Journal of Management Information Systems

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/mmis20

Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements

Xia Zhao [a], Ling Xue [a] & Andrew B. Whinston [b]

[a] Bryan School of Business and Economics, University of North Carolina at Greensboro

[b] Center for Research in Electronic Commerce, University of Texas at Austin

Published online: 08 Dec 2014.

To cite this article: Xia Zhao , Ling Xue & Andrew B. Whinston (2013) Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements, Journal of Management Information Systems, 30:1, 123-152

To link to this article: http://dx.doi.org/10.2753/MIS0742-1222300104

Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements

XIA ZHAO, LING XUE, AND ANDREW B. WHINSTON

XIA ZHAO is an assistant professor of information systems at the Bryan School of Business and Economics, University of North Carolina at Greensboro. She received her Ph.D. in management science and information systems from the McCombs School of Business at the University of Texas at Austin. Her research interests include online advertising, information security, electronic commerce, and IT governance. She has published in *Journal of Management Information Systems, Production and Operations Management, Decision Support Systems, Information Systems Frontiers, IEEE Computer, International Journal of Electronic Commerce,* and many conference proceedings.

LING XUE is an assistant professor of information systems at the Bryan School of Business and Economics, University of North Carolina at Greensboro. He received his Ph.D. in management science and information systems from the McCombs School of Business at the University of Texas at Austin. His research interests are in the areas of IT governance, the business value of IT, electronic commerce, and information security. His papers have been published in *Information Systems Research, MIS Quarterly, Academy of Management Journal, Journal of Operations Management, Production and Operations Management, Journal of Management Information Systems, Decision Support Systems, International Journal of Electronic Commerce, Journal of Global Information Management,* and the proceedings of the International Conference on Information Systems.

ANDREW B. WHINSTON is the Hugh Roy Cullen Centennial Chair in Business Administration, Professor of Information Systems, Computer Science and Economics, John Newton Centennial IC2 Fellow, and Director of the Center for Research in Electronic Commerce at the University of Texas at Austin. He received his Ph.D. in management from Carnegie Mellon University. He was the editor-in-chief of *Decision Support Systems* and serves on the editorial or the advisory board of a number of journals. He has published over 400 articles in refereed journals, 27 books, and 62 book chapters. Among other career awards, he received recently the LEO Award for lifetime exceptional achievement in information systems and AIS Fellowship from the Association for Information Systems in 2005.

ABSTRACT: The interdependency of information security risks often induces firms to invest inefficiently in information technology security management. Cyberinsurance has been proposed as a promising solution to help firms optimize security spending.

Journal of Management Information Systems / Summer 2013, Vol. 30, No. 1, pp. 123–152.

ISSN 0742–1222 (print) / ISSN 1557–928X (online)
DOI: 10.2753/MIS0742-1222300104

However, cyberinsurance is ineffective in addressing the investment inefficiency caused by risk interdependency. In this paper, we examine two alternative risk management approaches: risk pooling arrangements (RPAs) and managed security services (MSSs). We show that firms can use an RPA as a complement to cyberinsurance to address the overinvestment issue caused by negative externalities of security investments; however, the adoption of an RPA is not incentive-compatible for firms when the security investments generate positive externalities. We then show that the MSS provider serving multiple firms can internalize the externalities of security investments and mitigate the security investment inefficiency. As a result of risk interdependency, collective outsourcing arises as an equilibrium only when the total number of firms is small.

KEY WORDS AND PHRASES: cyberinsurance, information security, interdependent risks, managed security services, risk management, risk pooling.

IN THE NETWORK ECONOMY, product innovation and value creation are achieved via networks of firms, operating on large scales. The scope of information technology (IT) has been expanding beyond the traditional organizational boundaries [17, 40]. As a result, information security risks have become intricately interdependent. For example, interorganizational information systems essentially physically connect firms' IT infrastructure via the Internet and expose the participating firms to network-wide security risks. An organization's network is at risk if a hacker gains access to its partner's network. Even firms without close business relationships may be logically interdependent: Strategic hackers often evaluate the security level of firms and select their targets on the basis of whose systems they can break into quickly without being detected [35]. In these examples, a firm's security risks depend not only on its own security practices but also on the security protections of others.

Firms' security risks can be either positively interdependent or negatively interdependent. The security risk is defined as the probability for a firm to have a security incident. Positive interdependency occurs when a company has higher security risks while other companies also have higher security risks. For example, a security threat that affects a firm may also influence the firm's partners via the interorganizational information systems. The hacker who breaks into the firm's network may steal sensitive data about the partners or penetrate the partners' networks via the trust connections. The security risks of the firm and its partners are thus positively interdependent. With positive interdependency, a firm's security investment not only strengthens its protection but also reduces the likelihood that other firms have security breaches. The security investments therefore generate positive externalities [19, 31].

Negative interdependency occurs when a company has higher security risks while other companies have lower security risks. A typical example of a negatively interdependent security risk is a targeted attack. A targeted attack refers to a malware attack aimed at one firm or a small set of firms. Strategic hackers often evaluate the security level of firms using various hacking techniques, such as port scans or eavesdropping, and select as their target firms whose systems can be broken into

quickly without detection [35]. They usually put more effort into attacking systems with lower security levels [5]. According to the CSI Computer Crime and Security Survey 2010/2011 [6], 22 percent of respondents reported that their companies experienced targeted attacks between July 2009 and June 2010. In this case, a firm's self-protection, while reducing its own risks, potentially diverts hackers to other firms and thus increases other firms' risks. Therefore, security investments in this case generate negative externalities [5].

Because of the network externalities of security investments, firms often invest inefficiently from the perspective of a central decision maker who maximizes the total payoffs of all stakeholders. Researchers from previous literature have identified both the underinvestment and overinvestment issues caused by the interdependency of security risks [5, 19, 31]. When the firms' security investments generate positive externalities, a firm's security investments strengthen not only its own security but also other firms' security. Often, self-interested firms invest at a level lower than the optimal level, which maximizes the total profit of all firms [19, 31]. Examples of security investments that generate positive externalities include antivirus software and firewalls. The installation of antivirus software helps prevent viruses from widely propagating, and therefore benefits others. However, underinvestment in antivirus protection is prevalent. A study by McAfee reported that 17 percent of computers around the world had no antivirus protection installed or that the antivirus subscriptions had expired. Furthermore, the United States outpaced the average, with 19 percent of computers unprotected, according to the data [37]. When the firms' security investments generate negative externalities, self-interested firms invest at a level that is higher than the optimal level for all firms. Security measures that are used to defend against distributed denial of service (DDoS) attacks, such as content caching and redundant network devices, are more likely to generate negative externalities. Many e-commerce Web sites, for example, prepare for 10 times the amount of peak traffic when designing their networks to defend the DDoS attacks. Such cost of risk mitigation is fairly high given that the possibility of DDoS attack is usually very low [29, 41].

This paper examines risk management solutions to the investment inefficiency caused by interdependent information security risks. Cyberinsurance has been proposed as a promising approach to managing information security risks and optimizing security expenditures [12, 31, 42]. Cyberinsurance is a range of first-party and third-party coverage that enables firms to transfer their security risks to the commercial insurance market. With cyberinsurance, firms can balance their expenditures between investing in security protections and acquiring insurance. However, cyberinsurance is ineffective in addressing the issue of investment inefficiency caused by interdependent security risks [31]. It does not internalize the externalities of security investments and cannot mitigate firms' incentives to underinvest or overinvest. In addition, the cyberinsurance market is still underdeveloped. Only a few insurers offer cyberinsurance, and actuarial data on information security, breaches, and damages is scarce. The ever-changing nature of security threats also impedes the development of the third-party cyberinsurance market. The deficiency of cyberinsurance calls for new risk management solutions to address issues related to information security risks.

Table 1. Comparison Between Cyberinsurance and RPAs

	Cyberinsurance	RPA
Owner	Third-party insurers	Policyholders
Risk transfer	Policyholders can completely transfer risks to insurers	Policyholders always retain some risks
Examples	AIG's NetAdvantage, Lloyd's eComprehensive, Chubb's CyberSecurity, Hiscox's Hacker	Captives, risk retention groups, self-insurance groups

We consider two potential risk management solutions: risk pooling arrangements (RPAs) and managed security services (MSSs). We study whether and how these solutions can be used to address the investment inefficiency and whether the self-interested firms have incentives to adopt these solutions. An RPA is a mutual form of insurance organization in which the policyholders are also the owners. Mutual insurance was widely adopted in the insurance market for medical malpractice and municipal liability during the late 1980s [22] and has since also been used in other lines of insurance, such as employee pension and employee health insurance. The traditional advantages of an RPA over commercial insurance include tax benefits, reduced overhead expenses, and flexible policy development [32].

RPAs are different from third-party cyberinsurance in terms of risk transfer. RPAs can never completely eliminate the risks for an individual policyholder. Even though the risk pool can issue full coverage for the firms' security losses, each individual firm still bears part of the risk pool's loss through its equity position. Table 1 compares cyberinsurance and RPAs.

We find that even though an RPA endogenizes the network externalities of security investments for firms, the adoption of the RPA is incentive-compatible for firms only when security investments generate negative externalities. The key reason is that by pooling the risks of individual firms, the RPA induces *moral hazard in teams,* which refers to firms' reluctance to invest in loss prevention when they can transfer security losses to others [15]. This type of moral hazard is shown to be desirable when security investments generate negative externalities. However, in the case of positive externalities, moral hazard further reduces the firms' investment incentives and exacerbates the underinvestment problem.

The second solution is MSSs, or IT security outsourcing. MSS providers (MSSPs) provide a range of security services, such as security monitoring and vulnerability assessments, network protection and penetration testing, managed spam services, antivirus and content filtering services, incident management and forensic analysis, data archiving and restoration, and on-site audits and consulting [1, 3]. The CSI Computer Crime and Security Survey 2010/2011 reported that as many as 36 percent of respondents outsourced part or all of their computer security functions to MSSPs. In addition, 14.1 percent of respondents indicated that their companies outsourced more than 20 percent of their security functions [6]. The global MSS market is fore-

casted to more than double between 2011 and 2015, when it is expected to reach $16.8 billion [24].

We show that MSSs can address investment inefficiency caused by both positive and negative externalities of security investments when the total number of firms is small. Using MSSs with a service level agreement (SLA), firms not only delegate the security operations but also transfer their security risks to MSSPs. Because the MSSP collectively manages the interdependent security risks for multiple client firms, it can internalize the externalities of security investments. However, collective outsourcing may not always arise as an equilibrium because of the interdependent nature of security risks. When the total number of firms is large, an individual firm can leverage the MSSP's collective operations for others and receive a higher payoff by managing security in-house. Even if the MSSP is better able to manage security (i.e., is more cost-efficient in managing security) than the firms, this result still holds. This paper characterizes the condition under which all firms will adopt the MSS solution.

