Journal of Management Information Systems

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

Information Security Outsourcing with System Interdependency and Mandatory Security Requirement

Kai-Lung Hui [a], Wendy Hui [b] & Wei T. Yue [c]

[a] Department of Information Systems, Business Statistics, and Operations Management, Hong Kong University of Science and Technology

[b] Hong Kong University of Science and Technology

[c] Department of Information Systems, City University of Hong Kong

Published online: 09 Dec 2014.

To cite this article: Kai-Lung Hui , Wendy Hui & Wei T. Yue (2012) Information Security Outsourcing with System Interdependency and Mandatory Security Requirement, Journal of Management Information Systems, 29:3, 117-156

To link to this article: http://dx.doi.org/10.2753/MIS0742-1222290304

Information Security Outsourcing with System Interdependency and Mandatory Security Requirement

KAI-LUNG HUI, WENDY HUI, AND WEI T. YUE

KAI-LUNG HUI is an associate professor in the Department of Information Systems, Business Statistics, and Operations Management at the Hong Kong University of Science and Technology. He holds a Ph.D. in information systems from the Hong Kong University of Science and Technology. His research interests include information security and privacy, electronic commerce, and social interaction. His research has been published in scholarly journals, including *American Economic Review: Papers and Proceedings, Management Science, Journal of Management Information Systems,* and *MIS Quarterly.*

WENDY HUI is a senior lecturer at Curtin University. She holds a Ph.D. in information systems from the Hong Kong University of Science and Technology. She has taught in Zayed University and University of Nottingham Ningbo China. Her current research interests include information security and quantitative research methods. Her work has appeared in IS journals, including *Journal of Management Information Systems, Decision Support Systems,* and *IEEE Transactions on Systems, Man and Cybernetics Part A.*

WEI T. YUE is an associate professor in the Department of Information Systems at City University of Hong Kong. He holds a Ph.D. in management information systems from Purdue University. He has done extensive research in the area of information security. His work has appeared in journals including *Management Science, Information Systems Research, Journal of Management Information Systems,* and *Decision Support Systems.*

ABSTRACT: The rapid growth of computer networks has led to a proliferation of information security standards. To meet these security standards, some organizations outsource security protection to a managed security service provider (MSSP). However, this may give rise to system interdependency risks. This paper analyzes how such system interdependency risks interact with a mandatory security requirement to affect the equilibrium behaviors of an MSSP and its clients. We show that a mandatory security requirement will increase the MSSP's effort and motivate it to serve more clients. Although more clients can benefit from the MSSP's protection, they are also subjected to greater system interdependency risks. Social welfare will decrease if the mandatory security requirement is high, and imposing verifiability may exacerbate social welfare losses. Our results imply that recent initiatives such as issuing certification to enforce computer security protection, or encouraging auditing of managed security services, may not be advisable.

Journal of Management Information Systems / Winter 2012–13, Vol. 29, No. 3, pp. 117–155.

ISSN 0742–1222 (print) / ISSN 1557–928X (online)
DOI: 10.2753/MIS0742-1222290304

KEY WORDS AND PHRASES: information security, information security outsourcing, interdependency risks, mandatory security requirement, security compliance.

> Typically, the outsourcer . . . has a central operations room with lots of monitors displaying plenty of monitoring output. Oversubscribed staff attempt to process the barrage of alerts, but focus primarily on the top three to five clients listed on a whiteboard in the corner. If you aren't on the whiteboard, nobody is looking after your gear. [10]

RECENT REPORTS HAVE UNDERSCORED THE GROWTH OF SECURITY OUTSOURCING. For example, more than 30 percent of firms are now outsourcing some part of their security functions [30]. The managed security service provider (MSSP) market in North America is expected to hit a revenue of $3.9 billion in 2016 [50]. A recent survey found that 55 percent and 44 percent of firms are either outsourcing or planning to outsource, respectively, penetration tests and security assessments [40]. The security services that are outsourced range from managing firewalls to implementing security architecture [55]. Firms are also taking greater responsibility in meeting regulatory-driven security requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) or the Gramm–Leach–Bliley Act. Indeed, many firms have highlighted regulatory compliance as a motivating factor for outsourcing; in particular, 77 percent of firms considered regulatory compliance to be either a "very important" or an "important" priority in their information security activities [40].

