2009

Managing Interdependent Information Security Risks: A Study of Cyberinsurance, Managed Security Service and Risk Pooling

Xia Zhao
University of North Carolina at Greensboro, x_zhao3@uncg.edu

Ling Xue
University of Scranton, xuel2@scranton.edu

Andrew B. Whinston
University of Texas at Austin, abw@uts.cc.utexas.edu

MANAGING INTERDEPENDENT INFORMATION SECURITY RISKS: A STUDY OF CYBERINSURANCE, MANAGED SECURITY SERVICE AND RISK POOLING

Completed Research Paper

Xia Zhao
The University of North Carolina at Greensboro
Greensboro, NC 27455
X_zhao3@uncg.edu

Ling Xue
The University of Scranton
Scranton, PA 18510
Xuel2@scranton.edu

Andrew B. Whinston*
The University of Texas at Austin
Austin, TX 73712
abw@uts.cc.utexas.edu

Abstract

The interdependency of information security risks poses a significant challenge for firms to manage security. Firms may over- or under-invest in security because security investments generate network externalities. In this paper, we explore how firms can use three risk management approaches, third-party cyberinsurance, managed security service (MSS) and risk pooling arrangement (RPA), to address the issue of investment inefficiency. We show that compared with cyberinsurance, MSS is more effective in mitigating the security investment inefficiency because the MSS provider (MSSP) serving multiple firms can endogenize the externalities of security investments. However, the investment externalities may discourage a for-profit MSSP from serving all firms even on a monopoly market. We then show that firms can use RPA as a complement to cyberinsurance to address risk interdependency for all firms. However, the adoption of RPA is incentive-compatible for firms only when the security investments generate negative externalities.

Keywords: Information security, cyberinsurance, risk pooling, risk management, managed security service, economics of information systems

Introduction

Information security has become a major concern for public and private organizations. Studies indicate that security-related spending accounts for a significant portion of IT expenditure. According to the 2008 CSI Computer Crime and Security Survey (Richardson 2009), 47% respondents reported that their organizations allocated more than 5% of their IT budget to information security. In academia, information security has drawn a tremendous amount of attention. Researchers have addressed information security from technical perspectives (e.g., Garfinkel et al. 2002; Muralidhar et al. 1999; Sarathy and Muralidhar 2002), economic perspectives (e.g., Cavusoglu et al. 2004; 2005; Gal-Or and Ghose 2005; Ghose and Rajan 2006; Gordon and Loeb 2002, 2006; Kannan and Telang 2005; Parameswaran et al. 2007; Zhao et al. 2008), and organizational perspectives (e.g. Gattiker and Kelley 1999; Loch et al. 1992; Straub and Welke 1998; Tanaka et al. 2005). A central research question is how firms can allocate security expenditures in an effective and efficient way.

An issue long plaguing researchers and practitioners is the interdependency of information security risks. Over the Internet, organizations and individuals are linked either physically or logically and information security risks are intricately interrelated. The risks faced by one organization depend on not only its security strategies but also others'. In other words, an organization's security investment mitigates its security risks, as well as affects those of others. The network externalities of security investments often induce firms to invest inefficiently from a social planner's perspective (Kunreuther and Heal 2003; Ogut et al. 2005; Powell 2005). This paper examines three risk management approaches and explores solutions to this issue.

Previous literature has identified both the underinvestment and overinvestment issues caused by the interdependent nature of security risks (e.g., Kunreuther and Heal 2003; Powell, 2005). When security risks are positively interdependent and thus the organizations' security investments generate positive externalities[1], self-interested organizations invest lower than the socially optimal level (Kunreuther and Heal, 2003; Ogut, et al. 2005). For example, if a hacker breaks into one firm's network, he may steal sensitive data about its partners or penetrate into its partners' networks via the trust connections. In this case, a firm's security investment not only strengthens its protection, but also reduces the likelihood of other firms having security breaches. Examples of security practices with positive externalities include antivirus software and firewalls. Self-interested organizations tend to ignore the positive externalities and underinvest in information security protections.

When security risks are negatively interdependent and thus organizations' security investments generate negative externalities[2], self-interested organizations invest higher than the socially optimal level. Negatively interdependent security risks are often associated with targeted attacks. A *targeted attack* refers to a malware attack aimed exclusively at one organization or organizations within a small subset of the general business population. According to the 2008 CSI Computer Crime and Security Survey(Richardson 2009), 32% of respondents reported their companies experienced such attacks in the past year. In targeted attack, hackers generally target firms with less security protections. Thus, a highly protected website can divert hackers to other websites and increase others' risks[3]. Individual websites often ignore the negative impact of their investments on others' security and may invest more than the socially optimal level. The issue of overinvestment in security, although received relatively little attention, has been evidenced in some studies. For instance, a Symantec research investigated the efficiency of firms' IT risk management programs and the levels of IT risks they experience, and found that some organizations are addressing IT risks through overinvestment (Symantec 2007). In this paper, we consider both overinvestment and underinvestment caused by the interdependency of information security risks.

[1] Positive interdependency of security risks means that if a company has higher security risks, other companies have higher security risks. In this regard, when a company invests more in security protections, it not only better protects itself but also better protects other companies. Thus, the security investments generate positive externalities.

[2] Negative interdependency of security risks means that if a company reduces its own security risks, it threatens other companies' security. In this regard, when a company invests more in security protections, it reduces other companies' security levels. Thus, the security investments generate negative externalities.

[3] In a similar scenario, Ayres and Levitt (1998) find that increasing home security by one home owner increases neighbors' likelihood of being attacked.

Researchers and practitioners have long been studying how to help firms optimally allocate security resources. In this research, we examine three risk management approaches to addressing investment inefficiency caused by the interdependent security risks. We first consider third-party cyberinsurance. Cyberinsurance is a range of first-party and third-party coverage that enables firms to transfer their security risks to the commercial insurance market. Examples of cyberinsurance 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. Cyberinsurance has been proposed as a promising approach to managing information security risks and optimizing security expenditures (Gordon et al. 2003; Kesan et al. 2005; Ogut et al. 2005; Varian 2000). With cyberinsurance, firms can balance their expenditure between implementing security protections and purchasing insurance, and thus prevent firms from investing in cost-ineffective protections. However, we show that cyberinsurance cannot address the issue of investment inefficiency caused by interdependent security risks.

We next consider managed security service (MSS, or IT security outsourcing). MSS providers (MSSPs) provide a range of security services, such as security monitoring; compliance auditing; information security risk assessments; vulnerability assessment and penetration testing; managed spam services; anti-virus and content filtering services; network boundary protection; incident management, including emergency response and forensic analysis; data archiving and restoration; and on-site consulting (Allen et al. 2003; Ding and Yurcik 2006). The 2008 CSI Computer Crime and Security Survey reported that as high as 39% respondents outsourced part or all of computer security functions. In addition, 5% respondents indicated that their companies outsourced more than 60% of security functions (Richardson 2009). The global MSS market is forecasted to more than double between 2007 and 2011, when it will reach $13.8 billion (Infonetics Research 2008).

We show that compared with cyberinsurance, MSS has an advantage in addressing investment inefficiency caused by both positive and negative externalities of security investments. MSS enables firms to delegate the security decisions to the MSSP. To make the MSSP's incentive aligned with the client firms' interests, firms can use the service level agreement (SLA) to specify performance expectations, establishes accountability, and details remedies or consequences if performance or service quality standards are not met (Allen et al. 2003). Consequently, firms can transfer not only IT security investment decisions but also their security risks to MSSPs. Since a MSSP collectively manages the interdependent security risks for multiple client firms, it can internalize the externalities of security investments when making investment decisions for firms.

Although MSS can be used to endogenize the externalities, we find that the MSSP may not be willing to serve all firms, even on a monopoly MSS market. The key insight is that the security investments made by the MSSP can indirectly benefit other unenrolled firms through externalities. This makes unenrolled firms even less willing to use MSS. Therefore, if the MSSP intends to serve more firms, it has to lower the service fee charged for MSS. As a consequence, MSSP may not serve all firms and the socially optimal security investments cannot be achieved.