This paper contributes to the research on alternative risk transfer (ART) solutions. RPAs, as an ART approach, have been recognized by practitioners as having the advantages of reduced overhead expense and flexible policy development [32]. We find that, in addition to these advantages, RPAs can serve as a potential solution to investment inefficiency caused by interdependent security risks and can optimize firms' security spending. This finding helps policymakers recognize the potential benefit of RPAs in security management and guide the development of policies for the mutual insurance industry. This paper also contributes to the literature on IT security outsourcing. It has been well recognized that firms outsourcing security services can benefit from cost savings, reduced staffing needs, broader skills acquisition, security awareness, dedicated facilities, liability protection, and around-the-clock service [1]. We illustrate that the use of MSSs can also be justified from the perspective of mitigating the investment inefficiency caused by risk interdependency.

The rest of the paper is organized as follows. In the next section, we review related literature on the economics of information security, cyberinsurance, RPAs, and MSSs. We then outline the model setup, followed by the analysis of the cyberinsurance, RPAs, and MSSs solutions. We also extend the model to account for heterogeneous firms. Finally, we draw managerial and policy implications and conclude this paper with future extensions.

Related Literature

RESEARCHERS IN PRIOR STUDIES ON THE ECONOMICS OF INFORMATION SECURITY have examined many issues related to information security investments (e.g., [14, 16, 18]). Anderson and Moore [2] discussed how moral hazard and adverse selection distort firms' incentives to invest in information security. Gordon and Loeb [10] developed an economic model to determine the optimal level of investment in information security. Gal-Or and Ghose [9] examined firms' incentives to share security information and showed that information sharing and security investment complement each other. Kunreuther and Heal [19] characterized a class of interdependent security risks and demonstrated

that firms generally underinvest in security protections when their security risks are interdependent. Our paper complements this stream of research by exploring risk management solutions to the investment inefficiency associated with interdependent information security risks.

There is an emerging body of literature that has examined the use of insurance in information security management. Gordon et al. [12] discussed the advantages of using cyberinsurance to manage information security risks. Ogut et al. [31] used an economic model to examine firms' investments in security protections and the use of cyberinsurance in the context of interdependent security risks. They showed that interdependence of security risks reduces firms' incentives to invest in security technologies and to buy insurance coverage. All these studies focused on third-party commercial cyberinsurance, whereas in this paper, we propose and examine two alternative risk management approaches to information security risks: RPAs and MSSs.

Prior literature on risk management has justified the existence of RPAs from various 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 [8, 25]. The mutual form of insurance can also address the conflicts of interest between insurers and policyholders because policyholders themselves are the owners of a mutual insurer [7, 26, 27]. Moreover, mutual insurers can coexist with independent insurers as a result of the adverse selection of risk-averse policyholders [22]. This paper complements these studies by illustrating the use of mutual insurance to endogenize network externalities of security investments.

Our work is also related to prior work on contracting in IT outsourcing, especially IT security outsourcing. Richmond et al. [34] analytically characterized the conditions under which an organization outsources its software enhancements, considering information asymmetry and different profit-sharing rules. Whang [45] proposed a contract for outsourcing software development that achieves the outcome of in-house development. Wang et al. [44] characterized the efficiency loss resulting from investment externalities for both in-house software development and outsourced custom software development. Sen et al. [38] proposed a dynamic, priority-based, price-penalty scheme for outsourcing IT services and found that it is more effective than a fixed-price approach. IT security outsourcing has not received adequate research attention until recently. Allen et al. [1], Axelrod [3], and McQuillan [28] provided organizations with general guidance to help them knowledgeably engage MSSPs. Gupta and Zhdanov [13] analytically explained the growth and sustainability of MSSP networks and found that the initial investment is critical in determining the size of MSS networks with positive externalities. In their setting, the issue of free-riding never occurred. Our paper examines the use of MSSs to address interdependent information security risks that often lead to free-riding. Hui et al. [16] examined both an MSSP and its clients' equilibrium effort decisions when risk interdependency arose among the MSSP's clients. In our paper, firms' security risks are interdependent even though firms do not use an MSSP. Lee et al. [20] proposed a multilateral contract to solve the double moral hazard issues between the client firm and the MSSP. Our paper complements this stream of research by examining the use of IT security outsourcing to address the investment inefficiency caused by interdependent information security risks among firms.

Model

We consider n risk-averse firms. Each firm has an initial wealth A. All firms have an identical payoff function $U(.)$, where $U(.)$ satisfies the conditions that $U(.) > 0$ and $U(.) < 0$ (i.e., $U(.)$ is concave). The assumption of an increasing and concave utility function is consistent with the literature on risk management (e.g., [21, 23, 36, 39]). Firms invest in security protection to safeguard their information assets. As we discussed in the Introduction, security investments often generate network externalities. The breach probability for an individual firm, firm i, is affected not only by its own security investment but also by the security investments of others. We let $\mu(x_i, X_{-i})$ be firm i's breach probability, where x_i represents firm i's security investment, and where $X_{-i} = [x_1, ..., x_{i-1}, x_{i+1}, ..., x_n]$ represents the other $n-1$ firms' security investments. A firm loses L in a security breach. Firm i's expected payoff can be represented by

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

It is assumed that the investment cost is linear in the investment level. In particular, the investment cost is equal to the investment level. The qualitative insights still hold if the investment cost is an increasing and convex function of the investment level. A firm's security investment decreases its breach probability, and the investment exhibits a diminishing marginal return in reducing the breach probability. That is,

$$\mu_i'(x_i, X_{-i}) = \frac{\partial \mu(x_i, X_{-i})}{\partial x_i} < 0$$

and

$$\mu_i''(x_i, X_{-i}) = \frac{\partial^2 \mu(x_i, X_{-i})}{\partial x_i^2} > 0.$$

The assumption about the declining marginal return of the security investment is consistent with the CERT (Computer Emergency Response Team) incident data [30] and is widely used in the literature on security management (e.g., [4, 10, 11]).

We consider two types of network externalities: *positive externalities* and *negative externalities.* In the case of positive externalities, a firm's security investment, while decreasing its breach probability, also *decreases* the breach probability of other firms (i.e., $\zeta_i'(x_j, X_{-j}) = (\partial \mu(x_j, X_{-j})/x_i) < 0, i \neq j$). In the case of negative externalities, a firm's security investment *increases* the breach probability of other firms (i.e., $\zeta_i'(x_j, X_{-j}) = (\partial \mu(x_j, X_{-j})/x_i) > 0, i \neq j$). Table 2 summarizes and compares the features of different network externalities.

Although firms' security risks are interdependent, a firm's security investment generally has a greater effect on its own security than on other firms' security. We therefore assume that

$$|\mu_i'(x_i, X_{-i})| > |\zeta_i'(x_j, X_{-j})|, \quad j \neq i. \tag{1}$$

In addition, we assume that

$$\sum_{j=1...n} \mu_{ij}''(x_j, X_{-j}) > 0. \tag{2}$$

Table 2. Characteristics of Network Externalities

Derivatives of breach probability	$\mu_i'(x_i, X_{-i})$	$\mu_{ii}''(x_i, X_{-i})$	$\zeta_i'(x_j, X_{-j})$
No externalities	< 0	> 0	= 0
Positive externalities	< 0	> 0	< 0
Negative externalities	< 0	> 0	> 0

Condition (2) requires that the second-order effect of a firm's security investment on its breach probability dominates the aggregate second-order effect of other firms' investments on its breach probability. These conditions reflect the reality that, even though security risks are interdependent in cyberspace, a firm's security investment is still an effective strategy for self-protection.

Third-Party Cyberinsurance

We establish the benchmark case in which firms use cyberinsurance to cover their security risks. We assume that firms can buy an insurance policy from the cyberinsurance market to cover their security losses. In practice, before issuing insurance policies, insurance companies often formally audit the client firms to ensure that firms take proper actions to protect themselves. Therefore, we assume that the security investment is observable to the insurers. The same assumption has been used in the literature [31].

The timing of events 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; and (3) the security losses are realized and the insurance compensations are made.

In this paper, we consider a mature insurance market in which firms are charged an actuarially fair premium. When firm i purchases an insurance policy with coverage I_i, the insurance premium is $P_i = \mu(x_i, X_{-i})I_i$. Firm i's optimization problem can be represented by

$$\begin{aligned}\pi_i = \max_{I_i, x_i} & \mu\left(x_i, X_{-i}\right) U\left(A - L + I_i - \mu\left(x_i, X_{-i}\right) I_i - x_i\right) \\ & + \left(1 - \mu\left(x_i, X_{-i}\right)\right) U\left(A - \mu\left(x_i, X_{-i}\right) I_i - x_i\right).\end{aligned} \tag{3}$$

According to the first-order condition with respect to (w.r.t.) I_i, we get $I_i^e = L$, where the superscript e denotes the cyberinsurance-only case. Equation (3) can be simplified as

$$\pi_i = \max_{x_i} U\left(A - \mu\left(x_i, X_{-i}\right) L - x_i\right). \tag{4}$$

In the symmetric case, we have $\mu_i'(x_i^e, X_{-i}^e) = -1/L$, where x_i^e represents firm i's equilibrium security investment and $X_{-i}^e = [x_1^e, ..., x_{i-1}^e, x_{i+1}^e, ..., x_n^e]$.

To evaluate the investment efficiency, we compare the firms' investment levels in the cyberinsurance-only case with the optimal investment level. The optimal investment level is defined as the security investment level when all the firms jointly maximize their total payoffs. It is equivalent to the case in which a central decision maker maximizes the joint payoff and determines the investment levels for all firms. We next examine the central decision maker's problem:

$$\begin{aligned}\Pi_s = \max_{I_i, x_i} \sum_{i=1}^{n} \Big(&\mu\left(x_i, X_{-i}\right) U\left(A - L + I_i - \mu\left(x_i, X_{-i}\right) I_i - x_i\right) \\ &+ \left(1 - \mu\left(x_i, X_{-i}\right)\right) U\left(A - \mu\left(x_i, X_{-i}\right) I_i - x_i\right)\Big).\end{aligned} \tag{5}$$

Again, according to the first-order condition w.r.t. I_i, we get $I_i^o = L$, $i = 1...n$, where the superscript o denotes the centralized case. Equation (5) can be simplified as

$$\Pi_s = \max_{I_i, x_i} \sum_{i=1}^{n} U\left(A - \mu\left(x_i, X_{-i}\right) L - x_i\right). \tag{6}$$

The first-order condition of Equation (6) w.r.t. x_i is

$$\begin{aligned}&U'\left(A - \mu\left(x_i, X_{-i}\right) L - x_i\right)\left(-\mu_i'\left(x_i, X_{-i}\right) L - 1\right) \\ &+ \sum_{j=1, j\neq i}^{n} U'\left(A - \mu\left(x_j, X_{-j}\right) L - x_j\right)\left(-\zeta_i'\left(x_j, X_{-j}\right) L\right) = 0.\end{aligned}$$

In the symmetric case, we have $\mu_i'(x_i^o, X_{-i}^o) + (n-1)\zeta_i'(x_j^o, X_{-j}^o) = -1/L$, where x_i^o represents the optimal level of security investment for firm i in the centralized case and $X_{-i}^o = [x_1^o, ..., x_{i-1}^o, x_{i+1}^o, ..., x_n^o]$.