Increasingly, firms are required to compare their information security activities to established performance expectations in security. This phenomenon, known as "base-lining" [56], is mostly spearheaded by external forces, such as the government, professional organizations such as the Information Systems Audit and Control Association (ISACA) or the Information Systems Security Association (ISSA), and service providers [44]. An indirect consequence of base-lining is that the quality of the protected systems has to meet well-defined security requirements, such as reviewing access logs regularly, adopting clear reporting standards, and so forth. It may not be easy for firms to fulfill these security requirements. For example, the PCI DSS requires firms to conduct vulnerability scanning and penetration tests with a third-party qualified security assessor on a quarterly basis [48]. For firms that do not possess the know-how to manage their own information security functions, outsourcing the protection to an MSSP has become an attractive option [50, 53]. Besides having better expertise and state-of-the-art facilities, an MSSP enjoys economies of scale [49] and often provides complementary services, such as the detection and prevention of security breaches [12, 13].

Despite its many advantages, information security outsourcing may homogenize the architecture or platform of the clients' security systems, which may effectively "endogenize" the security risks of all the clients [37]. Essentially, any security breach

of a client may now spill over to other clients because of the shared architecture and/or platform. As an illustrative example, in 2009, the Chinese government proposed that all personal computers be installed with the Green Dam Youth Escort (GDYE) software, which later was found to contain remotely exploitable vulnerabilities [57]. If a hacker could successfully penetrate one client's system and exploit the GDYE vulnerabilities, then it may be able to compromise the systems of thousands of other clients via the same vulnerabilities. In this case, the clients' systems became virtually "connected" via the use of the common GDYE software. Similarly, in 2010, a successful attack on the database of Silverpop, a popular e-mail service provider with more than 105 corporate clients, contributed to data losses of a number of Silverpop's clients, including McDonald's and Walgreen. It is arguable whether these data losses would have occurred if Silverpop had used a heterogeneous architecture to host its services.

Further, the MSSP may not always deliver a high quality of service. In 2005, CardSystems, which specializes in payment processing, suffered a theft of more than 40 million credit card numbers. Although CardSystems was certified by Savvis, a provider of managed computing and network services, and was believed to have followed the Cardholder Information Security Program (CISP), a later incident response analysis revealed that it did not comply with CISP [60]. The security breach had affected major clients of CardSystems, such as the Merrick Bank.

In 2009, seven restaurants in Louisiana and Mississippi filed a class-action lawsuit against Radiant Systems and Computer World for selling them the Aloha point-of-sale (POS) systems, which were incorrectly described as compliant with the PCI DSS. The suit further alleged that poor business practices related to the Aloha systems had contributed to major data security breaches, which resulted in multiple cases of identity theft. These two examples suggest that the MSSP may not always deliver the promised service quality.

In this paper, we investigate how a mandatory security requirement, such as the GDYE, may affect the extent and benefit of information security outsourcing. In our problem, the clients can choose between outsourcing and in-house development. If they outsource, they would not be able to evaluate or monitor the MSSP's service. The information asymmetry between the clients and the MSSP may cause the MSSP to shirk its duty and provide substandard security quality. More importantly, the clients who outsource their protection to the MSSP may face system interdependency risks, which may offset the benefit that they obtain from the MSSP's better protection. Because the clients' outsourcing decisions are often driven by compliance, the mandatory security requirement is a critical variable that drives some of our key findings.

Our analysis shows that the clients may use the MSSP's service despite expecting the service quality to be lower than that specified in the service-level agreement (SLA). Such a decision is economically rational because of the need to satisfy the mandatory security requirement.[1] Overall, a stringent mandatory security requirement would shift the surplus from clients to the MSSP. Although it may induce the MSSP to work harder, it would also motivate the MSSP to serve more clients, which indirectly decreases social welfare by spawning a greater interdependency risk.[2] Our analysis

shows that the common practice of auditing the MSSP's effort is less effective than liability-driven SLAs in enhancing social welfare.

