_h}$$

If a low-type vendor mimics the high-type vendor by choosing the equilibrium release time for high-type vendors, its profit can be represented as

$$\int_0^{s_l^p} \hat{r}dt + \int_{s_l^p}^{s_{lh}} r(t)\,dt + \int_{s_{lh}}^{s_h} \hat{r}_h dt + \int_{s_h}^{T} r_h dt - C_l(s_h)$$

$$= 2\sqrt{k_l\left(r_l - \hat{r}_h\right)} - 2\sqrt{k_l\left(r_l - \hat{r}\right)} + r_h + \left(\hat{r}_h - r_h\right)s_h - \frac{k_l}{s_h}$$

Then a low-type vendor's incentive constraint can be represented as

$$r_l - 2\sqrt{k_l\left(r_l - \hat{r}\right)} \geq 2\sqrt{k_l\left(r_l - \hat{r}_h\right)} - 2\sqrt{k_l\left(r_l - \hat{r}\right)} + r_h + \left(\hat{r}_h - r_h\right)s_h - \frac{k_l}{s_h}$$

$$r_l \geq 2\sqrt{k_l\left(r_l - \hat{r}_h\right)} + r_h + \left(\hat{r}_h - r_h\right)s_h - \frac{k_l}{s_h}$$

$$\left(r_h - \hat{r}_h\right)s_h^2 - \left(r_h - r_l + 2\sqrt{k_l\left(r_l - \hat{r}_h\right)}\right)s_h + k_l \geq 0$$

We can derive the marginal release times which prevent low-type vendors from mimicking high-type vendors as follows.

$$s_h^{a*} = \frac{r_h - r_l + 2\sqrt{k_l\left(r_l - \hat{r}_h\right)} - \sqrt{\left(r_h - r_l + 2\sqrt{k_l\left(r_l - \hat{r}_h\right)}\right)^2 - 4k_l\left(r_h - \hat{r}_h\right)}}{2\left(r_h - \hat{r}_h\right)}$$

$$s_h^{a**} = \frac{r_h - r_l + 2\sqrt{k_l\left(r_l - \hat{r}_h\right)} + \sqrt{\left(r_h - r_l + 2\sqrt{k_l\left(r_l - \hat{r}_h\right)}\right)^2 - 4k_l\left(r_h - \hat{r}_h\right)}}{2\left(r_h - \hat{r}_h\right)}$$

High-type vendors' release time must satisfy

$$s_h \geq s_h^{a**}$$

Next we check whether a high-type vendor will choose a time in the range $[0, s_{lh}]$.

Consider the belief profile

$$\mu' = \left\{ \Pr_{t\in[0,,s_{lh}]}(h \mid A_t = 0) = \delta, \Pr_{t\in(s_{lh},s_h)}(h \mid A_t = 0) = 1, \Pr_{t\in[0,,s_h)}(h \mid A_t = 1) = 0, \right.$$
$$\left. \Pr_{t\in[s_h,1]}\left(h \mid A_{(s_h)^-} = 0\right) = 1 \right\}.$$

The high-type vendor will choose s_{lh} as the release time if $\sqrt{\frac{k_h}{r_l - \hat{r}}} > s_{lh} = \sqrt{\frac{k_l}{r_l - \hat{r}_h}}$.

The release time that a high-type vendor chooses with the belief profile μ is no earlier than that with μ'. s_{lh} will be the release time that a high-type vendor choose in the range $[0, s_{lh}]$ with belief μ. Consequently, this case merges to the next case we consider.

Consider the case that the high-type vendor chooses an earlier release time in the range $[s_{lh}, s_h)$, we can derive its release time and profit as follows.

$$\max_s \int_0^{s_l^p} \hat{r} dt + \int_{s_l^p}^{s_{lh}} r(t)\, dt + \int_{s_{lh}}^{s} \hat{r}_h dt + \int_s^T r_l dt - C_h(s)$$
$$= 2\sqrt{k_l(r_l - \hat{r}_h)} - 2\sqrt{k_l(r_l - \hat{r})} + r_l + (\hat{r}_h - r_l)s - \frac{k_h}{s}$$
$$s_{hl} = \sqrt{\frac{k_h}{r_l - \hat{r}_h}}$$

$$\pi_{hl} = 2\sqrt{k_l(r_l - \hat{r}_h)} - 2\sqrt{k_l(r_l - \hat{r})} + r_l - 2\sqrt{k_h(r_l - \hat{r}_h)}$$

Since $k_l < k_h$, $s_{hl} > s_{lh}$.