In the case of negative externalities, because $\mu_{ii}''(x_i, X_{-i}) > 0$ and $\zeta_i'(x_j, X_{-j}) > 0$, we get $x_i^e > x_i^o$. In the case of positive externalities, because $\mu_{ii}''(x_i, X_{-i}) > 0$ and $\zeta_i'(x_j, X_{-j}) < 0$, we get $x_i^e < x_i^o$. Therefore, the firms overinvest when the security investments generate negative externalities and underinvest when the security investments generate positive externalities.

In the cyberinsurance-only case, we find that when security investments generate negative (positive) externalities, firms purchase full insurance (i.e., $I_i^e = L$) and invest more (less) than the optimal level. These results are in line with the findings in the existing literature [19, 31]. Even though commercial cyberinsurance can hedge firms' risks, it cannot internalize the externalities of security investments and therefore is incapable of resolving either the overinvestment or underinvestment issues. A fine for liability has been proposed to address the investment inefficiency issues caused by the interdependent security risks [19, 31]. This mechanism requires the liable firm to compensate the loss that it causes to other firms. As a result, a self-interested firm will consider the impact of its investment on other firms' security [19, 31]. However, a fine for liability between firms is difficult to enforce. Because the Internet has no clear delineation of jurisdiction, the imposition of liability across countries by enforcement powers (e.g., governments, regulatory agencies, or trade associations) is extremely costly, if not impossible. We next examine other risk management approaches—RPAs or MSSs—that can be used to address the investment inefficiency caused by risk interdependency.

Risk Pooling Arrangements

In this section, we examine the use of RPAs in addressing interdependent risks. We use $q \in [0,1]$ to denote the ratio of loss covered by the risk pool. When a firm suffers a security loss of L, the mutual insurer compensates the firm qL. Because the firms are the equity holders of the mutual insurer, the total security losses collected by the mutual insurer are then shared equally among all the firms. If $q < 1$, the firms transfer only partial losses to the mutual insurer. If $q = 1$, the RPA provides full coverage to the firms, but each firm still retains part of the risk because of its equity position.

The timing of events is as follows: (1) n firms cooperatively choose q; (2) given q, each firm 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; and (4) the security losses are realized, and the compensation stemming from both cyberinsurance and the RPA is received.

The compensation from an RPA is modeled as follows [21]. Assume that k firms out of $n - 1$ firms (excluding firm i) suffer a security loss L. If firm i also suffers a loss L, each of the other $n - 1 - k$ firms shares qL/n for firm i. Consequently, firm i bears only a loss of $L - ((n - 1 - k)qL)/n$ in total. If firm i does not suffer any loss, it shares qL/n for each of the k firms that suffer a loss. As a result, firm i has to compensate kqL/n in total to the k firms.

When the RPA does not cover all the risks, firms can purchase third-party cyberinsurance in addition to using an RPA. The principle of indemnity[1] requires that the cyberinsurance coverage satisfies the constraint that $I_i + qL \le L$; that is, the total insurance compensation from both the RPA and the cyberinsurance cannot exceed the total loss. In the symmetric case, firm i's expected payoff can be represented by

$$\pi_i = \max_{q, x_i, I_i} \mu(x_i, X_{-i}) \sum_{k=0}^{n-1} b(k, n-1, \zeta) U\left(A - L + \frac{(n-1-k)qL}{n} + I_i - \mu(x_i, X_{-i}) I_i - x_i \right)$$
$$+ (1 - \mu(x_i, X_{-i})) \sum_{k=0}^{n-1} b(k, n-1, \zeta) U\left(A - \frac{kqL}{n} - \mu(x_i, X_{-i}) I_i - x_i \right),$$
$$\text{s.t. } I_i \le (1-q)L,$$

where $\zeta = \zeta_k = \mu(x_k, X_{-k})$ represents the breach probability for firm k ($k \neq i$). We drop the subscript k in the symmetric case. The function

$$b(k, n-1, \zeta) = \frac{(n-1)!}{k!(n-1-k)!} \zeta^k (1-\zeta)^{n-1-k}$$

denotes the binomial probability that k out of $n - 1$ firms have security breaches. Proposition 1 characterizes the complementary relationship between the RPA and the cyberinsurance:

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

Proposition 1 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

$$\pi_i = \max_{q,x_i} \mu(x_i, X_{-i}) \sum_{k=0}^{n-1} b(k, n-1, \zeta) U\left(A - L + \frac{(1+k)qL}{n} - \mu(x_i, X_{-i})(1-q)L - x_i \right) + \left(1 - \mu(x_i, X_{-i})\right) \sum_{k=0}^{n-1} b(k, n-1, \zeta) U\left(A - \frac{kqL}{n} - \mu(x_i, X_{-i})(1-q)L - x_i \right). \quad (7)$$

When a firm uses only cyberinsurance, it purchases full coverage ($I_i = L$) and completely transfers its risks to the cyberinsurance market. However, if firms adopt an RPA, they still retain part of the risks because they are equity holders of the risk pool (i.e., the mutual insurance entity). Presumably, a risk-averse firm always wants to minimize its risk exposure and prefers the third-party cyberinsurance to the RPA. However, in the context of interdependent security risks, cyberinsurance may not be superior because it cannot address network externalities of security investments. The question is whether, given interdependent security risks, firms have an incentive to use RPAs as a complement to cyberinsurance. We show next that the RPA solution is incentive-compatible for firms in the case of negative externalities but not in the case of positive externalities.

Negative Externalities

We first examine how the use of an RPA in addition to cyberinsurance influences firms' security investments and payoffs when negative externalities exist:

> *Proposition 2: When security investments generate negative externalities, firms invest less in security in the case with both an RPA and cyberinsurance than in the case with cyberinsurance only.*

The underlying insights of Proposition 2 are as follows. When $q = 0$, a firm uses cyberinsurance only and purchases full insurance. Considering the marginal effect of q on a firm's investment at $q = 0$, we have $(\partial x_i/\partial q)|_{q=0} < 0$. In other words, an individual firm invests less in security protections if all the firms collectively set up a risk pool and allocate a very small proportion of risk to the pool. The use of an RPA influences a firm's investment incentives through two effects. The first is the internalization effect. Firms essentially share their security losses with one another via the RPA. Because an individual firm bears other firms' losses, it takes into consideration the negative effect of its security investments on others and thus invests less. The second is the moral hazard effect. The RPA allows a firm to transfer its security loss to others, which also dampens the firm's investment incentives (i.e., a firm would like to free ride on other firms because of moral hazard in teams [15]). In the case of negative externalities, firms have excess incentives to invest in security. The moral hazard effect helps mitigate the overinvestment incentive and hence *strengthens* the internalization effect. Therefore, firms invest less in security protections when they participate in an RPA.

> *Proposition 3: When security investments generate negative externalities, participating in an RPA (i.e., $q > 0$) is incentive-compatible for individual firms.*

Proposition 3 generates an important implication: When firms overinvest because of the negative externalities of their security investments, they have the incentives to adopt an RPA as a complement to the third-party cyberinsurance. In other words, individual firms are willing to pool their security risks using an RPA in addition to purchasing cyberinsurance. To better explain this incentive compatibility, we derive the marginal effect of q on firm i's expected payoff when $q = 0$:

$$\begin{aligned}\frac{\partial \pi_i}{\partial q}\Big|_{q=0} &= U'\left(A-\mu\left(x_i,X_{-i}\right)L-x_i\right)\mu\left(x_i,X_{-i}\right)L \\ &- U'\left(A-\mu\left(x_i,X_{-i}\right)L-x_i\right)\left(\frac{1}{n}\mu\left(x_i,X_{-i}\right)L+\frac{n-1}{n}\zeta L\right) \\ &- U'\left(A-\mu\left(x_i,X_{-i}\right)L-x_i\right)\left(\sum_{j=1,j\neq i}^{n}\frac{\partial \mu\left(x_i,X_{-i}\right)}{\partial x_j}\frac{\partial x_j}{\partial q}\right)L.\end{aligned} \tag{8}$$

The first term of Equation (8) represents the marginal benefit that a firm receives from the reduced cyberinsurance premium. When the coverage of the risk pool, q, increases, a firm can purchase less cyberinsurance coverage I_i and thus pay a lower premium $\mu_i I_i$ to the commercial insurer. The second term of Equation (8) represents the marginal loss that a firm incurs from being exposed to the risks within the risk pool. In particular, $(1/n)\mu(x_i, X_{-i})L$ represents the marginal loss that a firm incurs from retaining its own security damage and $((n-1)/n)\zeta L$ represents the marginal loss that a firm incurs from compensating others in the risk pool. The third term of Equation (8) represents the marginal effect of other firms' security investments on the firm's payoff. The first two terms cancel out in a symmetric equilibrium. Because $U'(A-\mu(x_i,X_{-i})L-x_i)>0$, $\partial\mu(x_i,X_{-i})/\partial x_j=\zeta_i'(x_i,X_{-i})>0$, and $\partial x_j/\partial q<0$, the third term (including the negative sign) is positive, which means that the firm benefits from the reduced investments of others. The overall marginal effect of q on the firm's expected payoff is positive (i.e., $(\partial\pi_i/\partial q)|_{q=0}>0$); thus, firms always have an incentive to set up a risk pool when the security investments generate negative externalities. Note that the findings in Propositions 1 to 3 do not depend on the functional forms of the utility function $U(.)$ and breach probability function $\mu(.)$, as long as $U(.)$ and $\mu(.)$ satisfy the conditions specified in the section of model setup.