We make three contributions. First, we develop an integrated analytical framework that incorporates the key features of security outsourcing. This framework can be readily used to analyze different security initiatives and draw practical insights for firms in the security outsourcing business. Second, we show that recent security trends, such as the establishment of security protection standards or the auditing of MSSPs' services [39], can actually reduce social welfare. Third, we extend existing theories in the economics of information security, credence goods, and asymmetric information [2, 3, 19, 20, 58] by critically assessing the robustness of their findings in view of several important contextual characteristics, such as interdependency between clients' systems, the presence of hackers who threaten the clients' information systems, and the presence of industry security regulations.

The rest of this paper is organized as follows. The next section reviews the related literature. We then present our main models and findings. We also extend the model to account for heterogeneous clients, competition, strategic hacking, and shirking clients. We draw managerial and policy implications, and conclude the paper in the last two sections.

Related Literature

THERE HAS BEEN A GROWING BODY OF LITERATURE on the economics of information security (e.g., [11, 15, 21]). In a pioneering work, Gordon and Loeb [24] model the security investment problem from the welfare-maximizing firm's perspective, in which security investment would lead to reduced likelihood of security breach, but too high an investment would bring only marginal benefit. Hence, there exists an optimal investment level that maximizes the firm's profit. Since then, there has been a growing literature that specifically addresses information security investment [27, 32]. Similar to Gordon and Loeb, our model also considers the trade-off between the probability of security breach and security protection efforts. We further allow the clients to outsource security protection to an MSSP, who enjoys greater efficiency in reducing the probability of security breaches. This allows us to extend the analysis in several meaningful ways. First, the clients and the MSSP are engaged in a principal–agent relationship and so information asymmetry becomes prevalent [16]. Second, system interdependency risks arise because the clients share the same security protection platform via the MSSP. Lastly, the possibility to outsource provides an alternative solution for the clients to fulfill the mandatory security requirement.

The literature on information security outsourcing has often assumed that an MSSP will honestly serve the clients (e.g., [17, 18]). In reality, such an assumption may not hold with information asymmetry because clients often cannot fully inspect the quality of the MSSP's service, which could lead to a shirking of responsibility on the part of the MSSP. Our setting, where the MSSP's protection effort is related to security breach probability, and the fact that the MSSP is liable for the client's damage when protection fails, is commonly seen in the product failure and insurance literature (e.g., [46,

51, 52]). Also, the use of software or system liability as an incentive mechanism in managing security risks has been widely proposed (e.g., [4, 31, 47]). For example, August and Tunca [6] analyze the impact of different liability policies on software vulnerability and derive the conditions under which loss liability and patch liability can be effective. They found that patch liability is an effective policy when the software vulnerabilities are not exploited by the attackers immediately.[3] We extend this stream of work by considering how liability should be provided in the presence of system interdependency risks.

A small stream of research has highlighted the importance of system interdependency risks. Kunreuther and Heal [33] examine firms' optimal decisions regarding security investment when their risks are interdependent. When the number of firms increases, firms have more incentive to underinvest in security. Varian [54] suggests that such behavior is a type of free-riding, much like that observed in the provision of public goods. Yue et al. [59] examine the decisions on how a firm should distribute its security resources between system-specific versus general security protections. Although general protections may curb external attacks, system-specific protections alleviate the threat of system interdependency risks. August and Tunca [5] model interdependency risk arising on the user side due to unpatched software. They discuss the impact of policies such as mandatory patching, patching rebate, and usage tax in managing security risks. In our problem, we restrict system interdependency risks to only clients who are outsourcing to the MSSP (because then they share the same security platform) and analyze how the clientele and quality decisions of the MSSP affect the overall risks of the clients and social welfare.

There is also a growing literature on policy and mechanism design in information security. Ghose and Rajan [23] consider the economic effect of regulatory information disclosure on firms' security investment, whereby mandatory security disclosure could motivate firms to make optimal production decisions. Lee et al. [34] consider the impact of security standardization when such initiatives can only partially cover the overall security effort in an organization. While security standardization could be done only under verifiable control, Lee et al. found that such standardization could lead to suboptimal results with unverifiable control. Our model also considers a mandatory security requirement (also known as "standardization"), but in a setting whereby shirking of responsibility is possible on both the MSSP's and the client's side.