We then consider the solution of the risk pooling arrangement (RPA). RPA 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.[4] Mutual insurance was widely adopted in the insurance market for medical malpractice and municipal liability during the late 1980s (Ligon and Thistle 2005), and has since been used also in other lines of insurance, such as employee pension and employee health insurance. The traditional advantages of RPA over commercial insurance include reduced overhead expense and flexible policy development (Swiss Re 2003).

RPA is different from third-party cyberinsurance in terms of risk transfer. It can never completely eliminate the risks for an individual policyholder. Even though the risk pool can issue full coverage for individual firms' security losses, each individual firm has to bear part of the risk pool's loss through its equity position. This is equivalent to the case that firms share their risks with one another. Since a firm's payoff is influenced by other firms' security

[4] Group captives are special insurance companies that are set up by a group of companies to insure their 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 companies 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 companies 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 Re 2003).

losses, it will consider other firms' security levels when making its investment decision. The risk sharing capability of RPA makes it possible for firms to endogenize the externalities of security investments and resolve the investment inefficiency.

We find that the effectiveness of RPA is contingent on the nature of interdependency. Even though RPA enables firms to endogenize both positive and negative externalities of security investments, the adoption of RPA is incentive-compatible for firms only in the case of negative externalities. The key reason is that by pooling risks of individual firms, RPA induces *moral hazard*, which refers to firms' reluctance to invest in loss prevention when they can transfer security losses to others (Lee and Ligon 2001). The moral hazard is desirable when security investments generate negative externalities and firms overinvest. However, in the case of positive externalities, moral hazard further reduces the firms' investment incentives and exaggerates the underinvestment problem.

The contribution of this paper is threefold. First, by proposing the solutions of MSS and RPA, this study expands the view on addressing the investment inefficiency caused by interdependent information security risks. Previous studies on cyberrisk management primarily focused on cyberinsurance. In the context of interdependent risks, cyberinsurance however is inefficient in inducing efficient security investments. Therefore, this paper provides new insights on the use of alternative solutions in IT security risk management. In addition, we consider the implementation issue of these solutions. Some other potential solutions are difficult to implement. For example, although the imposition of liability among firms is proved to be effective in endogenizing security externalities (Ogut et al. 2005), it is difficult for organizations to trace and enforce liabilities in the Internet environment. In contrast, MSS is available in the market and RPA can be implemented by following the standard processes of mutual insurance organization. In addition, the adoption of MSS and RPA is proved to be *incentive-compatible* for individual firms.

Second, this paper contributes to the stream of research on IT security outsourcing. It has been well recognized that firms outsourcing security services can benefit from cost saving, staffing, skills, security awareness, dedicated facility, liability protection and round-the-clock service (Allen et al. 2003). This paper illustrates that the use of MSS can also be justified from the perspective of mitigating the investment inefficiency caused by risk interdependency. In this regard, even if the MSSPs do not necessarily have the cost advantages or technological advantages in managing information security, they are still favorable from the perspective of social welfare.

Finally, this paper contributes to the research on mutual insurance and alternative risk transfer (ART) vehicles. RPA, as an ART approach, has been recognized by practitioners as having the advantages of reduced overhead expense and flexible policy development (Swiss Re 2003). This paper, on the other hand, finds that RPA can be a solution to the interdependent security risks and help firms optimize their security spending. This finding generates important implications for the policy makers regarding the regulation of the insurance industry. Although the capacity limit of the commercial insurance market stimulates the demand for ART solutions, the development of RPA is still highly subject to regulatory attitudes. Therefore, it is important for policy makers to recognize the potential benefit of RPA in security management in the context of risk interdependency. Such recognition can help guide the development of appropriate policies for RPA and improve social welfare overall.

The rest of the paper is organized as follows. Section 2 reviews related literature on economics of information security, insurance, MSS and RPA. In section 3, we outline the model setup. Section 4, 5 and 6 examine the uses of cyberinsurance, MSS and RPA in managing interdependent security risks respectively. In section 7, we discuss the managerial and policy implications, and then conclude the paper with future extensions.

Related Literature

Prior research on economics of information security has studied many issues regarding information security investments. 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 determine 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 and security investment complement each other. Kunreuther and Heal (2003) characterize a class of interdependent security risks and demonstrate that firms generally underinvest in security protections when their security risks are interdependent. Our paper complements this stream of research by exploring implementable solutions to the investment inefficiency caused by independent information security risks.

There is an emerging body of literature examining the role of insurance in the area of information security. Gordon et al. (2003) and Kesan et al. (2005) discuss the advantages of using cyberinsurance to manage information security risks. Ogut et al. (2005) use an economic model to examine firms' investments in security protections and their use of cyberinsurance in the context of interdependent security risks. All of these studies focus on the third-party commercial cyberinsurance. This paper examines RPA and MSS in addition to third-party cyberinsurance.

IT security outsourcing has not received adequate research attention until recently. Allen et al. (2003), Axelrod (2004) and McQuillan and Hill (2007) summarize various issues on outsourcing IT security services and provide organizations guidance to knowledgeably engage MSSPs. Ding, et al. (2005) study the moral hazard problem in IT security outsourcing. They show that an optimal contract should depend on both the current performance and the reputation of the MSS, and the influence of performance decreases as the reputation effect becomes more significant. Ding and Yurcik (2006) study IT outsourcing decisions using a simulation approach which evaluates the cost-and-benefit tradeoff of using MSS. They find that the MSSP outsourcing decision is relatively insensitive to variation in service quality but hypersensitive to the business risk of MSSP bankruptcy. Ding and Yurcik (2005) explore the impact of transaction costs on MSSPs and find that market competition drives MSSPs to cut the price and share transaction costs with client organizations. The network externalities associated with IT security outsourcing have also been examined. Rowe (2007) suggests that government should subsidize firms for IT security outsourcing in presence of positive externalities. Gupta and Zhdanov (2007) analytically explain the growth and sustainability of MSS networks. They find that initial investment is critical in determining the size of MSS networks with positive externalities. Our paper examines using MSS to manage interdependent information security risks.

Prior literature on risk management has justified 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.,Doherty and Dionne 1993; Marshall 1974). 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 (Cummins and Weiss 1999; Mayers 1988; Mayers and Smith 1981). Moreover, mutual insurers may coexist with independent insurers as a result of 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, mutual insurance can be used to endogenize network externalities of security investments.

Model Setup

We consider n risk-averse firms. Each firm has an initial wealth A. All firms have an identical payoff function $U(.)$, where $U(.)$ satisfies that $U'(.)>0$, $U''(.)<0$ (i.e., $U(.)$ is concave). The breach probability for an individual firm, say firm i, is determined not only by its own security investment, but also by those of others. Specifically, we assume that firm i's breach probability is $\mu(x_i, X_{-i})$ where x_i denotes firm i's security investment and $X_{-i} = [x_1,...,x_{i-1},x_{i+1},...,x_n]$ denotes the security investments of firms except i. A firm loses L in a security breach. Firm i's expected payoff can be represented by

$$\mu(x_i, X_{-i})U(A - L - x_i) + (1 - \mu(x_i, X_{-i}))U(A - x_i).$$

For notational simplicity, we use μ_i to denote $\mu(x_i, X_{-i})$.