Because the analytical solutions of the n-firm game with an RPA are intractable, we use numerical examples to illustrate the equilibrium pool coverage, the equilibrium investment, and the firms' payoffs given n. In the numerical examples, we assume that the security investments are additive [24]. In particular, $\mu(x_i,X_{-i})=\exp(-2(x_i+b\Sigma_{k=1\ldots n,k\neq i}x_k))$. This breach probability function ensures that $\mu_i'(x_i,X_{-i})<0$ and $\mu_{ii}''(x_i,X_{-i})>0$. The degree of network externalities is captured by b, with $b<0$ for the case of negative externalities, $b>0$ for the case of positive externalities, and $b=0$ for no externalities. This function form of breach probability nicely captures the interdependent nature of security investments. For the case of negative externalities, we let $b=-(1/15)$. This value ensures that $\zeta_i'(x_j,X_{-j})>0$, $\mu_{ij}''(x_j,X_{-j})<0$, $|\mu_i'(x_i,X_{-i})|>|\zeta_i'(x_j,X_{-j})|$, $(j\neq i)$, and $\Sigma_{j=1\ldots n}\mu_{ij}(x_j,X_{-j})>0$ when the total number of firms is less than 15. In the numerical example, we let $A=8$, $L=6$, and $U(w)=-w(w-20)$ for illustration.[3]

Figure 1a compares an individual firm's security investments in the cyberinsurance-only case, the RPA case, and the optimal case when security investments generate negative externalities. When the number of firms increases, the security investment of an individual firm becomes less effective because of the higher negative aggregate effect of other firms' security investments. A higher level of security investment is desirable to cancel out this aggregate effect. Therefore, the security investments in the optimal case and the cyberinsurance case are increasing in n. The higher negative effect with larger n also leads to a wider gap between the optimal investment and the investment in the cyberinsurance-only case. Specifically, as the number of firms increases, each individual firm's security investment in the cyberinsurance-only case further deviates from the optimal level. RPAs can effectively mitigate firms' overinvestment incentives. An individual firm's security investment is significantly lower in the RPA case than in the cyberinsurance-only case. Relative to the investment in the cyberinsurance-only case, the investment in the RPA case comes closer to the optimal level. Figure 1b compares the firm's expected payoffs in the cyberinsurance-only case, the RPA case, and the optimal case. The curves show that relative to the cyberinsurance-only case, the firm's expected payoff in the RPA case is much closer to the optimal payoff.

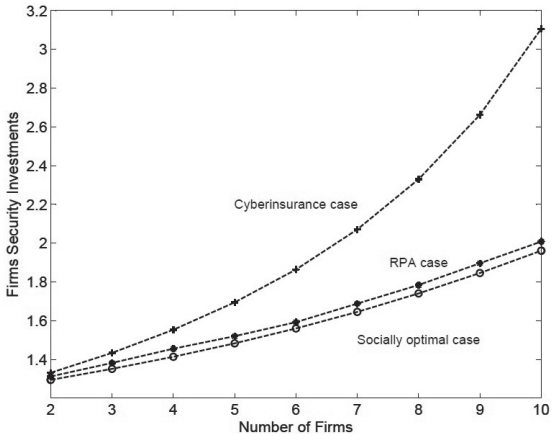
Figure 1c illustrates the optimal ratio of loss that firms allocate to the risk pool. The proportion of the loss allocated to the risk pool increases as the number of firms in the pool increases. When the number of firms increases, firms have more incentives to overinvest because of the higher negative aggregate effect of security investments by other firms. Firms allocate more risks to the risk pool to better leverage the internalization and moral hazard effects and to mitigate overinvestment. Figure 1 thus illustrates that an RPA is an effective solution to the investment inefficiency caused by the negative externalities of security investments.

Positive Externality

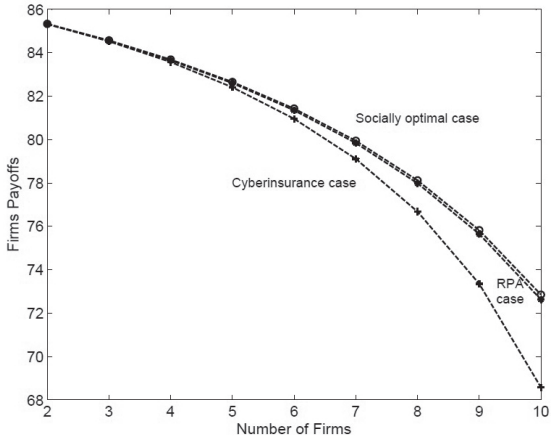
The preceding subsection demonstrates that when security investments generate negative externalities, firms will set up a risk pool and use it to cover a positive proportion of risks. RPAs help address firms' overinvestment incentives through the internalization and moral hazard effects. When security investments generate positive externalities, do firms still have an incentive to set up an RPA? Proposition 4 provides some insights on the firms' investment incentive with an RPA:

> *Proposition 4: When security investments generate positive externalities, firms invest less in security in the RPA case (as compared with the cyberinsurance-only case) if the risks covered in the RPA are sufficiently small (i.e., $\partial x_i/\partial q|_{q=0} < 0$).*

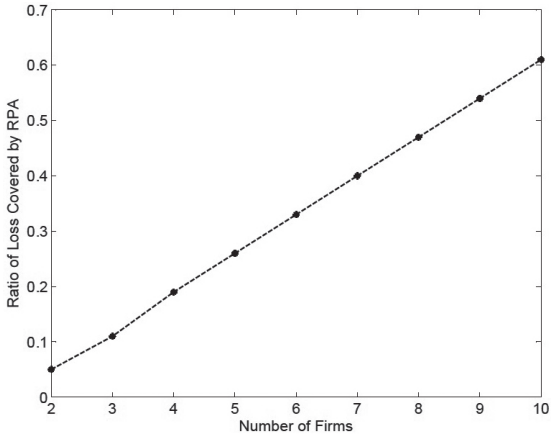
In the case of positive externalities, we have $\partial x_i/\partial q|_{q=0} < 0$. Again, a firm invests less in security protections if firms set up a risk pool and allocate a very small proportion of risk to the pool. The positive externalities of security investments lead to insufficient investment incentives for firms. Even though the internalization effect helps mitigate the underinvestment incentive, the moral hazard effect dampens firms' investment incentives and undermines the capability of RPAs to internalize the positive externalities. The moral hazard effect always dominates over the internalization



(a) Firms' security investments



(b) Firms' payoffs



(c) Ratio of loss covered by an RPA

Figure 1. Firms' Security Investments, Firms' Payoffs, and the Ratio of Loss Covered by an RPA When Security Investments Generate Negative Externalities

effect. Therefore, when an RPA is used in addition to cyberinsurance, firms have even fewer incentives to invest. Proposition 5 sheds light on firms' incentives to set up a risk pool for positively interdependent security risks:

> *Proposition 5: When security investments generate positive externalities, an RPA is not an incentive-compatible solution for individual firms if it is used to cover only a small proportion of the risk (i.e.,* $\partial x_i/\partial q|_{q=0} < 0$*).*

To understand Proposition 5, we examine Equation (8) in the context of positive externalities. As in the case with negative externalities, the first two terms of Equation (8) cancel out. Because $U'(A-\mu(x_i,X_{-i})L-x_i)>0$, $\partial\mu(x_i,X_{-i})/x_j<0$, and $\partial x_j/q<0$, the third term (including the negative sign) is negative. Therefore, Equation (8) is negative overall. Thus, using a risk pool to cover a small proportion of risks decreases an individual firm's expected payoff. Therefore, firms have no incentive to set up a risk pool for a small proportion of risks. The question, then, is whether firms have an incentive to set up an RPA with a large coverage. Because the closed-form solution of q in this multiplayer game is intractable, we used a numerical approach to search for the possibility that firms are willing to adopt an RPA. In our search, we used a series of exponential breach probability functions, $\mu(x_i,X_{-i})=\exp(-\tau(x_i+b\Sigma_{k=1\ldots n,k\neq i}x_k))$. The exponential function ensures that the value of breach probability is always between 0 and 1 for a positive amount of security investments. We let $\tau\in\{1,2,\ldots,10\}$, which represents different degrees of convexity of the breach probability function. The total number of firms, n, ranges from 2 to 30. We let $b\in\{1/10(n-1), 9/10(n-1),\ldots,1/(n-1)\}$, which ensures that the externality is positive. In addition, the aggregate effect of others' security investments is lower than that of the firm's own security investment. Three increasing and concave payoff functions are examined. They are $U(w)=-\exp(-w)+1$, $U(w)=-w(w-20)$, and $U(w)=\log(w+1)$, which represent different degrees of concavity of the firms' payoffs. We did not find any parameter space in which firms have an incentive to set up a risk pool. Therefore, the incentive-compatibility of the RPA solution is difficult to achieve in the case with positive externalities of security investments.

Managed Security Services

In the previous section, we showed that the effectiveness of RPAs depends on the nature of security risks. The RPA solution is effective in addressing overinvestment issues associated with negatively interdependent risks. However, it cannot address the underinvestment issues associated with positively interdependent risks. In this section, we examine a different security management solution: MSSs (or security management outsourcing). We first assume that the MSSP has the same level of security expertise as the firms. This assumption enables us to highlight the insight that the use of MSSs can be justified from the perspective of risk interdependency—not on the basis that the MSSP is more cost-efficient than the client firms. We later extend the analysis and study the case that the MSSP has a cost advantage.

If a firm uses MSSs, it pays a fixed fee, denoted by t, to the MSSP. We refer to the firms using MSSs as the *member firms* and the firms not using MSSs as *nonmember*

firms. In practice, an SLA is often used to ensure that the MSSP assumes accountability for the security loss and manages the security for the member firms' benefits. In this paper, we assume that the SLA specifies the compensation level that the MSSP pays to a member firm if the latter suffers a security loss. We denote the compensation level as d.

The timing of events is as follows: (1) the MSSP announces the service fee, t; (2) firms decide whether or not to use the MSSs; (3) the MSSP invests in security protections for the member firms, and the nonmember firms obtain the expected reservation payoff, U_s; and (4) the security losses are realized and the compensations are made according to the SLAs.

Because firms are homogeneous, we focus on the symmetric case in which all firms choose the same strategies. The MSSP's problem can be formulated as

$$\begin{aligned} \Pi_m &= \max_{d,t,x_i} \sum_{i=1}^{n} t - \mu\left(x_i, X_{-i}\right) d - x_i \\ \text{s.t. } & \mu\left(x_i, X_{-i}\right) U\left(A - L + d - t\right) + \left(1 - \mu\left(x_i, X_{-i}\right)\right) U\left(A - t\right) \geq U_s. \end{aligned} \tag{9}$$

Constraint (9) ensures that a firm has a higher payoff when outsourcing security management to the MSSP than when it manages security in-house and achieves the reservation payoff. Lemma 1 characterizes the optimal compensation level that the MSSP will establish.

Lemma 1: The loss compensation d satisfies that $d = L$.