Then the high-type vendor's incentive constraint can be represented as

$$2\sqrt{k_l(r_l - \hat{r}_h)} - 2\sqrt{k_l(r_l - \hat{r})} + r_h + (\hat{r}_h - r_h)s_h - \frac{k_h}{s_h} \geq 2\sqrt{k_l(r_l - \hat{r}_h)} - 2\sqrt{k_l(r_l - \hat{r})} + r_l - 2\sqrt{k_h(r_l - \hat{r}_h)}$$
$$r_h + (\hat{r}_h - r_h)s_h - \frac{k_h}{s_h} \geq r_l - 2\sqrt{k_h(r_l - \hat{r}_h)}$$
$$(r_h - \hat{r}_h)s_h^2 - \left(r_h - r_l + 2\sqrt{k_h(r_l - \hat{r}_h)}\right)s_h + k_h \leq 0$$

We can derive the marginal release times as

$$s_{hl}^{a*}=\frac{r_h-r_l+2\sqrt{k_h\left(r_l-\hat{r}_h\right)}-\sqrt{\left(r_h-r_l+2\sqrt{k_h\left(r_l-\hat{r}_h\right)}\right)^2-4k_h\left(r_h-\hat{r}_h\right)}}{2\left(r_h-\hat{r}_h\right)}$$

$$s_{hl}^{a**}=\frac{r_h-r_l+2\sqrt{k_h\left(r_l-\hat{r}_h\right)}+\sqrt{\left(r_h-r_l+2\sqrt{k_h\left(r_l-\hat{r}_h\right)}\right)^2-4k_h\left(r_h-\hat{r}_h\right)}}{2\left(r_h-\hat{r}_h\right)}$$

A high-type vendor's equilibrium release time must satisfy

$$s_{hl}^{a*}\le s_h\le s_{hl}^{a**}$$

Overall, the equilibrium release time must satisfy $s_h\in\left[\max\left\{s_h^{a**},s_{hl}^{a*}\right\},s_{hl}^{a**}\right]$.

The existence of an atypical separating equilibrium requires $s_h^{a**}\le s_{hl}^{a**}$ and $\sqrt{\frac{k_h}{r_l-\hat{r}}}>\sqrt{\frac{k_l}{r_l-\hat{r}_h}}$

$$\frac{r_h-r_l+2\sqrt{k_l\left(r_l-\hat{r}_h\right)}+\sqrt{\left(r_h-r_l+2\sqrt{k_l\left(r_l-\hat{r}_h\right)}\right)^2-4k_l\left(r_h-\hat{r}_h\right)}}{2\left(r_h-\hat{r}_h\right)}$$

$$<\frac{r_h-r_l+2\sqrt{k_h\left(r_l-\hat{r}_h\right)}+\sqrt{\left(r_h-r_l+2\sqrt{k_h\left(r_l-\hat{r}_h\right)}\right)^2-4k_h\left(r_h-\hat{r}_h\right)}}{2\left(r_h-\hat{r}_h\right)}$$

$$\sqrt{r_h-r_l}\left(\sqrt{r_h-r_l+4\sqrt{k_l\left(r_l-\hat{r}_h\right)}-4k_l}-\sqrt{r_h-r_l+4\sqrt{k_h\left(r_l-\hat{r}_h\right)}-4k_h}\right)$$