Modeling Positive Externalities of Security Investments

To model positive externalities of security investments, we follow Ogut et al. (2005) and classify security risks as direct risks and indirect risks. Direct risks refer to the probability that malicious hackers target a firm and break into its information systems directly. A firm can reduce its direct risks by investing in security protections. We use $\rho(x_i)$ to represent the probability that malicious hackers break into firm i's systems directly, where x_i is firm i's security investment. $\rho(.)$ is a decreasing convex function, $\rho'(.) < 0$ and $\rho''(.) > 0$. Moreover, $\rho(0) \le 1$. Indirect risks refer to the probability that malicious hackers break into a firm's information systems through other firms' systems. A firm's indirect risks are determined by other firms' security investments and the interdependency factor, γ. γ measures the probability that a firm has a security breach if another firm has a security breach, and $\gamma\rho(x_j)$ represents the probability that malicious hackers break into other firms' systems through firm j's systems. Therefore, firm i's breach probability can be expressed as

$$\mu_i = \rho(x_i) + (1-\rho(x_i))\gamma\rho(x_1) + (1-\rho(x_i)-(1-\rho(x_i))\gamma\rho(x_1))\gamma\rho(x_2) + ... \quad (1).$$

The first term of (1) represents firm *i*'s direct risks; the second term represents firm *i*'s indirect risks from firm 1; the third term represents firm *i*'s indirect risks from firm 2; etc. We rearrange the breach probability function as follows.

$$\mu_i = 1 - \left((1-\rho(x_i)) \prod_{j \neq i} (1-\gamma\rho(x_j)) \right), \; i = 1, 2, \ldots n .$$

In the symmetric case,

$$\mu_i = 1 - \left((1-\rho(x_i))(1-\gamma\rho(x_{-i}))^{n-1} \right), \; i = 1, 2, \ldots n .$$

where x_{-i} stands for other firms' investments. For notational simplicity, we use ρ_i to represent $\rho(x_i)$, ρ_{-i} to represent $\rho(x_{-i})$, ρ_i' to represent $\frac{\partial\rho}{\partial x}|_{x=x_i}$, and ρ_{-i}' to represent $\frac{\partial\rho}{\partial x}|_{x=x_{-i}}$. Note that $\frac{\partial\mu_i}{\partial x_i} = \rho_i'(1-\gamma\rho_{-i})^{n-1} < 0$, which means that firm *i*' breach probability is decreasing in its security investment. Also, $\frac{\partial\mu_i}{\partial x_{-i}} = (1-\rho_i)(1-\gamma\rho_{-i})^{n-2}\gamma\rho_{-i}' < 0$, which means that firm *i*' breach probability is also decreasing in other firms' security investments (i.e., the positive externalities).

Modeling Negative Externalities of Security Investments

In the case of negative externalities, a firm's security investment, while reducing its breach probability, increases the breach probabilities of other firms. For example, in the targeted attacks, hackers are more likely to choose firms with lax security protection. If a firm invests more than others, its investment is more effective in driving hackers away and lowering the likelihood of having security breaches. Security measures that are used to defend DDoS attacks, such as content caching and redundant network devices, are more likely to generate negative externalities.

We model the negative externalities of security investments by assuming firm *i*'s breach probability as $\mu_i = p\left(x_i \frac{x_i}{\bar{x}_i}\right)$ where $\bar{x}_i = \frac{\Sigma_{j\neq i} x_j}{n-1}$. $p(.)$ is a decreasing convex function, i.e., $p'(.) < 0$ and $p''(.) > 0$. Moreover, $p(0) \leq 1$. We use the term $\frac{x_i}{\bar{x}_i}$ to characterize the relative effectiveness of a firm's security investment. Note that if $\frac{x_i}{\bar{x}_i} > 1$, we have $x_i \frac{x_i}{\bar{x}_i} > x_i$. That is, if a firm's investment is higher than the average investment of other firms, its investment is more effective in reducing its security risks. Otherwise, its investment is less effective. It is easy to verify that $\frac{\partial\mu_i}{\partial x_i} = p'\left(\frac{x_i^2}{\bar{x}_i}\right)\frac{2x_i}{\bar{x}_i} < 0$ and $\frac{\partial\mu_i}{\partial x_{-i}} = p'\left(\frac{x_i^2}{\bar{x}_i}\right)\left(-\frac{\frac{1}{n-1}x_i^2}{\bar{x}_i^2}\right) > 0$. The breach probability of firm *i* is increasing in other firms' investments, i.e. the negative externalities. [5,6]

Third-Party Cyberinsurance

We assume that firms can buy insurance policy from a mature cyberinsurance market to cover their security losses. In the mature cyberinsurance market, firms are always charged an actuarially fair premium for the coverage.[7] When

[5] We also examined the case that the effectiveness of security investment is represented by the ratio of a firm's investment to the average investment of all firms including itself. That is, $\bar{x}_i = \frac{\Sigma x_j}{n}$. The results are consistent in these two cases.

[6] In this paper, we characterize the interdependent security risks among firms using a multiplicative function form. We also examined the additive function form. That is, firm *i*'s breach probability is $\mu(x_i, X_{-i}) = p\left(x_i + (x_i - \bar{x}_i)\right)$. We derived the similar results.

[7] The cyberinsurance market is mature when the competition among insurers is perfect (so that no one can exert any oligopoly power) and the actuarial data about firms' security risks are available (so that risks can be accurately assessed). In reality, the cyberinsurance market is under-developed. There are a few insurers offering cyberinsurance and each with limited capacity. In addition, actuarial data on information security, breaches and damages is scarce. In this paper, we focus on the mature insurance

firm i purchases an insurance policy with coverage I_i, the insurance premium is $P_i = \mu_i I_i$. Therefore, the insured firms extract all surplus and insurers always make zero profit. Firm i's expected payoff can be represented by

$$\Pi_i = \mu_i U\left(A - L + I_i - \mu_i I_i - x_i\right) + \left(1 - \mu_i\right) U\left(A - \mu_i I_i - x_i\right).$$

We use a multi-stage game to examine firms' investment and insurance decisions. The sequence of the game is as follows. (1) Each firm chooses its security investment x_i (i=1…n); (2) each firm purchases cyberinsurance with coverage I_i (i=1…n) from third-party insurers; (3) the security losses are realized and the insurance compensations are made. It is assumed that firms' security investments are observable.[8] Proposition 1 summarizes the equilibrium of the cyberinsurance case.

Proposition 1*: When security investments generate positive (negative) externalities, firms will purchase full insurance, i.e. I_i=L, and invest less (more) than the socially optimal level.*[9]

Proposition 1 shows that firms underinvest (overinvest) in security when the investments generate positive (negative) externalities. This is in line with the findings in the existing literature (Kunreuther and Heal 2003; Ogut et al 2005). Commercial cyberinsurance cannot internalize the externalities of security investments, and therefore is incapable to resolve either the overinvestment or underinvestment issues. Liability has been proposed to address interdependent security risks (Kunreuther and Heal 2003, Ogut, et al. 2005). However, liability is difficult to implement. Since the Internet has no clear delineation of jurisdiction, it is extremely costly, even not impossible for enforcement powers, such as governments, regulatory agencies or trade associations, to impose liability across countries.