When a member firm has a security breach and losses L, the MSSP compensates the firm to the level of d. Because the member firms are risk averse but the MSSP is risk neutral, the MSSP is willing to provide full insurance to the member firms. As a result, the member firms transfer all security risks to the MSSP. In this regard, the MSSP serves as a third-party insurer in addition to a professional service provider [1]. This is in contrast to the RPA, with which each member firm has to share $1/n$ of the total loss.

Using the result in Lemma 1, the MSSP's problem can be simplified as

$$\begin{aligned} \Pi_m &= \max_{t,x_i} \sum_{i=1}^{n} t - \mu\left(x_i, X_{-i}\right) L - x_i \\ \text{s.t. } & U\left(A - t\right) \geq U_s. \end{aligned} \tag{10}$$

Proposition 6 gives the MSSP's investment decisions for the member firms:

Proposition 6: When all individual firms collectively outsource their security management to the MSSP, the MSSP makes the security investment at the optimal level.

Collective outsourcing occurs when all firms outsource their security management to the MSSP. Proposition 6 shows that in collective outsourcing, investment inefficiency caused by risk interdependency is addressed: the MSSP makes the security investment at the optimal level for all member firms. The optimal level is achieved because the

investment decision making is shifted to one entity, so that network externalities are completely internalized. As a result, the investment inefficiency is eliminated.

Sustainability of Collective Outsourcing

Although collective outsourcing can lead to optimal security investments (made by the MSSP), whether this solution is incentive-compatible to individual firms is still unclear. The question is this: When all other firms use MSSs, does an individual firm have the incentive to defect from using the MSSs? When a firm defects, it has to manage security in-house, but it can still use cyberinsurance to hedge against its security risks. The payoff of the defecting firm can be considered as a firm's reservation payoff (outside option) when deciding on whether to use MSSs (i.e., U_s). We next examine whether collective outsourcing is sustainable as an equilibrium for individual firms. For analysis tractability, we again assume that the security investments are additive [24]. In particular, $\mu(x_i, X_{-i}) = p(x_i + b\Sigma_{k=1\ldots n, k\neq i} x_k)$, where p is a decreasing and convex function, $p'(.) < 0$, and $p''(.) > 0$. This breach probability function ensures that $\mu_i'(.) < 0$ and $\mu_{ii}''(.) > 0$. In the case of negative externality, let $b < 0$. This ensures $\zeta_i'(.) > 0$. In the case of positive externality, let $b > 0$. This ensures $\zeta_i'(.) < 0$.

Suppose that a firm defects but that the other $n-1$ firms still outsource their security management to the MSSP. The defecting firm's payoff is $\pi^d = U(A - p(x^d + b(n-1)x^{md})L - x^d)$ where x^d represents the defecting firm's security investment level and x^{md} represents the MSSP's investment level for a member firm when a firm defects.

Let $U_s = \pi^d$. The MSSP's problem can be represented as

$$\Pi_m^d = \max_{t, x_i} \sum_{i=1}^{n} t - p\left(x_i + b \sum_{k=1, k\neq i}^{n} x_k\right)L - x_i \tag{11}$$

$$\text{s.t. } U(A-t) \geq U\left(A - p\left(x^d + b(n-1)x^{md}\right)L - x^d\right). \tag{12}$$

Constraint (12) is an individual rationality constraint ensuring that a firm has a higher payoff when using MSSs than when managing security in-house and purchasing cyberinsurance. This constraint requires that the MSSP establishes a fee that would not result in member firm defection. Lemma 2 characterizes the optimal service fee that the MSSP charges:

> *Lemma 2: The optimal service fee charged by the MSSP satisfies* $t = p(x^d + b(n-1)x^{md})L + x^d$.

The MSSP profits from the service fee. A for-profit MSSP charges a service fee that is as high as possible to maximize its profit, while still ensuring that firms are willing to use the MSS. Suppose a firm defects. The total expected cost for IT security for the defecting firm is $p(x^d + b(n-1)x^{md})L + x^d$ (i.e., the cyberinsurance premium plus the security investment). The maximum service fee for the MSSs is therefore equal to the expected total security cost of the defecting firm, so that any firm is indifferent between defecting or not.

According to Equation (11) and Lemma 2, the MSSP's profit is

$$\Pi_m^d = n\left[p\left(x^d + b(n-1)x^{md}\right)L + x^d - \left(p\left(\left(1+b(n-1)\right)x^o\right)L + x^o\right)\right].$$

For collective outsourcing to be viable, the MSSP must charge a fee that can cover its service cost. To derive additional insight, we use a general exponential breach probability (i.e., $p(y) = \exp(-\lambda y)$) to compare between the service fee (i.e., $p(x^d + b(n-1)x^{md})L + x^d)$) and the service cost (i.e., $p((1 + b(n-1))x^o)L + x^o)$. Proposition 7 characterizes the condition under which collective outsourcing is sustainable as an equilibrium:

Proposition 7: All firms are willing to outsource their security management if

$$(1-b)b(n-1) - \ln\left(\left(1+b(n-2)\right)^{b(n-1)}\left(1+b(n-1)\right)^{(1-b)}\right) > 0.$$

When the condition in Proposition 7 holds, the expected security cost incurred by a defecting firm (i.e., $p(x^d + b(n-1)x^{md})L + x^d)$) is higher than the service cost incurred by the MSSP for each member firm in collective outsourcing (i.e., $p((1 + b(n-1))x^o)L + x^o)$. According to Lemma 2, the MSSP charges a fee equal to a defecting firm's security cost. This service fee not only ensures that all firms have incentives to use MSSs but also yields a positive profit for the MSSP. Therefore, the equilibrium of collective outsourcing using MSSs is sustainable when the condition in Proposition 7 holds.

The sustainability of collective outsourcing, although achievable with a small number of firms, becomes increasingly difficult to achieve as the number of firms increases. When the number of firms is larger, an individual defecting firm gains more from the MSSP's collective operations. In the case of negative externalities, a larger number of firms provides the MSSP with more incentives to reduce the security investment to address the overinvestment issue for each member firm, making it easier for a defecting firm to beat the MSSP in security investment and drive hackers away. In the case of positive externalities, a larger number of firms induces the MSSP to increase the security investment to address the underinvestment issue for each member firm, making it easier for a defecting firm to free-ride. Therefore, an individual firm is more likely to defect, and the retention of all member firms is then more difficult for the MSSP. As a result, there is a maximum number of firms with which the MSSP can induce all firms to use the MSSs and address the investment inefficiency. Figure 2 demonstrates the maximum number of firms for which a sustainable equilibrium exists, given the degree of network externalities, b.

The increase in the degree of network externalities generates two countervailing effects on firms' incentives to defect. In the case of negative externalities ($b < 0$), when the degree of network externalities is higher (b is smaller), the advantage of the MSS solution in internalizing externalities of the security investments is more evident, and a firm is more willing to use the MSSs. Whereas a firm also benefits more if it deviates from using the MSSs. This is because higher negative externalities induce the MSSP to invest less aggressively, and, as a result, it is easier for a defecting firm to beat the MSSP in security investment and drive hackers away. An individual firm is thus less

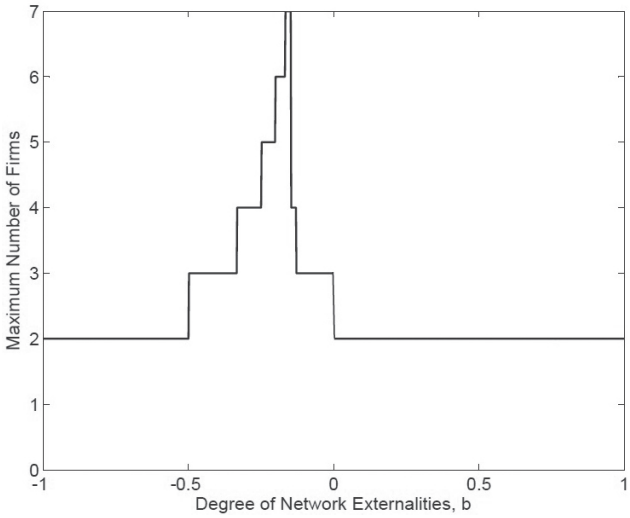


Figure 2. Maximum Number of Firms in Collective Outsourcing Equilibrium as a Function of b

willing to pay for MSSs, forcing the MSSP to lower the service fee. The fee that the MSSP can charge depends on the trade-off between these two effects. As a result, the maximum number of firms that ensures a sustainable equilibrium is first increasing in b and then decreasing in b.

When the security investments generate positive externalities (i.e., $b > 0$), the defecting firm can free-ride on the MSSP's collective security operations for member firms. As a result, the MSSP has to keep the service fee low to retain the member firms. When the number of firms is larger, the benefit of free-riding is higher, and the service fee that the MSSP charges cannot cover the expected cost of serving a firm. As a result, collective outsourcing to the MSSP is a sustainable equilibrium only when $n = 2$. It is worth noting that when security investments generate positive externalities and the MSSP is more cost-efficient, the maximum number of firms in a sustainable equilibrium may be higher than two, as is illustrated in the next section.

When $b = 0$, the firms' security risks are independent, and security investments have no externalities. The service fee that the MSSP charges is equal to the security cost that the MSSP incurs to serve a member firm. As a result, the MSSP always makes zero profit (i.e., P7's condition never holds). This case is a trivial one.

MSSP's Cost Efficiency

The previous analysis presents a counterintuitive result: Even though the MSSP serving all firms invests at the optimal level and firms all benefit from security outsourcing, collective outsourcing to the MSSP might not arise as an equilibrium. This phenomenon occurs because a firm, even after defecting, might indirectly benefit from the MSSP's

security operations, resulting in a higher payoff for the firm than actually using the MSSs. As a result, the MSSP cannot charge a fee that sustains collective outsourcing and results in a profit.