Basic Model

We start with a simple model and extend it to include other important features of security outsourcing such as system interdependency, strategic hacking, and competition in later sections. Our basic model encompasses the following assumptions:

Assumption 1: There is one client ("she") and one MSSP ("he"). The client values her system at v.

Assumption 2: A hacker ("it") attacks the client's system with probability $a \in [0, 1]$.

Assumption 3: The SLA between the client and the MSSP includes a compensation term ("liability"), $\beta \in [0, 1]$. If the client suffers a loss of v because of the hacker's attack, then the MSSP has to compensate her by βv.

Assumption 4: The client's cost of developing security protection is an increasing convex function, $(1/2)c_k q^2$, where c_k is a cost coefficient and q denotes the security quality, which represents the probability *that the client's system can deter the hacker's attack. The corresponding cost for the MSSP is $(1/2)c_s q^2$, where $c_s < c_k$.*

Assumption 5: v, c_k, c_s, and a are public information.

Assumption 6: $av \le c_s$.

Assumption 6 ensures that the analysis will not arrive at a corner solution. If $av > c_s$, then the expected loss to the client is excessive, to the extent that she will always engage the highest level of security protection, $q = 1$. This case is not interesting, and thus we exclude it from the analysis. Figure 1 presents the game sequence.

If the client did not protect her system, her utility would be $u_0 = (1 - a)v$. If the client developed the protection in-house, her expected utility would be

$$u_k = \left[1 - a\left(1 - q_k\right)\right]v - \frac{1}{2}c_k q_k^2,$$

where q_k denotes the security quality from in-house development.[4] Differentiating u_k with respect to q_k, the optimal security quality, $q_k^* = av/c_k$. By Assumptions 4 and 6, $0 \le q_k^* \le 1$. The utility of the client from in-house development is then

$$u_k^* = \left(1 - a\right)v + \frac{1}{2}\frac{\left(av\right)^2}{c_k}. \tag{1}$$

Since $u_k^* > u_0$, u_k^* is the client's reservation utility.

If the client outsourced the protection, her net utility is

$$u_s = \left[1 - a\left(1 - q_s\right)\right]v + a\beta v\left(1 - q_s\right) - p, \tag{2}$$

where p denotes the price charged by the MSSP and q_s denotes the quality of the MSSP's protection, which is not observable to the client. The second term in Equation (2) is the expected compensation receivable by the client. The MSSP's profit is

$$\pi = p - a\beta v\left(1 - q_s\right) - \frac{1}{2}c_s q_s^2. \tag{3}$$

To induce the client to choose his service, the MSSP has to ensure that the client is no worse off than getting the reservation utility, that is, $u_s \ge u_k^*$. By Equations (1) and (2), we must have

$$p \le avq_s + a\beta v\left(1 - q_s\right) - \frac{1}{2}\frac{\left(av\right)^2}{c_k}.$$

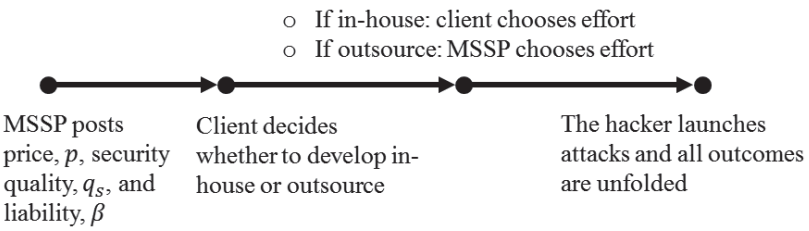

Figure 1. Game Sequence

The MSSP's problem becomes

$$\max_{p,q_s,\beta}\left[p - a\beta v(1-q_s) - \frac{1}{2}c_s q_s^2\right]$$

$$\text{s.t. } p \le avq_s + a\beta v(1-q_s) - \frac{1}{2}\frac{(av)^2}{c_k}.$$

The solution is

$$q_s^* = \frac{av}{c_s},$$

$$p^* = \frac{(av)^2}{c_s} + a\beta^* v\left(1 - \frac{av}{c_s}\right) - \frac{1}{2}\frac{(av)^2}{c_k},$$

and

$$\pi^* = \frac{1}{2}(av)^2\left(\frac{1}{c_s} - \frac{1}{c_k}\right) > 0$$

because $c_k > c_s$. Lemma 1 summarizes these results:

Lemma 1: In equilibrium, the MSSP will set price and liability such that $p^* - a\beta^* v(1-(av/c_s)) = ((av)^2/c_s) - (1/2)((av)^2/c_k)$. *He will exert effort,* $q_s^* = av/c_s$. *The client will use the MSSP's service, and her expected utility will be*

$$u_s^* = (1-a)v + \frac{1}{2}\frac{(av)^2}{c_k}. \tag{4}$$

The MSSP's equilibrium profit is

$$\pi^* = \frac{1}{2}(av)^2\left(\frac{1}{c_s} - \frac{1}{c_k}\right). \tag{5}$$

The proofs of all the results are in the Appendix.

By Equations (1) and (4), $u_s^* = u_k^*$. Because $\pi^* > 0$, the availability of the security service improves social welfare. This is obvious because, by assumption, it is more cost-effective for the MSSP to develop the protection than the client. Further, because

$c_k > c_s$, $q_s^* > q_k^*$, which means that the client is better protected when she uses the MSSP's service.

We now ask: What if the external environment requires the client to attain a minimum level of security? To address this question, we add two assumptions:

Assumption 7: There is a minimum security requirement, $\underline{q}$, $0 \le \underline{q} \le 1$.

Assumption 8: The client must develop up to $\underline{q}$ if she chooses the in-house option. She will not be able to verify the MSSP's effort if she outsources the protection.

Assumptions 7 and 8 apply to settings whereby the mandatory security requirement is enforced by third-party certifications. For example, a firm may deploy internal programmers to develop the ISO 27000 requirements. To complete the certification processes, however, its effort will be subject to controls and audits by the relevant certification bodies. By contrast, if a client outsources her protection to a certified MSSP, she could fulfill her security obligation (despite not being able to verify the MSSP's effort). With Assumption 8, the MSSP could offer a lower level of security quality than that specified in the service contract ("shirk") if it is in his best interest to do so.[5]

To analyze the impact of imposing $\underline{q}$, we need to consider two cases:

Case (i): $\underline{q} \le q_k^* = av/c_k$. The mandatory security requirement is immaterial because it is lower than what the client would choose with in-house development anyway.

Case (ii): $\underline{q} > q_k^*$. The client must develop $\underline{q}$ if she chooses in-house development, and so her new reservation utility becomes

$$\breve{u}_k^* = (1-a)v + av\underline{q} - \frac{1}{2}c_k\underline{q}^2. \tag{6}$$

By Equation (1), $\breve{u}_k^* - u_k^* = -(1/2)c_k(\underline{q} - (av/c_k))^2 < 0$, that is, a high mandatory security requirement decreases the reservation utility that the client could obtain from in-house development.[6]

In case (ii), to attract the client, the MSSP must ensure that the client gets at least her (new) reservation utility, $\breve{u}_k^*$. By Equations (2) and (6), the constraint on price and liability becomes $p \le av(q_s - \underline{q}) + a\beta v(1 - q_s) + (1/2)c_k\underline{q}^2$. Following a similar analysis as leading to Lemma 1, our first proposition follows:

Proposition 1: When there is a mandatory security requirement, $\underline{q}$:

(a) If $\underline{q} \le av/c_k$, the results in Lemma 1 apply. The MSSP will supply the security quality stated in the service contract, $q_s^* = av/c_s$.

(b) If $\underline{q} > av/c_k$, the MSSP will supply $\breve{q}_s^* = av/c_s$ and set price and liability such that

$$\breve{p}^* - a\breve{\beta}^* v\left(1 - \frac{av}{c_s}\right) = \frac{(av)^2}{c_s} - av\underline{q} + \frac{1}{2}c_k\underline{q}^2.$$

The client's expected utility is

$$\breve{u}_s^* = (1-a)v + av\underline{q} - \frac{1}{2}c_k\underline{q}^2. \tag{7}$$

The MSSP's equilibrium profit is

$$\breve{\pi}^* = \frac{1}{2}\frac{(av)^2}{c_s} + \frac{1}{2}c_k\underline{q}^2 - av\underline{q}. \tag{8}$$

Further, if $\underline{q} \le av/c_s$, the equilibrium service quality exceeds the mandatory requirement; the MSSP will truthfully supply the quality stated in the service contract. By contrast, if $\underline{q} > av/c_s$, the MSSP will claim to supply $\underline{q}$ when in fact supplying only $\breve{q}_s^* < \underline{q}$. The client knows that the MSSP will shirk but will nevertheless use his service.