Managed Security Service (MSS)

We next consider the impact of IT security outsourcing on interdependent security risks. In order to separate the impact of risk interdependency on firms' incentives to use MSS, we assume that the MSSP has the same level of security expertise as firms. We examine the case where firms can choose between outsourcing their security to a single MSSP and managing security in-house. If the firm manages security in-house, it can still buy cyberinsurance to cover risks. We assume that if the MSSP serves s firms in total, it charges a service fee t_s to each client firm. If a client firm suffers a security loss, the MSSP compensates the client firm for the security loss L. In other words, the MSSP assumes the accountability of security loss. The payoff of a firm enrolling in MSS (we refer to it as the *enrolled firm* thereafter), can be represented by $U\left(A - t_s\right)$. The payoff of an unenrolled firm can be represented by $U\left(A - \mu_s^I L - x_s^I\right)$, where $\mu_s^I = \mu\left(x_s^I, x_s^M, \bar{X}_s^I\right)$ represents an unenrolled firm's breach probability, x_s^I represents an unenrolled firm's security investment, x_s^M represents the MSSP's investment for each enrolled firm, and $\bar{X}_s^I$ is a 1×(n-s-1) vector representing the security investments of other unenrolled firms. The subscript s represents the number of enrolled firms. In summary, a firm's payoffs can be represented by

$$\Pi = \begin{cases} U\left(A - \mu_{s-1}^I L - x_{s-1}^I\right) & \text{if not enrolled,} \\ U\left(A - t_s\right) & \text{if enrolled.} \end{cases}$$

The MSSP's payoff is influenced by the security investments made for the enrolled firms, x_s^M, the service fee t_s that the MSSP charges, and the total number of enrolled firms s. The MSSP's optimization problem can be represented by

$$\Pi_{MSSP} = \max_{x_s^M, t_s, s} s\left[\mu_s^M\left(t_s - L - x_s^M\right) + \left(1 - \mu_s^M\right)\left(t_s - x_s^M\right)\right]$$
$$s.t.\quad U\left(A - t_s\right) \geq U\left(A - \mu_{s-1}^I L - x_{s-1}^I\right) \qquad \text{(IR)}.$$

market to illustrate the insight that MSS and RPA can outperform the traditional insurance scheme in managing the interdependent risks.

[8] The common practices of the insurance industry include evaluating applicants' protections and estimating the risks before issuing the insurance policy.

[9] To conserve space, the proofs of all propositions are not included here but are available from the authors upon request.

where $\mu_s^M = \mu\left(x_s^M, X_s^I\right)$ stands for an enrolled firm's breach probability, X_s^I is a 1×(n-s) vector representing the security investments of all unenrolled firms. The individual-rationality (IR) constraint ensures that the enrolled firms are willing to outsource MSS. Note that the right-hand side (RHS) of (IR) is an enrolled firm's payoff if it switches to managing security in-house, i.e., investing security protections and purchasing cyberinsurance. From (IR), we can conclude that the service fee satisfies that $t_s = \mu_{s-1}^I L + x_{s-1}^I$, i.e. to make a firm indifferent between using MSS and managing security in-house, the service fee of MSS should be equal to the sum of in-house security investment and cyberinsurance premium. We next examine the security investments in the cases of positive externalities and negative externalities respectively.

Positive Externalities

We first consider the case that the security investments generate positive externalities. That is, breach probabilities are $\mu_{s-1}^I = 1-\left(1-p\left(x_{s-1}^I\right)\right)\left(1-\gamma p\left(x_{s-1}^M\right)\right)^{s-1}\left(1-\gamma p\left(x_{s-1}^I\right)\right)^{n-s}$ and $\mu_s^M = 1-\left(1-p\left(x_s^M\right)\right)\left(1-\gamma p\left(x_s^M\right)\right)^{s-1}\left(1-\gamma p\left(x_s^I\right)\right)^{n-s}$.

Proposition 2*: When s firms use MSS, both the security investments at the enrolled firms and those at unenrolled firms are greater than the security investments when firms use cyberinsurance. Moreover, the security investments at the enrolled firms are greater than those at unenrolled firms. That is,* $x_s^M > x_s^I > x^I$.

Proposition 2 reveals that in the case of positive externalities, the MSS addresses the underinvestment issue in two ways. First, since the MSSP jointly optimizes the security investments for enrolled firms, it considers the externalities of security investments and chooses a higher investment than unenrolled firms. Second, by increasing the investments of the enrolled firms, the MSSP also motivates the unenrolled firms to invest more. As a result, the underinvestment issue is alleviated (These results are illustrated later in Figure 3).

We next consider how many firms the MSSP is willing to serve. From the social planner's perspective, it is optimal for the MSSP to serve all firms so that the externalities can be completely internalized. However, it may not be at the MSSP's interest to serve all firms.

Lemma 1*: Given a total number of firms, if more firms use MSS, then: (1) the security investments,* x_s^M *and* x_s^I *increase; and (2) and the service fee* t_s *decreases.*

The explanation of Lemma 1 is as follows. When one more firm enrolls in MSS, the MSSP increases its security investments for each enrolled firms since more externalities are endogenized. The increased investments at enrolled firms also motivate unenrolled firms to improve their investments. As a result, both the security level of enrolled firms and that of unenrolled firms increase, i.e. the breach probabilities are decreased. The improved overall security benefits unenrolled firms by saving them expenditure on cyberinsurance. Therefore, in order to attract more unenrolled firms to switch from using cyberinsurance to using MSS, the MSSP has to lower the service fee.

The fact that the MSS has to lower service fee to attract more firms can potentially limit the MSSP's profitability. An important implication for the MSS market is: *a MSSP may not find it optimal to serve all firms, even in a monopoly MSS market.* We next consider the optimal number of enrolled firms. Since the close-form solution is intractable in this multi-player game, we use numerical analysis to illustrate this insight. We use a breach probability function $\rho(x) = e^{-2x}$, which is consistent with the assumption that $\rho'(x) < 0$ and $\rho''(x) > 0$. The interdependency factor $\gamma = 0.9$. The firm's utility function is $U(x) = -x(x-20), x \in [0,10]$. This functional form is consistent with the assumption that $U'(x) > 0$, and $U''(x) < 0$. The initial wealth A is 8 and the loss L is 6. Figure 1 shows how the optimal number of enrolled firms changes with the total number of firms. As Figure 1 shows, the number of enrolled firms is always less than the total number of firms. The linear increase of enrolled firms in Figure 1 and the concavity of the MSSP's payoff in Figure 2 imply the service fee is decreasing. In this analysis, we consider risk interdependency as one of the reasons that firms use MSS. Even if the MSSP has the same level of security expertise, firms still outsource security services because the approach can internalize the externalities. If the MSSP has the best-in-security expertise, it may further motivate firms to pay for the services. However, when the MSSP serves more firms, the increased overall security level of the network environment will still eventually undermine firms' willingness to pay for MSS.

Figure 3 compares the security investments in the cyberinsurance, MSS and socially optimal cases. Figure 3 shows that the security investments at both enrolled firms and unenrolled firms in the MSS case are higher than those in the cyberinsurance case. In addition, the security investments at enrolled firms are higher than those at unenrolled firms. Note that the security investments at enrolled firms first decrease and then increase. This is because when the total number of firms n increases from 3 to 6, the MSSP does not find it optimal to enroll more firms (as shown in Figure 3, the number of enrolled firms stays at 2). Therefore, the increased total number of firms only exacerbates the externality issue and discourages both the MSSP and unenrolled firms from investing. When n exceeds 6, the MSSP starts to enroll more firms and internalize more externalities, and therefore, the security investments at enrolled firms start to increase.