$$<2\sqrt{r_l-\hat{r}_h}\left(\sqrt{k_h}-\sqrt{k_l}\right)$$

and

$$\sqrt{\frac{k_h}{r_l-\hat{r}}}>\sqrt{\frac{k_l}{r_l-\hat{r}_h}}$$

If $s_h^c\in\left[\max\left\{s_h^{a**},s_{hl}^{a*}\right\},s_{hl}^{a**}\right]$,

$\left\{\sigma_l,s_h^c,s_l^p<s_h^c,\Pr_{t\in\left[0,s_l^p\right)}\left(h\mid A_t=0\right)=\delta,\Pr_{t\in\left[s_l^p,s_{lh}\right]}\left(h\mid A_t=0\right)=\frac{r_l-\hat{r}_l}{\hat{r}_h-\hat{r}_l}-\frac{k_l}{\left(\hat{r}_h-\hat{r}_l\right)t^2},\Pr_{t\in\left[0,s_h^c\right)}\left(h\mid A_t=1\right)=0,\right.$

$\left.\Pr_{t\in\left(s_{lh},s_h^c\right)}\left(h\mid A_t=0\right)=1,\Pr_{t\in\left[s_h^c,1\right]}\left(h\mid A_{\left(s_h^c\right)^-}=0\right)=1\right\}$ is an atypical separating equilibrium.

If $s_h^c < \max\left\{s_h^{a**}, s_{hl}^{a*}\right\}$,

$\left\{\sigma_l, s_h^a, s_l^p < s_h^a, \Pr_{t\in\left[0,s_l^p\right)}\left(h \mid A_t = 0\right) = \delta, \Pr_{t\in\left[s_l^p, s_{lh}\right]}\left(h \mid A_t = 0\right) = \frac{r_l - \hat{r}_l}{\hat{r}_h - \hat{r}_l} - \frac{k_l}{(\hat{r}_h - \hat{r}_l)t^2}, \Pr_{t\in\left[0,s_h^a\right)}\left(h \mid A_t = 1\right) = 0,\right.$

$\left.\Pr_{t\in\left(s_{lh}, s_h^a\right)}\left(h \mid A_t = 0\right) = 1, \Pr_{t\in\left[s_h^a, 1\right]}\left(h \mid A_{(s_h^a)^-} = 0\right) = 1\right\}$ is an atypical separating equilibrium

where $s_h^a = \max\left\{s_h^{a**}, s_{hl}^{a*}\right\}$

Bibliography

Akerlof, G. 1970. The market for lemons: Quality uncertainty and the market mechanism. *Quarterly Journal of Economics* 84 488-500

Anderson, R. 2001. Why Information Security is Hard - An Economic Perspective. *Working paper*, University of Cambridge Computer laboratory, Cambridge, UK. http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf

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

Arora, A., J. P. Caulkins, R. Telang. 2006a. Research note-Sell first, fix later: Impact of patching on software quality. *Management Science* 52(3) 465-471

Arora, A., C. Forman, A. Nandkumar, R. Telang. 2006b. Competition and quality restoration: an empirical analysis of vendor response to software vulnerability. *Proceedings of the Workshop on the Economics of Information Security (WEIS2006)*, University of Cambridge, UK

Arora, A., R. Krishnan, R. Telang; Y. Yang. 2005. An empirical analysis of vendor response of software vulnerability disclosure. *SSRN Working Paper* http://ssrn.com/abstract=786128

Arora, A., A. Nandkumar, R. Telang. 2006c. Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information System Frontier* 8(5) 350-362

Arora A., R. Telang. 2005. Economics of software vulnerability disclosure. *IEEE Security and Privacy* 20-25 January/February 2005

Arora, A., R. Telang, H. Xu. 2007. Optimal Policy for Software Vulnerability Disclosure. *Working Paper*, Carnegie Mellow University

Asmussen, S., R. Y. Rubinstein. 1999. Sensitivity analysis of insurance risk models via simulation. *Management Science* 45(8) 1125-1142

August, T., T. I. Tunca. 2006a. Network software security and user incentives. *Management Science*, 52(11) 1703-1720

August, T., T. I. Tunca. 2006b. Let the pirates patch? An economic analysis of network software security patch restrictions. *Working Paper*, University of Stanford

Bailey Jr., A. D., G. L. Duke, J. Gerlach, C. Ko, R. D. Meservy, A. B. Whinston. 1985. TICOM And The Analysis Of Internal Controls. *Accounting Review* 60(2) 186-202