In practice, the MSSP is often more capable of managing security because of its better technology, more experienced staff, and higher operational efficiency. A major reason for which individual firms outsource security management is to leverage the MSSP's cost efficiency [1, 3]. In this subsection, we examine how the MSSP's cost advantage is weakened by network externalities of security investments. We assume that the MSSP incurs an investment cost, ψx_i, where $\psi \in [0, 1]$ captures the level of cost efficiency. When $\psi = 1$, the MSSP has the same level of cost efficiency as individual firms; as ψ decreases, the MSSP becomes more cost-efficient than individual firms. The MSSP's problem can be represented as

$$\Pi = \max_{t, x_i} \sum_{i=1}^{n} t - p\left(x_i + b\sum_{k=1, k\neq i}^{n} x_k\right)L - \psi x_i$$

$$\text{s.t. } U(A-t) \geq U\left(A - \boldsymbol{p}\left(x^d + b(n-2)x^{md}\right)L - x^d\right).$$

Proposition 8 presents the condition under which collective outsourcing arises as an equilibrium when the MSSP is more cost-efficient than individual firms:

Proposition 8: When the MSSP is more cost-efficient than the individual firms ($0 < \psi < 1$), all firms decide to outsource their security services if

$$(1-b)\left(1-\psi+b(n-1)\right)+\left(b(n-1)+(1-b)\psi\right)\ln\psi$$

$$-\ln\left(\left(1+b(n-2)\right)^{b(n-1)}\left(1+b(\boldsymbol{n}-1)\right)^{\psi(1-b)}\right)+(1-b)(1-\psi)\ln(\lambda L) > 0.$$

When the MSSP is more cost-efficient than individual firms ($0 < \psi < 1$), the maximum number of firms yielding a collective outsourcing equilibrium depends on the level of cost efficiency (ψ), in addition to the degree of network externalities (b). Figure 3 illustrates the maximum number of firms with which collective outsourcing arises as a sustainable equilibrium, given the level of cost efficiency. Similar to the degree of network externalities, cost efficiency affects the firms' defection incentives through two countervailing effects. On the one hand, a more efficient MSSP (ψ is smaller) is more capable of managing the security risks than are individual firms. Therefore, an individual firm is more willing to use the MSSs. This is the cost-efficiency effect. On the other hand, a defecting firm benefits more by taking advantage of the MSSP's collective security management when the MSSP is more cost-efficient. This effect decreases a firm's willingness to pay for the MSS. This is the defection effect. Figure 3 illustrates the maximum number of firms in a sustainable equilibrium when the MSSP is more cost-efficient. It shows that when the security investments generate positive externalities ($b = 0.1$), the maximum number of firms in a collective outsourcing equilibrium is first increasing and then decreasing in ψ. When the security investments generate negative externalities ($b = -0.1$), the cost-efficiency effect dominates the defection effect when the MSSP's cost efficiency is high (ψ is small). Therefore, collective outsourcing is more likely to arise (i.e., all firms are willing to use the MSS) when ψ is small.[4] However, when ψ is large enough (i.e., the MSSP is

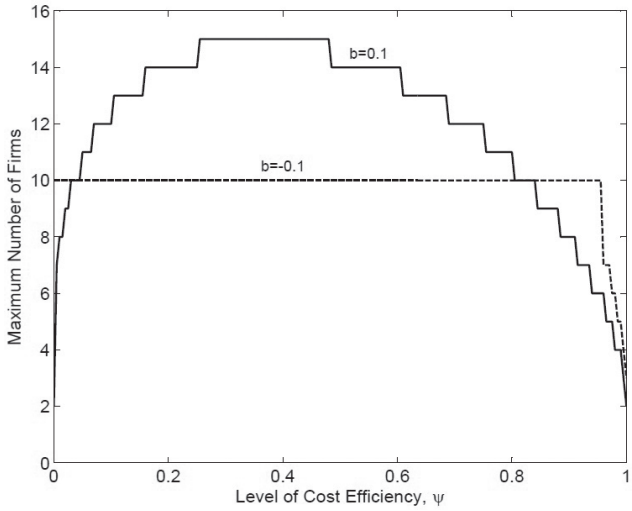


Figure 3. Maximum Number of Firms in a Collective Outsourcing Equilibrium as a Function of ψ

less cost-efficient), the cost-efficiency effect is weakened and the maximum number of firms decreases to two.

Heterogeneous Firms

In this paper, we follow the classic literature on risk pooling and focus on ex ante homogeneous firms. In this section, we extend the model and discuss the case that firms have heterogeneous security losses. In particular, we assume that there are two types of firms: type-1 firms and type-2 firms. In a security breach, a type-1 firm loses L_1, and a type-2 firm loses L_2, where $L_1 > L_2$. Let the total numbers of type-1 firms and type-2 firms be n_1 and n_2, respectively. We have $n = n_1 + n_2$.

When firms use cyberinsurance only, we can verify that a firm still overinvests when the security investments generate negative externalities and underinvests when the security investments generate positive externalities. We next examine firms' security investments and expected payoffs in the RPA case. The expected payoff of a type-1 firm can be represented by

$$\begin{aligned}\pi_i^1 = {} & \mu\left(x_i^1, X_{-i}^1\right)\left(\sum_{k=0}^{n_1-1}\sum_{j=0}^{n_2} b\left(k, n_1-1, \zeta\right) b\left(j, n_2, \zeta\right)\right. \\ & \cdot U\left(A - L_1 + \frac{\left(n-1-k-j\right)q_1 L_1}{n} + I_i^1 - \mu\left(x_i^1, X_{-i}^1\right) I_i^1 - x_i^1\right)\Bigg) \\ & + \left(1-\mu\left(x_i^1, X_{-i}^1\right)\right)\left(\sum_{k=0}^{n_1-1}\sum_{j=0}^{n_2} b\left(k, n_1-1, \zeta\right) b\left(j, n_2, \zeta\right)\right. \\ & \left. \cdot U\left(A - \frac{kq_1 L_1 + jq_2 L_2}{n} - \mu\left(x_i^1, X_{-i}^1\right) I_i^1 - x_i^1\right)\right), \\ & \text{s.t. } I_i^1 \le \left(1-q_1\right) L_1.\end{aligned}$$

And, the expected payoff of a type-2 firm can be represented by

$$\pi_i^2 = \mu\left(x_i^2, X_{-i}^2\right)\left(\sum_{k=0}^{n_1}\sum_{j=0}^{n_2-1} b\left(k, n_1, \zeta\right) b\left(j, n_2 - 1, \zeta\right)\right.$$
$$\left. \cdot\, U\left(A - L_2 + \frac{(n-1-k-j)q_2 L_2}{n} + I_i^2 - \mu\left(x_i^2, X_{-i}^2\right) I_i^2 - x_i^2\right)\right)$$
$$+ \left(1 - \mu\left(x_i^2, X_{-i}^2\right)\right)\left(\sum_{k=0}^{n_1}\sum_{j=0}^{n_2-1} b\left(k, n_1, \zeta\right) b\left(j, n_2 - 1, \zeta\right)\right.$$
$$\left. \cdot\, U\left(A - \frac{kq_1 L_1 + jq_2 L_2}{n} - \mu\left(x_i^2, X_{-i}^2\right) I_i^2 - x_i^2\right)\right),$$
$$\text{s.t. } I_i^2 \le \left(1 - q_2\right) L_2,$$

where q_1 (q_2) is the ratio of loss covered by the risk pool for type-1 firms (type-2 firms). Since the RPA is a mutual insurance organization and the participating firms equally share the loss as equity holders, the RPA covers the same amount of loss for all the firms. We therefore focus on the case that $q_1 L_1 = q_2 L_2$. Differentiating π_i^j w.r.t. I_i^j, we get $I_i^j = (1 - q_j)L_j$, where $j = 1, 2$.

The expected payoffs for type-1 and type-2 firms are, respectively,

$$\pi_i^1 = \mu\left(x_i^1, X_{-i}^1\right)\left(\sum_{k=0}^{n_1-1}\sum_{j=0}^{n_2} b\left(k, n_1 - 1, \zeta\right) b\left(j, n_2, \zeta\right)\right.$$
$$\left. \cdot\, U\left(A - \frac{(k+j+1)}{n} q_1 L_1 - \mu\left(x_i^1, X_{-i}^1\right)\left(1 - q_1\right) L_1 - x_i^1\right)\right)$$
$$+ \left(1 - \mu\left(x_i^1, X_{-i}^1\right)\right)\left(\sum_{k=0}^{n_1-1}\sum_{j=0}^{n_2} b\left(k, n_1 - 1, \zeta\right) b\left(j, n_2, \zeta\right)\right.$$
$$\left. \cdot\, U\left(A - \frac{k+j}{n} q_1 L_1 - \mu\left(x_i^1, X_{-i}^1\right)\left(1 - q_1\right) L_1 - x_i^1\right)\right)$$

and

$$\pi_i^2 = \mu\left(x_i^2, X_{-i}^2\right)\left(\sum_{k=0}^{n_1}\sum_{j=0}^{n_2-1} b\left(k, n_1, \zeta\right) b\left(j, n_2 - 1, \zeta\right)\right.$$
$$\left. \cdot\, U\left(A - \frac{(k+j+1)}{n} q_1 L_1 - \mu\left(x_i^2, X_{-i}^2\right)\left(1 - q_2\right) L_2 - x_i^2\right)\right)$$
$$+ \left(1 - \mu\left(x_i^2, X_{-i}^2\right)\right)\left(\sum_{k=0}^{n_1}\sum_{j=0}^{n_2-1} b\left(k, n_1, \zeta\right) b\left(j, n_2 - 1, \zeta\right)\right.$$
$$\left. \cdot\, U\left(A - \frac{k+j}{n} q_1 L_1 - \mu\left(x_i^2, X_{-i}^2\right)\left(1 - q_2\right) L_2 - x_i^2\right)\right).$$

Since the analytical solutions to the case with heterogeneous firm are intractable, we use numerical examples to illustrate the equilibrium security investments, the firms' payoffs, and the equilibrium pool coverages. Similar to the numerical examples in the Risk Pooling Arrangements section, we assume $\mu(x_i, X_{-i}) = \exp(-2(x_i + b\Sigma_{k=1\ldots n, k\neq i} x_k))$, where $b = -(1/15)$ and $U(w) = -w(w - 20)$. In addition, we let $A = 8$, $L_1 = 6$, and $L_2 = 4$. We assume that type-1 firms account for about half the firms. In particular, $n_1 = n_2 = n/2$ when n is an even number and $n_1 = n_2 - 1$ when n is an odd number. Figures 4 show

the security investments, the firms' payoffs, and the ratios of loss coverage for type-1 and type-2 firms.

Figure 4a shows the firms' security investments in the cyberinsurance-only case, the RPA case, and the optimal case when security investments generate negative externalities. The solid curves represent a type-1 firm's security investments, and the dash curves represent a type-2 firm's security investments. With heterogeneous firms, RPAs can still mitigate firms' overinvestment incentives. Both the type-1 firm's and type-2 firm's security investments in the RPA case are significantly lower than their investments in the cyberinsurance-only case. Figure 4b compares the firm's expected payoffs. The curves show that the firm's expected payoffs in the RPA case are higher than their payoffs in the cyberinsurance-only case. Figure 4c illustrates the optimal ratios of loss covered by the risk pool for type-1 firms and type-2 firms. Similar to Figure 1c, the pool coverages increase as the number of firms in the pool increases. We also examined the case in which security investments generate positive network externalities and found that the RPA cannot address the underinvestment issues. All the findings in the Risk Pooling Arrangements section hold qualitatively.