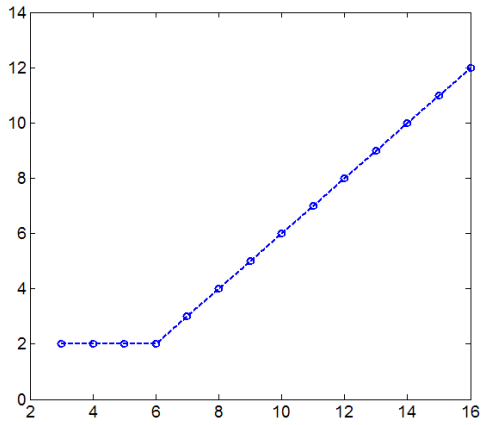

Figure 1. Optimal Number of Firms Using MSS

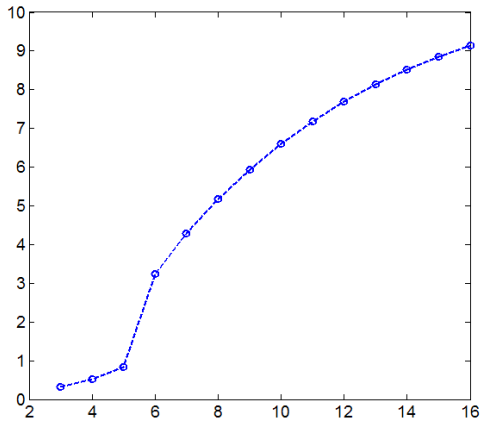

Figure 2. MSSP's Expected Payoff

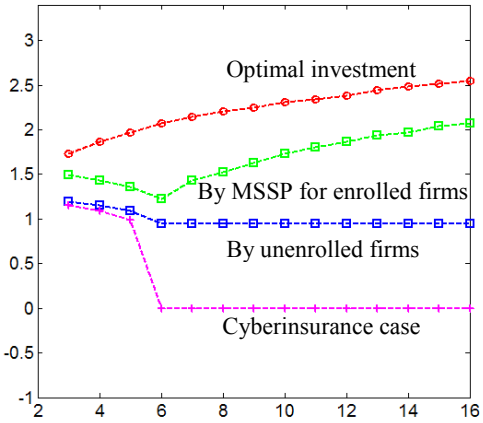

Figure 3. Security Investments

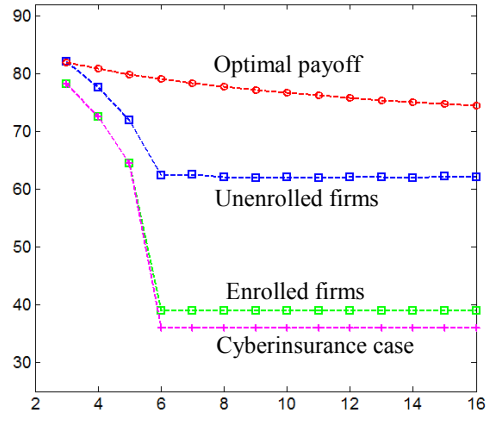

Figure 4. Firms' Expected Payoffs

The fact that the use of MSS by enrolled firms also benefits unenrolled firms leads to the following interesting result.

Proposition 3*: The unenrolled firms have higher expected payoffs than enrolled firms.*

Although the MSS addresses the underinvestment issue and improves the overall security, the benefits for the enrolled firms are appropriated by the MSSP through the service fee. In contrast, the unenrolled firms benefit from the improved security, but do not need to pay the MSSP. As a result, the unenrolled firms obtain higher payoffs than the enrolled firms. Then the question is why enrolled firms are still willing to use MSS? It is because if an enrolled firm chooses to step out, both the MSSP and the unenrolled firms will lower their investments and all firms will suffer from deteriorated security. Figure 4 compares the firms' payoffs in different cases.

Negative Externalities

We then consider the case where security investments generate negative externalities. In this case, the breach probability of an enrolled firm is $\mu_s^M = p\left(x_s^M \frac{x_s^M}{\bar{x}_s^M}\right)$ where $\bar{x}_s^M = \frac{s-1}{n-1} x_s^M + \frac{n-s}{n-1} x_s^I$, and that for an unenrolled firm is $\mu_s^I = p\left(x_s^I \frac{x_s^I}{\bar{x}_s^I}\right)$ where $\bar{x}_s^I = \frac{s}{n-1} x_s^M + \frac{n-s-1}{n-1} x_s^I$. In this case, the security investments made by the MSSP for enrolled firms are lower than the security investments made by unenrolled firms. In the numerical analysis, we assume that the breach probability function is $p(x)=e^{-x/2}$. This functional form is consistent with the assumption that $p'(x) < 0$ and $p''(x) > 0$. The analysis shows that the security investments at the enrolled firms and unenrolled firms are lower than those in the cyberinsurance case. In particular, $x_s^M < x_s^I < x^I$ (see Figure 5). As a result, the payoffs of enrolled firms and unenrolled firms in the MSS case are higher than the firms' payoffs in the cyberinsurance case (see Figure 6). Similar to the case of positive externalities, the MSSP is not willing to serve all firms. Figure 7 shows that the number of enrolled firms is smaller than the total number of firms except the total number of firms is 3. The increasing number of enrolled firms and the decreasing MSSP's payoff (see Figure 8) imply that the externalities constrain the service fee.

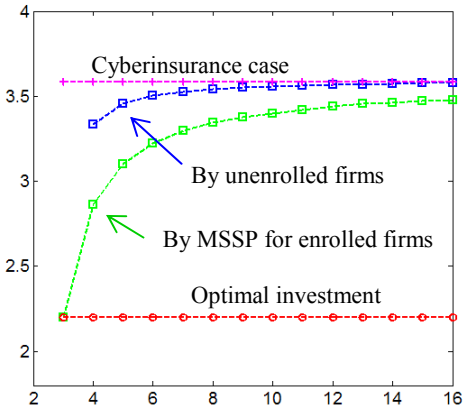

Figure 5. Security Investments

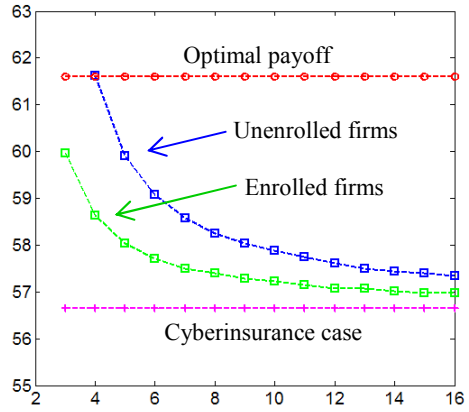

Figure 6. Firms' Payoffs

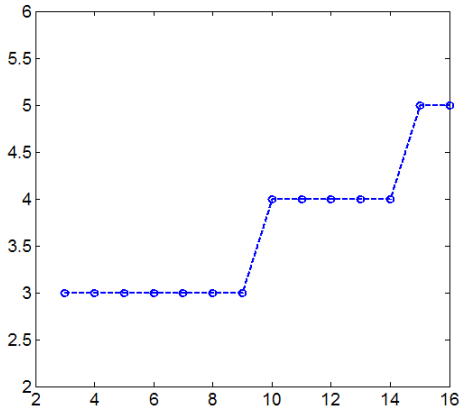

Figure 7. Optimal Number of Firms Using MSS

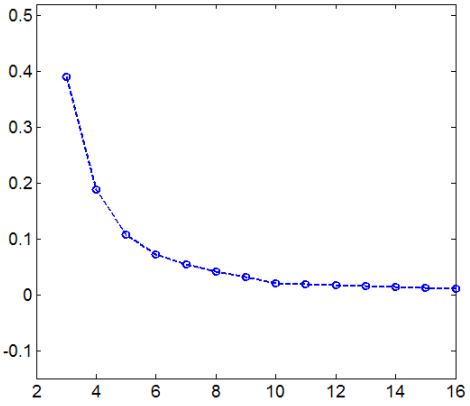

Figure 8. MSSP's Payoff

Risk Pooling Arrangement

Although MSS can be a potential solution for the interdependent information security risks, the MSSP may not be willing to serve all firms. In this regard, MSS cannot be used to eliminate the investment inefficiency for all firms. In this section, we study an alternative approach, risk pooling arrangement, which can potentially address the investment inefficiency of all firms.

We model RPA as follows. We use q to denote the ratio of loss covered by the risk pool. Assume that k out of n-1 firms (excluding firm i) have a security breach. If firm i also suffers a security breach, each of the other n-1-k firms must compensate firm i an amount of $\frac{qL}{n}$ and firm i will obtain $\frac{(n-1-k)qL}{n}$ in total. If firms i does not suffer any security breach, it must compensate each of the k suffering firms an amount of $\frac{qL}{n}$. As a result, firm i has to compensate $\frac{kqL}{n}$ in total to the k suffering firms.