Banerjee, A, D. Fudenberg. 2004. Word-of-Mouth learning. *Games and Economic Behavior*. 46 1-22

Berman, F., H. Brady. 2006. Final Report: NSF SBE-CISE Workshop on Cyberinfrastructure and the Social Sciences

Camp, J. L., C. Wolfram. 2000. Pricing security. *Proceedings of the CERT Information Survivability Workshop*, Boston, MA 31-39

Campbell, K., L. Gordon, M. Loeb. 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., H Cavusoglu, S. Raghunathan. 2007. Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. *IEEE Transactions on Software Engineering* 33(3) 171-185

Cavusoglu, H., B. Mishra, S. Raghunathan. 2004a. The effect of internet security breach announcements on market value: capital market reaction for breached firms and Internet security developers. *International Journal of Electronic Commerce* 9(1) 69-105

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

Cavusoglu, H., B. Mishra, S. Raghunathan. 2005. The value of intrusion detection systems in information technology security architecture. *Information Systems Research* 16(1) 28-46

Celent. 2006. IT security issues in insurance. Report published by Celent

Cho, I-K, D. M. Kreps. 1987. Signaling game and stable equilibrium. *Quarterly Journal of Economics* 102 179-221

Choi, J.P., C. Fershtman, N. Gandal. 2007. Network security: Vulnerabilities and disclosure policy. *Proceedings of the Workshop on the Economics of Information Security (WEIS2007),* Carnegie Mellon University, Pittsburgh, PA

Cummins, J. D., M. A. Weiss. 1999. Organizational form and efficiency: The coexistence of stock and mutual property-liability insurers. *Management Science* 45(9) 1254-1270

Cusumano, M.A. 2004. Who is liable for bugs and security flaws in software? *Communications of the ACM* 47(3) 25-27

Dulleck, U. and R. Kerschbamer. 2006 On doctors, mechanics, and computer specialists: the economics of credence goods. *Journal of Economic Literature*. XLIV 5-42

Doherty, N. A., G. Dionne. 1993. Insurance with undiversifiable risk: Contract structure and organizational form of insurance firms. *Journal of Risk and Uncertainty* 6 187-203

Dynes, S., H. Brechbuhl, M. E. Johnson. 2005. Information security in the extended enterprise: some initial results from a field study of an industrial firm. *Glassmeyer/McNamee Center for Digital Strategies, Tuck School of Business at Dartmouth, Working Paper Series 05-1* http://mba.tuck.dartmouth.edu/digital/Research/AcademicPublications/InfoSecurity.pdf

Ekmekci, M. 2005. Sustainable reputations with rating systems. *Working paper*, Princeton University

Ellison, G., D. Fudenberg. 1995. Word-of-Mouth communication and social learning. *Quarterly Journal of Economics* 110(1) 93-125

Gal-Or, E., A. Ghose. 2005. The economic incentives for sharing security information. *Information Systems Research* 16(2) 186-208

Garfinkel, R., R. Gopal, P. Goes. 2002. Privacy protection of binary confidential data against deterministic, stochastic, and insider threat. *Management Science* 48(6) 749-764

Gattiker, U. E., H. Kelley. 1999. Morality and computers: Attitudes and differences in moral judgments. *Information Systems Research* 10(3) 233-255

Gibbons, R. 1992. *Game Theory for Applied Economists*. Princeton University Press, Princeton, New Jersey

Ghose, A., U. Rajan. 2006. The economic impact of regulatory information disclosure on information security investments, competition, and social welfare. *Proceedings of the Workshop on the Economics of Information Security (WEIS2006),* University of Cambridge, UK

Gordon, L.A., M. P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security* 5(4) 438-457

Gordon, L. A., M. P. Loeb. 2006. Budgeting process for information security expenditure. *Communications of the ACM* 49(1) 121-125

Gordon, L. A., M.P. Loeb, W. Lucyshyn, R. Richardson, 2007. Eleventh annual CSI/FBI computer crime and security survey 2006. *Computer Security Institute*