We then examine firms' security investments and expected payoffs in the MSS case. The MSSP's profit can be represented as

$$\Pi_m = \sum_{i=1}^{n} t_i - \mu\left(x_i, X_{-i}\right) d_i - x_i$$

$$\text{s.t. } \mu\left(x_i, X_{-i}\right) U\left(A - L_i + d_i - t_i\right) + \left(1 - \mu\left(x_i, X_{-i}\right)\right) U\left(A - t_i\right) \geq U_{si}.$$

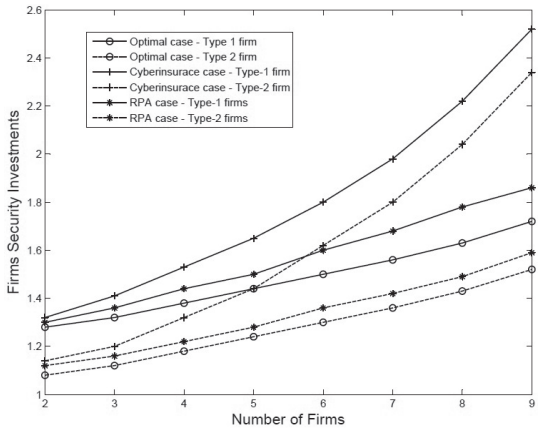
As we described in the Managed Security Services section, the MSSP has extensive security expertise and is therefore capable of evaluating the clients' security. In practice, the MSSP often needs to conduct an on-site inspection before serving a client. It is reasonable to assume that the MSSP can accurately diagnose and separate type-1 firms and type-2 firms. This assumption ensures that the MSSP does not need to practice price differentiation. Differentiating Π_m w.r.t. d_i, we have $d_i = L_i$. The MSSP's profit can be simplified as

$$\Pi_m = \max_{d_i, t_i, x_i} \sum_{i=1}^{n} t_i - \mu\left(x_i, X_{-i}\right) d_i - x_i$$

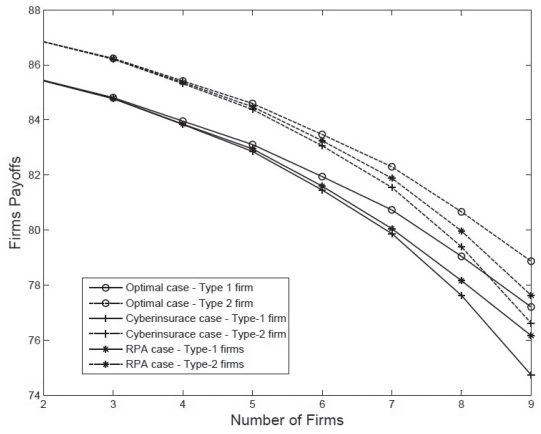
$$\text{s.t. } U\left(A - t_i\right) \geq U_{si}.$$

Again, we use numerical examples to illustrate the maximum number of firms for which a sustainable equilibrium exists, given the degree of network externalities, b. We use the same parameter specifications as in Figure 4. In particular, $\mu(x_i, X_{-i}) = \exp(-2(x_i + b\Sigma_{k=1\ldots n, k\neq i} x_k))$, $U(w) = -w(w - 20)$, $A = 8$, $L_1 = 6$, and $L_2 = 4$. In addition, $n_1 = n_2 = n/2$ when n is an even number, and $n_1 = n_2 - 1$ when n is an odd number.

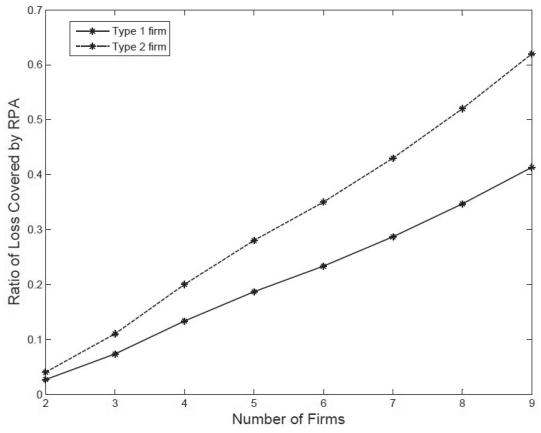
Figure 5 shows that when the security investments generate negative externalities (i.e., $b < 0$), the maximum number of firms that ensures a sustainable equilibrium is first increasing in b and then decreasing in b. When firms are heterogeneous, the countervailing effects of network externalities on the MSSP's service fee identified in the section of managed security services still exist. As a result, the maximum



(a) Firms' security investment in the heterogeneous case



(b) Firms' payoffs in the heterogeneous case



(c) Ratio of loss covered by an RPA in the heterogeneous case

Figure 4. Firms' Security Investments, Firms' Payoffs, and the Ratios of Loss Covered by an RPA When Security Investments Generate Negative Externalities in the Heterogeneous Case with Two Types of Firms

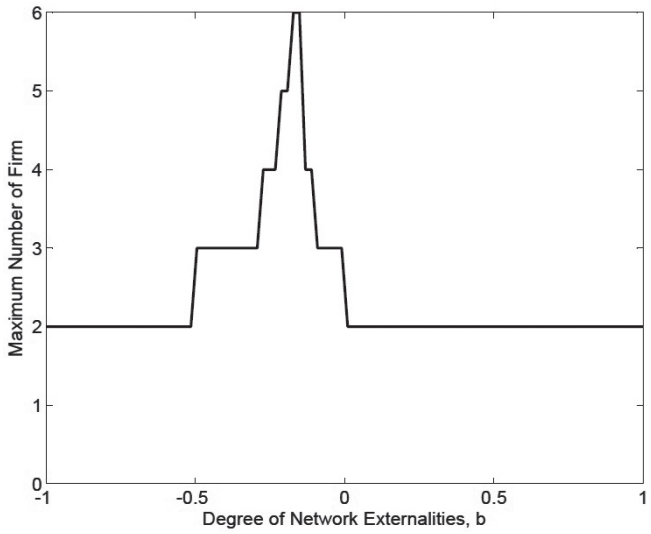


Figure 5. Maximum Number of Firms in Collective Outsourcing Equilibrium as a Function of b in the Heterogeneous Case with Two Types of Firms

number of firms for a sustainable equilibrium changes in the same pattern as that in the homogeneous case. When the security investments generate positive externalities (i.e., $b > 0$), collective outsourcing to the MSSP is a sustainable equilibrium only when $n = 2$. The analysis and numerical illustrations show that all the findings in the previous sections hold qualitatively.

It is worth noting that the use of a common increasing and concave utility function in this paper, although rooted in the risk management literature, could be potentially restrictive. In reality, the payoffs of heterogeneous firms may be better modeled using different functions. The present study is the first step to gaining insights in using alternative solutions to manage interdependent security risks. A thorough study of the alternative risk management solutions for heterogeneous firms deserves further research.

Discussion and Conclusion

THE OBJECTIVE OF SECURITY RISK MANAGEMENT is to appropriately use security resources to reduce firms' risk exposure. The risk management approaches considered in this paper—third-party cyberinsurance, MSSs, and RPAs—differ in their effectiveness in reducing risk exposure and inducing efficient security investments. Both cyberinsurance and MSSs provide complete risk transfer. As compared with cyberinsurance, MSSs induce more efficient allocation of security resources because the MSSP, when serving all firms, internalizes the externalities of security investments between the member firms. RPAs, in contrast, do not provide complete risk transfer. However, they still help to induce more efficient security investments than cyberinsurance when security investments generate negative externalities. Both the internalization

effect and the moral hazard effect associated with RPAs mitigate firms' overinvestment incentives.

In this paper, we focused on risk-averse firms. Note, however, that the analysis on the RPA and MSS solutions can also be applied to the case with risk-neutral firms, and all the findings still hold. Even though the risk-neutral firms are indifferent to the choices of adopting cyberinsurance to hedge risks and bearing random losses, they might still be willing to adopt the solutions that address interdependent security risks. In particular, risk-neutral firms have incentives to use RPAs when the security investments generate negative externalities. In addition, MSSs can be used to address the investment inefficiency caused by interdependent risks; however, collective outsourcing to an MSSP is not sustainable when the number of firms is large. Risk-loving firms are likely to actively pursue risks to maximize their payoffs, and they are beyond the scope of this research.

In this paper, we assumed that the amount of loss is fixed in a security breach. If a firm's loss is a random amount in a security breach and the insurance company can specify a *complete* contingent insurance contract, a risk-neutral insurance company still provides full insurance to the risk-averse firm. In that case, the insurance company must be able to expect all loss contingencies and write the *complete* contingent contract, which details the compensation level for each loss level. Similarly, the MSSP will offer full compensation for each loss level.

RPAs have traditionally been implemented in the forms of self-insurance, captives, risk retention groups, and pools to insure a wide variety of risks, such as medical practices, municipal liability, employee pension, and employee health care insurance. However, they have not been widely employed in the area of information security. Information security risks have the feature of risk interdependency, which challenges traditional risk management solutions and calls for alternative solutions. RPAs make firms share risks with one another within the pool and hence motivate firms to consider others' risks when making investment decisions. They thus have the potential to be an effective solution for interdependent risks in the area of information security. RPAs' ability to address interdependent information security risks also makes their use desirable, even when firms are risk-neutral. Thus, we see another advantage of using RPAs in information security: they empower firms to actively control interdependent risks, in addition to hedging risks for risk-averse firms.

Additional advantages of using RPAs in information security include flexible policy development and larger capacity. Insurability of information security risks is often limited in the cyberinsurance market because of the lack of experience in dealing with new security risks. RPAs allow the policy terms to be tailored to member firms and therefore to help cover new security risks. The cyberinsurance market is also limited in its capacity. RPAs could substantially increase the capacity of the risk management market, helping to insure against vast and ever-increasing information security risks.

Firms also face many operational challenges in implementing RPAs. In general, the process of implementation involves identifying the insurance coverages, determining premiums for the coverages, determining captive ownership and capitalization,

identifying where the captive is formed and regulated, issuing insurance policies, and managing claims [32]. Firms outside the insurance industry often lack experience in risk underwriting and claims management. Entering such a new business area would likely be very costly for them. In practice, insurance companies offer rent-a-captive services that provide firms with access to captive facilities. Thus, firms can use a rent-a-captive approach to establish and run their RPAs for information security risks. At the initial stage of implementation, a firm might start with a single-parent captive (i.e., an RPA within one firm) to manage security risks within its business units. Later, the firm might expand the RPA operation to the multifirm context.