Since RPA may not cover all the risks for firms, firms can purchase third-party cyberinsurance from the insurance market in addition to RPA. Again, it is assumed that the cyberinsurance market is mature. The principle of indemnity[10] requires that the cyberinsurance coverage satisfies that $I_i \le (1-q)L$, that is, the total insurance compensation (from both RPA and cyberinsurance) cannot exceed the total loss. The expected payoff of firm i can be represented by

$$\begin{aligned}\Pi_i = \underset{x_i, I_i, q}{\text{Max}}\ & \mu_i \sum_{k=0}^{n-1} b\left(k,(n-1),\zeta\right) U\left(A - L + \tfrac{(n-1-k)qL}{n} + I_i - \mu_i I_i - x_i\right) \\ & + (1-\mu_i)\sum_{k=0}^{n-1} b\left(k,(n-1),\zeta\right) U\left(A - \tfrac{kqL}{n} - \mu_i I_i - x_i\right) \\ s.t.\quad & I_i \le (1-q)L.\end{aligned}$$

where $\zeta_j = \mu\left(x_j, X_{-j}\right)$ represents the breach probability of firm j ($j \neq i$) and the subscript j is dropped in the symmetric case; and $b\left(k,(n-1),\zeta\right) = \frac{(n-1)!}{k!(n-1-k)!}\zeta^k\left(1-\zeta\right)^{n-1-k}$ denotes the binomial probability that k out of n-1 firms have security breaches.

The sequence of the game is as follows. (1) n firms cooperatively choose q; (2) given q, each firm noncooperatively chooses its security investment x_i (i=1..n); (3) each firm purchases cyberinsurance with coverage I_i (i=1..n) from third-party insurers; (4) the security losses are realized and the insurance compensations (of both third-party insurance and RPA) are made. The following Lemma characterizes the complementary relationship between RPA and cyberinsurance.

Lemma 2**:** *When firms use both RPA and third-party cyberinsurance, I_i=(1-q)L. That is, if the risk pool does not provide full coverage, firms will buy third-party insurance to cover the residual risks.*

Lemma 2 shows that risk-averse firms always choose to hedge against all risks. If the risk pool covers only part of a firm's risks (i.e. q<1), the firm will use the cyberinsurance to cover the residual risks. Thus, firm i's expected payoff can be represented by

$$\begin{aligned}\Pi_i = \underset{x_i, q}{\text{Max}}\ & \mu_i \sum_{k=0}^{n-1} b\left(k,(n-1),\zeta\right) U\left(A - \tfrac{(1+k)qL}{n} - \mu_i(1-q)L - x_i\right) \\ & + (1-\mu_i)\sum_{k=0}^{n-1} b\left(k,(n-1),\zeta\right) U\left(A - \tfrac{kqL}{n} - \mu_i(1-q)L - x_i\right).\end{aligned}$$

Section 4 (Proposition 1) shows that if a firm chooses to manage the security risks only using third-party cyberinsurance, it will purchase a full insurance policy ($I_i = L$) from a third-party insurer and completely transfer its risks to the cyberinsurance market. In contrast, if a firm adopts RPA, it still retains part of the risks since it is an

[10] The principle of indemnity is an insurance principle stating that an insured may not be compensated by the insurance company in an amount exceeding the insured's economic loss.

equity holder of RPA. Presumably, a risk-averse firm always wants to minimize its risk exposure and prefers third-party cyberinsurance to RPA. However, in the context of interdependent security risks, third-party cyberinsurance may not be superior since it cannot eliminate network externalities of security investments. The question is: with interdependent security risks, do firms have an incentive to use RPA as a complement to the cyberinsurance market? We will show next that the RPA solution is implementable in the case of negative externalities but not in the case of positive externalities.

Negative Externalities

We first consider the case that the security investments generate negative externalities. That is, the breach probability of firm *i* is $\mu_i = p\left(x_i \frac{x_i}{\bar{x}_i}\right)$ where $\bar{x}_i = \frac{\Sigma_{j\neq i} x_j}{n-1}$ and those of firms other than firm *i* are $\zeta = p\left(x_j \frac{x_j}{\bar{x}_j}\right)$ where $\bar{x}_j = \frac{\Sigma_{k\neq j} x_k}{n-1}$.

Proposition 4**:** *When security investments generate negative externalities and firms have access to a mature cyberinsurance market, firms have an incentive to adopt RPA as a complement to cyberinsurance, i.e., q>0.*

Proposition 4 generates an important implication. That is, when firms overinvest due to the negative externalities of security investments, the adoption of RPA as a complement to the third-party cyberinsurance is *incentive-compatible*. In other words, individual firms are willing to pool their security risks using RPA. To illustrate this incentive-compatibility, we derive the marginal impact of *q* on firm *i*'s expected payoff when *q*=0,

$$\frac{\partial \Pi_i}{\partial q}|_{q=0} = U'\left(A-\mu_i L-x_i\right)\mu_i L - U'\left(A-\mu_i L-x_i\right)\left(\frac{1}{n}\mu_i L + \frac{n-1}{n}\zeta L\right) - U'\left(A-\mu_i L-x_i\right)\left(\sum_{j\neq i}\frac{\partial \zeta}{\partial x_j}\frac{\partial x_j}{\partial q}\right)L. \quad (2)$$

The first term of (2) represents the marginal benefit that a firm obtains from the reduced cyberinsurance premium. In another word, when the coverage of the risk pool *q* increases, a firm will purchase a smaller cyberinsurance coverage I_i and hence pay a lower premium $\mu_i I_i$ to the commercial insurer. The second term of (2) represents the marginal loss that a firm incurs from exposing to more risks within the risk pool. In particular, $\frac{1}{n}\mu_i L$ represents the marginal loss that a firm incurs from retaining its own security damage and $\frac{n-1}{n}\zeta L$ represents the marginal loss that a firm incurs from compensating others in the risk pool. The third term of (2) represents the marginal impact of other firms' security investments on the firm's payoff. It is worth remarking that the third term of (2) is positive, which means that the firm benefits from the reduced investments of others. As the first two terms cancel out in a symmetric equilibrium, the overall marginal impact of *q* on the firm's expected payoff 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.

Next, we consider how firms allocate their risks between RPA and cyberinsurance. We first present a set of numerical results which illustrate the ratio of risks allocated to the risk pool (i.e., *q*), the equilibrium investment and the payoff of the firm when *n* increases. Then we analytically show a key result that the firm's security investments and expected payoff approach the socially optimal levels when *n* approaches infinity.

In the numerical analysis, we use the same specifications as in Section 5.2. Figure 9 illustrates the optimal ratio of loss that firms will share within the risk pool. The horizontal axis represents the number of firms and the vertical axis represents the ratio of loss that firms allocate to the risk pool. The curve shows that the proportion of loss shared in the risk pool decreases as the size of the risk pool increases. The reason is that when there are more members in a risk pool, the moral hazard becomes more severe and firms have less incentive to invest in security, which increases firms' risk exposure within the risk pool. As a result, firms choose to allocate less risk to the risk pool and buy more insurance from the cyberinsurance market.

Figure 10 compares the firm's security investments in the cyberinsurance, the RPA and the socially optimal cases. The firm's security investment drops significantly in the RPA case compared with that in the cyberinsurance case. In addition, as the number of firms increases, the security investment in the RPA case keeps decreasing and approaches the socially optimal level from above. Note that firms do not underinvest in security even though moral hazard becomes severe within the risk pool. The reason is that firms can control the extent of moral hazard by limiting the coverage of the risk pool (i.e., the value of *q*). Figure 11 compares the firm's expected payoffs in the cyberinsurance,

RPA and socially optimal cases. Note that in the RPA case, the firm's expected payoff increases and approaches the socially optimal level as n becomes larger.