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

Gordon, L. A., W. Lucyshyn. 2003. Sharing information on computer system security: An economic analysis. *Journal of Accounting and Public Policy* 22 461-485

Holmstrom, B. 1982. Moral hazard in teams. *Bell Journal of Economics* 13(2) 324-340

Huang, Y., X. Geng, A. B. Whinston. 2007. Defeating DDoS attacks by fixing the incentive chain. *ACM Transactions on Internet Technology* 7(2)

Huang, C.D., Q. Hu, R. Behara. 2006. Economics of information security investment in the case of simultaneous attacks, *Proceedings of the Workshop on the Economics of Information Security (WEIS2006)*, University of Cambridge, UK

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

Kesan, J. P., R. P. Majuca, W. Yurcik. 2005. The economic case for cyberinsurance. *Securing Privacy in the Internet Age Symposium*, Stanford University Press

Kobayashi, B. H. 2005. An economic analysis of the private and social costs of the provision of cybersecurity and other public security goods. *Working paper*, George Mason University, School of Law

Kunreuther, H., G., Heal. 2003. Interdependent security, *Journal of Risk and Uncertainty* 26(2/3) 231-249

Lee, W., J. A. Ligon. 2001. Moral hazard in risk pooling arrangements. *Journal of Risk and Insurance* 68(1) 175-190

Leech. T. 2004. Controlling the high cost of SOX: Avoid costly mistakes. *Compliance Week* March 23, 2004

Lichtman, D., E. Posner. 2004. Holding Internet Service Providers accountable*, John M. Olin Law & Economics Working Paper No. 217*, http://ssrn.com/abstract_id=573502

Ligon, J. A., P. D. Thistle. 2005. The formation of mutual insurers in markets with adverse selection. *Journal of Business* 78(2) 529-555

Lin, L., X. Geng, A. B. Whinston. 2005. A sender-receiver framework for knowledge transfer. *MIS Quarterly* 29(2) 197-219

Loch K. D., H. H. Carr, M. E. Warkentin. 1992. Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly* 16(2) 173-186

Mailath, G. J. 1987. Incentive compatibility in signaling games with a continuum of types. *Econometrica* 55(6) 1349-1356

Marshall, J. M. 1974. Insurance theory: Reserves versus mutuality. *Economic Inquiry* 12 476-492

Mayers, D. 1988. Ownership structure across lines of property-causality insurance. *Journal of Law and Economics* 31 351-378

Mayers, D., C. W. Smith. 1981. Contractual provisions, organizational structure and conflict in insurance markets. *Journal of Business* 54 407-434

Muralidhar, K., R. Parsa, R. Sarathy. 1999. A general additive data perturbation method for database security. *Management Science* 45(10) 1399-1416

Nayyar P. R. 1990. Information Asymmetries: A Source of Competitive Advantage for Diversified Service Firms. *Strategic Management Journal* 11(7) 513-519. Nov.-Dec., 1990

Nizovtsev, D., M. Thursby. 2006. To disclosure or not? An Analysis of software user behavior. *SSRN paper.*

Ogut, H., N. Menon, S. Raghunathan. 2005. Cyber insurance and IT security investment: impact of interdependent risk," *Proceedings of the Workshop on the Economics of Information Security (WEIS2005)*, Harvard University, Cambridge, MA

Ogut, H., S. Raghunathan, N. M. Menon. 2005. Information security risk management through self-protection and insurance. *Working paper*, University of Texas at Dallas

Oversight. 2006. The 2006 Oversight Systems Financial Executive Report on Sarbanes-Oxley. Oversight Systems, 2006.

Parameswaran, M., X. Zhao, A.B. Whinston, F. Fang. 2007. Reengineering the Internet for better security *IEEE Computer* 40(1) 40-44

Paulk, M. C., B. Curtis, M. Chrissis, C.V. Weber. 1995. *The capability maturity model: guidelines for improving the software process for software*. Addison-Wesley, Reading, MA.