Regulatory restrictions pose additional challenges to the implementation of RPAs. The insurance market is highly regulated, and the development of RPAs is subject to regulatory attitudes. For example, in many jurisdictions, certain lines of insurance can be underwritten only by an admitted commercial insurer, not by a mutual insurer. Other factors affecting the adoption of RPAs 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. Considering the potential that RPAs offer in coordinating firms' security investments, firms should actively promote RPAs to their regulatory agencies.

Security outsourcing enables firms to tap into the MSSP's security resources, skills, and capabilities. In practice, SLAs are often used in service outsourcing to specify performance expectations, establish accountability, and detail remedies or consequences if performance or service quality standards are not met [1]. In security outsourcing, SLAs enable firms to transfer the security risks to external service providers. In this regard, the MSSP serves not only as a service provider but also as an insurer. The MSSP takes into account the interaction between member firms when making security decisions for them. The MSS approach, therefore, internalizes the externalities of security investments and provides a solution for interdependent security risks.

The MSS approach also provides a collective solution to create security protections that are difficult for individual firms to implement. For example, serving clients over different jurisdictions enables the MSSP to trace and collapse botnets, which are geographically distributed [33]. From individual firms' perspectives, devoting sufficient efforts to combat such distributed networks is often unwarranted. In this regard, MSSs can offer a potential approach for managing distributed and interdependent risks.

The MSS solution yields the optimal investment level when all interdependent firms adopt this solution. However, executives and security managers should recognize that collective outsourcing might not be incentive-compatible when the number of firms is large. Because of risk interdependency, an individual firm might be better off if it manages security in-house instead of using MSSs. Such an incentive of defection exists even when the MSSP has a cost advantage over individual firms in security management. These findings help explain why firms might not use the MSS solution, even when the MSSPs are often more capable of managing security risks. Executives and security managers should recognize the advantages and limitations of the MSS approach and choose their risk management solutions according to the interdependent nature of security risks.

The present study may be extended in many directions. First, we focused on the incentive-compatible solutions, and the proposed solutions help firms address the investment inefficiency issues and improve their security toward the optimal outcome. The findings in the present study provide useful managerial implications and insights. In the future, it would be desirable to investigate the incentive-compatible approaches that always yield the optimal solution in the domain of information security. Second, we compared RPA and MSS solutions with cyberinsurance in addressing interdependent security risks. Future research might consider the interactions among the cyberinsurance, RPA, and MSS solutions. For example, the MSSP has better security skills than do the firms, in addition to cost advantages, and it may differentiate its services to better compete against the other two security management mechanisms. This is particularly important when firms are heterogeneous. The MSSP's service differentiation and competitive strategies in the presence of heterogeneous firms merit in-depth study. Finally, future research might also study various implementation issues of the risk-management solutions. For example, the use of SLAs in security outsourcing requires firms to deploy various measures to monitor the MSSP's performance and enforce the contract terms. Reputation systems for MSSPs can be an effective mechanism to motivate the MSSP to behave properly in the long term. The design of diverse mutual insurance policies for different types of IT security risks deserves more research attention.

Acknowledgment: Andrew B. Whinston greatly appreciates support from National Science Foundation grant number 0831338 for the completion of this paper. The authors thank three anonymous reviewers and the seminar participants at the University of Utah, the University of North Carolina at Charlotte, the University of North Carolina at Greensboro, and International Conference on Information Systems (ICIS2009) for their feedback on the early draft of this paper.

Notes

1. The principle of indemnity is an insurance principle stating that an insured may not be compensated by the insurance companies in an amount exceeding the insured's economic loss. Therefore, a firm is not allowed to purchase insurance coverage from multiple insurers resulting in an amount of compensation or payout that is higher than the total economic loss [43].

2. The proofs of the lemmas and propositions are available upon request of the authors.

3. We also examined other parameter values (A and L) for the payoff function and other payoff function forms and found that the insights hold qualitatively.

4. When $b = -0.1$, the total number of firms must be no more than 10 to ensure that $x_i + b\Sigma_{k=1...n,k\neq i} x_k > 0$.

References

1. Allen, J.; Gabbard, D.; and May, C. Outsourcing managed security services. Carnegie Mellon Software Engineering Institute, Pittsburgh, 2003 (available at www.cert.org/archive/pdf/omss.pdf).

2. Anderson, R. and Moore, T. The economics of information security. *Science, 314* (October 27, 2006), 610–613.

3. Axelrod, C.W. *Outsourcing Information Security.* Boston: Artech House, 2004.

4. Cavusoglu, H.; Raghunathan, S.; and Yue, W.T. Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems, 25,* 2 (Fall 2008), 281–304.

5. Cremonini, M., and Nizovtsev. D. Risks and benefits of signaling information system characteristics to strategic attackers. *Journal of Management Information Systems,* 26, 3 (Winter 2009–10), 241–274.

6. CSI computer crime and security survey 2010/2011. Computer Security Institute, New York, 2011 (available at http://gocsi.com/survey/).

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

8. Doherty, N.A., and Dionne, G. Insurance with undiversifiable risk: Contract structure and organizational form of insurance firms. *Journal of Risk and Uncertainty, 6,* 2 (1993), 187–203.

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

10. Gordon, L.A., and Loeb, M.P. The economics of information security investment. *ACM Transactions on Information and Systems Security, 5,* 4 (2002), 428–457.

11. Gordon, L.A.; Loeb, M.P.; and Lucyshyn, W. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy, 22,* 6 (2003), 461–485.

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

13. Gupta, A., and Zhdanov, D. Growth and sustainability of managed security services networks: An economic perspective. *MIS Quarterly, 36,* 4 (2012), 1109–1130.

14. Herath, H.S.B., and Herath, T.C. Investments in information security: A real options perspective with Bayesian postaudit. *Journal of Management Information Systems, 25,* 3 (Winter 2008–9), 337–375.

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

16. Hui, K.-L.; Hui, W.; and Yue, W.T. Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems, 29,* 3 (Winter 2012–13), 117–154.

17. Humphreys, P.K.; Lai, M.K.; and Sculli, D. An inter-organizational information system for supply chain management. *International Journal of Production Economics, 70,* 3 (2001), 245–255.

18. Kumar, R.L.; Park, S.; and Subramaniam, C. Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems, 25,* 2 (Fall 2008), 241–280.

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

20. Lee, C.H.; Geng, X.; and Raghumathan, S. Contracting information security in the presence of double moral hazard. *Information Systems Research, 24,* 2 (2013), 295–311.

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

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

23. Malamud, S.; Rui, H.; and Whinston, A.B. Optimal risk sharing with limited liability. Working Paper, National Center of Competence in Research Financial Valuation and Risk Management, Lausanne, 2012.

24. Managed security services hot despite cool economy due to growing threats, mobile devices, move to cloud. Infonetics Research Report, Campbell, CA, September 27, 2011.

25. Marshall, J.M. Insurance theory: Reserves versus mutuality. *Economic Inquiry, 12,* 4 (1974), 476–492.

26. Mayers, D. Ownership structure across lines of property-casualty insurance. *Journal of Law and Economics, 31,* 2 (1988), 351–378.

27. Mayers, D., and Smith, C.W. Contractual provisions, organizational structure and conflict in insurance markets. *Journal of Business, 54,* 3 (1981), 407–434.

28. McQuillan, L.H. How to work with a managed security service provider. In H.F. Tipton and M. Krause (eds.), *Information Security Management Handbook.* Boca Raton, FL: CRC Press, 2007, pp. 631–642.

29. Mohan, R. 2010. How to defend against DDoS attacks? *Security Week,* April 27, 2010 (available at www.securityweek.com/content/how-defend-against-ddos-attacks/).

30. Moitra, S.D., and Konda, S.L. The survivability of network systems: An empirical analysis. Software Engineering Institute/Computer Emergency Response Team (SEI/CERT) Report no. CMU/SEI-2000-TR-021, Carnegie Mellon University, Pittsburgh, PA, December 2000.

31. Ogut, H.; Menon, N.; and Raghunathan, S. Cyber insurance and IT security investment: Impact of interdependent risk. Working Paper, University of Texas at Dallas, 2005 (available at http://infosecon.net/workshop/pdf/56.pdf).

32. The picture of ART. Swiss Re study, Zurich, February 5, 2003 (available at www.swissre.com/media/news_releases/new_swiss_re_sigma_study__the_picture_of_art.html).

33. Pitsillidis, A.; Levchenko, K.; Kreibich, C.; Kanich, C.; Voelker, G.M.; Paxson, V.; Weaver, N.; and Savage, S. Botnet judo: Fighting spam with itself. Paper presented at the Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 28–March 3, 2010 (available at www.isoc.org/isoc/conferences/ndss/10/pdf/12.pdf).

34. Richmond, W.B.; Seidmann, A.; and Whinston, A.B. Incomplete contracting issues in information systems development outsourcing. *Decision Support Systems, 8,* 5 (1992), 459–477.

35. Rippon, A. Cyber hackers can mess with Google—Are you afraid for your business? EzineArticles.com, 2010 (available at http://ezinearticles.com/?Cyber-Hackers-Can-Mess-With-Google--Are-You-Afraid-For-Your-Business?&id=3882184/).

36. Rothschild, M., and Stiglitz, J. Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. *Quarterly Journal of Economics, 90,* 4 (1976), 629–649.

37. Scott, C. Nearly a fifth of U.S. PCs have no antivirus protection. IDG News Service, May 29, 2012 (available at www.pcworld.com/article/256493/nearly_a_fifth_of_us_pcs_have_no_virus_protection_mcafee_finds.html).

38. Sen, S.; Raghu, T.S.; and Vinze, A. Demand heterogeneity in IT infrastructure services: Modeling and evaluation of a dynamic approach to defining service levels. *Information Systems Research, 20,* 2 (2009), 258–276.

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

40. Subramaniam, C., and Shaw, M.J. A study of the value and impact of B2B e-commerce: The case of Web-based procurement. *International Journal of Electronic Commerce, 6,* 4 (Summer 2002), 19–40.

41. Tung, L. Five ways to defend against a DDos attack. IT News for Australian Business, October 12, 2010 (available at www.itnews.com.au/News/234834,five-ways-to-defend-against-a-ddos-attack.aspx).

42. Varian, H.R. Managing online security risks. *New York Times,* June 1 (2000) (available at http://people.ischool.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html).

43. Vaughan, E.J., and Vaughan, T.M. *Fundamentals of Risk and Insurance,* 10th ed. Hoboken, NJ: John Wiley & Sons, 2008.

44. Wang, E.T.G.; Barron, T.; and Seidmann, A. Contracting structures for custom software development: The impacts of informational rents and uncertainty on internal development and outsourcing. *Management Science, 43,* 12 (1997), 1726–1744.

45. Whang, S. Contracting for software development. *Management Science, 38,* 3 (1992), 307–324.