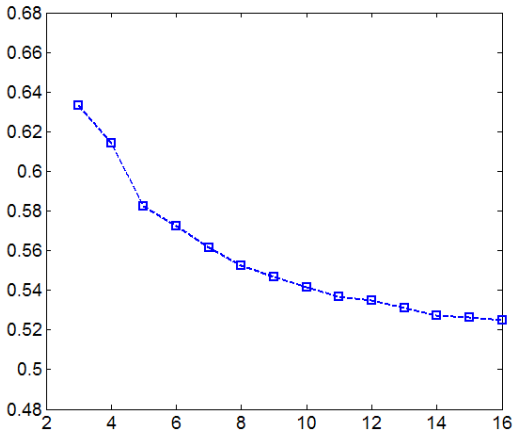

Figure 9: The Ratio of Loss Covered by the Risk Pool

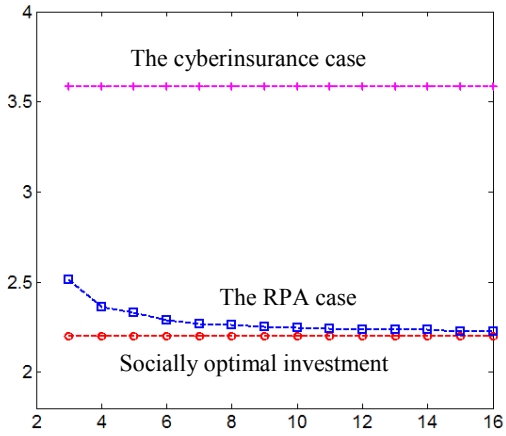

Figure 10: Firms' Security Investments

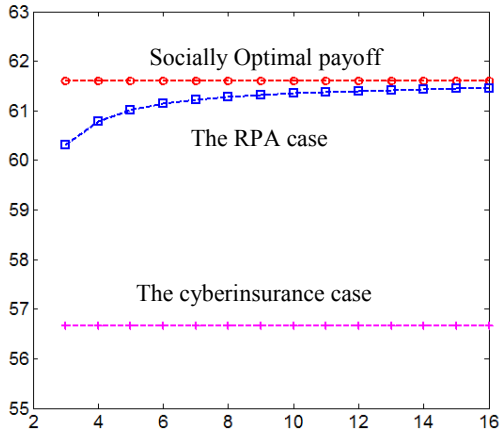

Figure 11: Firms' Expected Payoffs

Proposition 5: *When n approaches infinity, firms' security investments and expected payoffs approach the socially optimal levels*.

When n approaches infinity, in a symmetric equilibrium where $\mu_i=\mu$, the law of large numbers implies that the expected number of firms with a security breach approaches $n\mu$. Therefore, the expected loss that a firm affords in the risk pool is $\frac{n\mu qL}{n}$, and a firm's expected utility approaches

$$U\left(A-\mu qL-\mu L\left(1-q\right)-x_i\right). \tag{3}$$

where $\mu(1\text{-}q)L$ is the premium paid to commercial insurers. μqL is an total compensation that firm i pays to other firms who have security breaches. It can be understood as a "premium equivalence" paid to the risk pool. The firm's security investment can only reduce its own cyberinsurance premium $\mu(1\text{-}q)L$. It has an insignificant impact on the "premium equivalence" because the "premium equivalence" of firm i is determined by all firms' security investments. Therefore, by increasing q, the risk pool can reduce the firms' incentive to invest and thus can mitigate the overinvestment. In the extreme case where n approaches infinity, firms essentially obtain a full insurance by

paying a total premium of $\mu qL + \mu(1-q)L$. (3) can be rewritten as $U\left(A-\mu L-x_i\right)$. Therefore, firms obtain the socially optimal payoffs.

Positive Externalities

The preceding section demonstrates that when security investments generate negative externalities, firms will setup a risk pool and use it to cover a positive proportion of risks. The question here is: when security investments generate positive externalities, do firms still have an incentive to setup a RPA?

In the case of positive externalities, the breach probability functions are $\mu = 1-\left(\left(1-\rho_i\right)\left(1-\gamma\rho_{-i}\right)^{n-1}\right)$ and $\zeta = 1-\left(1-\rho_{-i}\right)\left(1-\gamma\rho_i\right)\left(1-\gamma\rho_{-i}\right)^{n-2}$ respectively. Proposition 6 shows firms have no incentive to setup a risk pool to cover a small portion of risks.

Proposition 6. *When security investments generate positive externalities, firms have no incentive to implement RPA if the risks covered in RPA are sufficiently small, i.e.* $\frac{\partial \Pi_i}{\partial q}|_{q=0} < 0$.

Then the question is whether firms have an incentive to setup a RPA with a large coverage. Since the close-form solution of q in this multi-player game is intractable, we use a numerical approach to exhaustively search for the possibility that firms are willing to adopt a RPA. We employ a series of exponential breach probability functions, increasing concave utility functions and interdependency factors in our search. However, we did not find any parameter space in which firms have an incentive to setup a risk pool.

The reason that the RPA is not effective is that the moral hazard associated with RPA undermines the benefit of RPA in endogenizing the positive externalities. By pooling security risks together, RPA generates two countervailing effects on firms' security investments. First, RPA induces firms to consider the positive impact of their security investments on others and motivates firms to increase their investments. Second, since RPA allows firms to transfer their security losses to others, firms have incentives to reduce their investments and free-ride others (the problem of moral hazard in teams, Holmstrom 1982). In the case of negative externalities, firms have excess incentives to invest. The moral hazard helps mitigate the overinvestment incentive and enhance the internalization of negative externalities. However, in the case of positive externalities, moral hazard further reduces firms' investment incentives and therefore undermines the capability of RPA in internalizing the positive externalities.

Discussion and Conclusion

The objectives of managing security risks include not only limiting firms' risk exposure, but also facilitating the appropriate allocation of security resources. The risk management approaches considered in this paper—third-party cyberinsurance, MSS and RPA—differ in their capabilities of reducing risk exposure and inducing efficient security investments. Both cyberinsurance and MSS provide complete risk transfer. Compared with cyberinsurance, MSS induces more efficient allocation of security resources since the MSSP, when serving multiple firms, internalizes the externalities of security investments among its client firms. RPA, in contrast, cannot provide complete risk transfer. However, it can still help induce more efficient security investments than cyberinsurance when security investments generate negative externalities. Risk sharing and moral hazard associated with RPA mitigate firms' overinvestment incentives.

Managerial Implications

In contrast to cyberinsurance whose merits have been widely recognized, MSS and RPA have not received adequate attention in cyberrisk management. This paper justifies the value of MSS in the context of interdependent information security risks. MSS can be a feasible approach to addressing both the negative externalities and positive externalities of security investments. Managers of firms whose information security risks are interdependent may consider using common MSSPs to manage risks. The key to the effectiveness of MSS in the context of interdependent risks is to make the MSSP accountable for security loss of its clients. It ensures that the MSSP considers the network externalities of security investments when it makes decisions for each firm. Another implication is that even if managers do not use MSS for their organizations, they may indirectly benefit from others' use of MSS. This helps managers better plan their in-house security investments.

A traditional advantage of using RPA is the flexibility for mutual insurers to develop and issue specialized insurance policies to its members. This study shows that firms can use RPA to cover the risks that are not covered by the commercial cyberinsurance. Therefore, managers need to realize the potential of using RPA as complement to, rather than substitute for, cyberinsurance. Combining cyberinsurance and RPA together can be an effective solution to interdependent security risks. Also, the fact that RPA is incentive-compatible only in the case of negative externalities implies that in using RPA, firms need to consider the nature of externalities.

Policy Implications

This paper also generates important policy implications for the social planner regarding the regulation of the markets of cyberinsurance, MSS and RPA. The competition between cyberinsurance and MSS makes it possible for firms to obtain more attractive policies to cover their risks. However, as this study reveals, such competition may discourage the MSSP from serving more firms. In this regard, the social welfare improvement may be constrained by this competition. The social planner may need to take into account this side effect when developing policies promoting these solutions.

In general, the insurance industry is highly regulated, and the development of RPA is subject to the 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 coordinate firms' security investments, it is worthwhile for the social planner to reexamine and improve existing regulatory policies on mutual insurance to encourage the development of RPA.