Pauly, M. V. 1968. The economics of moral hazard: Comment. *American Economic Review* 58(3) 531-536

Pew Internet and American Life Project. 2005. Survey report on email spam. http://www.pewinternet.org/pdfs/PIP_Spam_Ap05.pdf

Powell, B. 2005. Is cybersecurity a public good? Evidence from the financial services industry. *Independent Institute Working Paper, No. 57*

Ranger, S. 2005. Report: Sarbanes-Oxley could threaten security. *CNET*. http://news.com.com/Report+Sarbanes-Oxley+could+threaten+security/2100-7348_3-5783472.html

Rhee, M., P. R. Haunschild. 2006. The liability of good reputation: A study of product recalls in the US automobile industry. *Organization Science* 17(1) 101-117

Rowe, B. R., M. P. Gallaher. 2006 Private sector cyber security investment strategies: An empirical analysis. *Proceedings of Workshop on the Economics of Information Security (WEIS2006)* University of Cambridge, UK

Sarathy, R., K. Muralidhar. 2002. The security of confidential numerical data in databases. *Information Systems Research* 13(4) 389-403

Schneier, B. 2000. Full disclosure and the window of exposure. *CRYPTO-GRAM*

Schwartz, M. 2006. Beyond malware, sox, and data breaches: The 2006 security forecast, *IT Compliance Institute (ITCI)*, http://www.itcinstitute.com

Shavell, S. 1979. On moral hazard and insurance. *Quarterly Journal of Economics* 93 (4) 541-562

Spence, M. 1973. Job market signaling. *Quarterly Journal of Economics* 87 355-374

Straub, D. W., R. J. Welke. 1998. Coping with systems risk: Security planning models for managerial decision making. *MIS Quarterly* 22(4) 441-469

Swiss Re. 2003. The picture of ART. *Sigma* 1. Copyright Swiss Re.

Symantec. 2007. *IT Risk Management Report—Trend through December 2006*. Volume 1. Report published by Symantec, February 2007. http://www.symantec.com/riskreport/

Talbot, D. 2005. The Internet is broken, *Technology Review*, http://www.techreview.com/InfoTech/wtr_16051,258,p1.html?PM=GO

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

Telang, R., S. Wattal. 2005. Impact of software vulnerability announcements on the market value of software vendors-an Empirical investigation. *Proceedings of the Workshop on the Economics of Information Security (WEIS2005)*, Harvard University, Cambridge, MA

van Doorn, J., P. C. Verhoef. 2007. Managing customer relationships in business markets: The role of critical incidents. 2007 MSI Report. 07-000. http://www.msi.org/publications/publication.cfm?pub=1141

Varian, H. R. 2000. Managing online security risks," *New York Times* http://www.ischool.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html

Varian, H. R. 2004. System reliability and free riding. *Working Paper*, University of California, Berkeley

Ware, L. C. 2005. Phishing Sinks Confidence in E-commerce. *Computerworld*

Weigelt, K., C. Camerer. 1988. Reputation and corporate strategy: A review of recent theory and applications. *Strategic Management Journal* 9(5) 443-454

Werbel, J. D., M. S. Wortman. 2000. Strategic philanthropy: responding to negative portrayals of corporate social responsibility. *Corporate Reputation Review* 3(2) 124-136

Wilson, R. 1985. Reputations in games and markets. In Roth, A.E.(ed.), *Game-theoretic Models of Bargaining*. Cambridge University Press, Cambridge, 27-62

Zhao, X., F. Fang, A. B. Whinston. 2006. Designing online mediation services for C2C markets. *International Journal of Electronic Commerce* 10(3) 71-93

VITA

Xia Zhao was born in Pingyao, People's Republic of China on March 7th, 1977, the daughter of Jingen Zhao and Zhonglian Han. After completing her work at YuYing High School, Beijing, China, in 1995, she entered Tsinghua University in Beijing, China. She received the degree of Bachelor of Science in Automation and Master of Science in Control Theory and Control Engineering from Tsinghua University in June 1999 and 2002 respectively. In September 2002, she came to the United States to pursue a doctor degree in Information Systems at the University of Texas at Austin.

Address: 1646 W 6th Street, Apt M, Austin, TX 78703

This dissertation was typed by the author.