Future Directions

This study can be extended in many directions. First, future research may consider the situation with heterogeneous firms. For example, the impact of network externalities on firms depends on their scales or the degree of integrating with their partners. The MSSP may prefer to first enroll large firms or the firms who closely integrate with their partines. Also, the heterogeneity among firms may lead to the formation of different mutual organizations and different insurance policies. Thus, an analysis of heterogeneous firms can generate rich implications on the coexistence of miscellaneous mutual insurance organizations.

The second potential extension is to consider multiple MSSPs. The competition among MSSPs may render the MSS a more favorable solution to interdependent firms since the competition drives MSSPs to reduce the service fee and share the surplus with enrolled firms.

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

Acknowledgements

[*] Professor Andrew B. Whinston greatly acknowledges the support from NSF grant number 0831338 for the completion of this paper.

References

Allen, J, Gabbard, D., May C. 2003. "Outsourcing Managed Security Services," Carnegie Mellon Software Engineering Institute.

Anderson R., Moore, T. "The Economics of Information Security. *Science* (314), 2006, pp. 610-613.

Axelrod, C. W. "Outsourcing Information Security," Artech House. 2004.

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

Cavusoglu, H., Mishra, B., Raghunathan, S. "A Model for Evaluating IT Security Investments," *Communications of the ACM* (47:7), 2004, pp. 87-92.

Cavusoglu, H., Mishra, B., Raghunathan, S. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research* (16:1), 2005, pp. 28-46.

Cummins, J. D., Weiss, M. A. "Organizational Form and Efficiency: The Coexistence of Stock and Mutual Property-Liability Insurers," *Management Science* (45:9), 1999, pp.1254-1270.

Ding, W., Yurcik, W. "Outsourcing Internet Security: The Effect of Transaction Costs on Managed Service Providers," *The International Conference on Telecommunication Systems-Modeling and Analysis*, Dallas, Texas, November 17-20, 2005.

Ding, W., Yurcik, W. "Economics of Internet Security Outsourcing: Simulation Results Based on the Schneier Model," *The Workshop on the Economics of Securing the Information Infrastructure (WESII)*, Washington D.C., October 23-24, 2006.

Ding, W., Yurcik, W., Yin, X. "Outsourcing Internet Security: Economic Analysis of Incentives for Managed Security Service Providers," *The Workshop on Internet and Network Economics (WINE)*, Hong Kong, China, December 15-17, 2005.

Doherty, N. A., Dionne, G. "Insurance with Undiversifiable Risk: Contract Structure and Organizational Form of Insurance Firms," *Journal of Risk and Uncertainty* (6), 1993, pp.187-203.

Gal-Or, E., Ghose, A. "The Economic Incentives for Sharing Security Information," *Information Systems Research* (16:2), 2005, pp. 186-208

Garfinkel, R., Gopal, R., Goes, P. "Privacy Protection of Binary Confidential Data against Deterministic, Stochastic, and Insider Threat," *Management Science* (48:6), 2002, pp.749-764.

Gattiker, U. E., Kelley, H. "Morality and Computers: Attitudes and Differences in Moral Judgments," *Information Systems Research* (10:3), 1999, pp. 233-255.

Ghose, A., Rajan, U. "The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare," *The Fifth Workshop on Economics of Information Security (WEIS2006)*, University of Cambridge, United Kingdom, June 26-28, 2006.

Gordon, L. A., Loeb, M. P. "The Economics of Information Security Investment," *ACM Transactions on Information and Systems Security* (5:4), 2002, pp. 428-457

Gordon, L. A., Loeb, M. P. "Budgeting Process for Information Security Expenditure," *Communications of the ACM* (49:1), 2006, pp. 121-125

Gordon, L. A., Loeb, M. P., Sohail, T. "A Framework for Using Insurance for Cyber-risk Management," *Communication of ACM* (46:3), 2003, pp. 81-85

Gordon, L. A., Lucyshyn, W. "Sharing Information on Computer System Security: An Economic Analysis," *Journal of Accounting and Public Policy* (22), 2003, pp. 461-485

Gupta, A., Zhdanov, D. "Growth and Sustainability of Managed Security Services Networks: An Economic Perspective," *The Workshop of the Economics on Information Security (WEIS)*, Pittsburgh, Pennsylvania, June 7-8, 2007

Holmstrom, B. "Moral Hazard in Teams," *Bell Journal of Economics* (13:2), 1982, pp. 324-340.

Infonetics Research. Security and Encrypted VPN Services. Infornetics Report, 2008.

Kannan, K., Telang, R. "Market for Software Vulnerabilities? Think Again," *Management Science* (51:5), 2005, pp. 726-740.

Kesan, J. P., Majuca, R. P., Yurcik, W. "The Economic Case for Cyberinsurance," *Securing Privacy in the Internet Age Symposium*, Stanford University Press, 2005.

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

Lee, W., Ligon, J. A. "Moral Hazard in Risk Pooling Arrangements," *Journal of Risk and Insurance* (68:1), 2001, pp. 175-190.

Ligon, J. A., Thistle, P. D. "The Formation of Mutual Insurers in Markets with Adverse Selection," *Journal of Business* (78:2), 2005, pp. 529-555.

Loch K. D., Carr, H. H., Warkentin, M. E. "Threats to Information Systems: Today's Reality, Yesterday's Understanding, " *MIS Quarterly* (16:2), 1992, pp. 173-186 .

Marshall, J. M. "Insurance Theory: Reserves versus Mutuality," *Economic Inquiry* (12), 1974, pp. 476-492.

Mayers, D. "Ownership Structure across Lines of Property-Causality Insurance, " *Journal of Law and Economics* (31), 1988, pp. 351-378.

Mayers, D., Smith, C. W. "Contractual Provisions, Organizational Structure and Conflict in Insurance Markets," *Journal of Business* (54), 1981, pp. 407-434.McQuillan, L. H. "How to Work with a Managed Security Service Provider?" Harold F. Tipton, Micki Krause (eds.) *Information Security Management Handbook*. CRC Press. 2007, pp. 631-642.

Muralidhar, K., Parsa, R., Sarathy, R. "A General Additive Data Perturbation Method for Database Security," *Management Science* (45:10), 1999, pp. 1399-1416.

Ogut, H., Menon, N., Raghunathan, S. "Cyber Insurance and IT Security Investment: Impact of Interdependent Risk," *Working paper*, University of Texas at Dallas, 2005.

Parameswaran, M., Zhao, X., Whinston, A.B. and Fang F. "Reengineering the Internet for Better Security," *IEEE Computer*, (40:1), 2007, pp. 40-44.

Powell, B. "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry," *Independent Institute Working Paper*, No. 57, 2005.

Richardson, R. 2008 CSI Computer Crime & Security Survey, 2009.

Rowe, B. R. "Will Outsourcing IT Security Lead to a Higher Social Level of Security?" *The Workshop of the Economics on Information Security (WEIS)*, Pittsburgh, Pennsylvania. June 7-8, 2007.

Sarathy, R., Muralidhar, K. "The Security of Confidential Numerical Data in Databases," *Information Systems Research* (13:4), 2002, pp. 389-403.

Straub, D. W., Welke R. J. "Coping with Systems Risk: Security Planning Models for Managerial Decision Making," *MIS Quarterly* (22:4), 1998, pp. 441-469.

Swiss Re. "The Picture of ART, " *Sigma*, No.1 2003. Copyright Swiss Re.

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

Tanaka, H., Matsuura, K., Sudoh, O. "Vulnerability and Information Security Investment: An Empirical Analysis of E-local Government in Japan," *Journal of Accounting and Public Policy* (24), 2005, pp. 37-59.

Varian, H. R. "Managing Online Security Risks," *New York Times* 2000

Zhao, X., Fang, F. and Whinston, A.B. "An Economic Mechanism for Better Internet Security," *Decision Support Systems*, (45:4), 2008, pp. 811-821.