By Equations (5) and (8),

$$\breve{\pi}^* - \pi^* = \frac{1}{2}c_k\underline{q}^2 + \frac{1}{2}\frac{(av)^2}{c_k} - av\underline{q} = \frac{1}{2}c_k\left(\underline{q} - \frac{av}{c_k}\right)^2 > 0,$$

and so the MSSP earns a higher profit when $\underline{q}$ is high. By Equations (4) and (7),

$$\breve{u}_s^* - u_s^* = -\frac{1}{2}c_k\left(\underline{q} - \frac{av}{c_k}\right)^2 < 0,$$

and so the client's expected utility decreases. Accordingly, by moving from Lemma 1 to Proposition 1, we see that the mandatory security requirement is immaterial when it is low ($\underline{q} \le av/c_k$), but when it is high ($\underline{q} > av/c_k$), it facilitates the earning of a higher profit by the MSSP. The mandatory security requirement *will not* change the equilibrium service quality, which is always av/c_s whether $\underline{q}$ is imposed or not. Figures 2 and 3 plot how the client's utility and MSSP's profit vary with $\underline{q}$.[7]

Further, by Equations (4) and (7), $du_s^*/da = -v(1 - (av/c_k)) < 0$ and $d\breve{u}_s^*/da = -v(1 - \underline{q}) < 0$, and so the client always prefers the attack probability, a, to be small. By contrast, by Equations (5) and (8), $d\pi^*/da = av^2(1/c_s - 1/c_k) > 0$ and $d\breve{\pi}^*/da = v((av/c_s) - \underline{q}) < 0$ if and only if $\underline{q} > av/c_s$. So, the MSSP actually prefers the attack probability to *increase* when there is no mandatory security requirement or when the mandatory security requirement is low.

When $\underline{q}$ is immaterial (i.e., Proposition 1a), the MSSP makes a profit mostly from his superior cost efficiency relative to the client, the scale of which increases as the threat from the hacker, a, increases. On the other hand, if $\underline{q} > av/c_s$ is high, by rearranging Equation (8), we have

$$\breve{\pi}^* = \frac{1}{2}(av)^2\left(\frac{1}{c_s} - \frac{1}{c_k}\right) + \frac{1}{2}c_k\left(\underline{q} - \frac{av}{c_k}\right)^2.$$

The first term is identical to π^* in Equation (5) and represents the MSSP's profit due to his superior cost efficiency, which increases in a. The second term is the supranormal

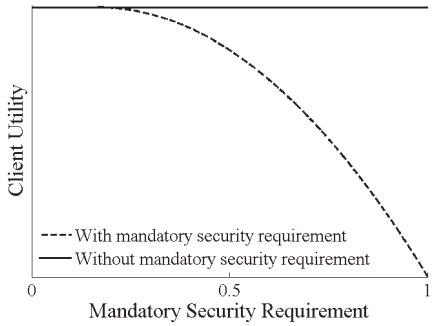

Figure 2. Client Utility

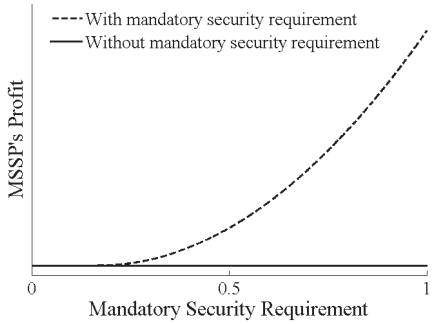

Figure 3. MSSP's Profit

profit due to the fact that the MSSP could shirk but not the client. As a increases, the client would prefer a higher level of security protection, and so the gap between $\underline{q}$ and av/c_k (the security level that the client would choose with in-house development) decreases, which implies that the second term decreases in a. Whether $\breve{\pi}^*$ increases or decreases in a then depends on the balance of these two terms. When $\underline{q} > av/c_s$, the second term prevails. The MSSP would prefer the attack probability to *decrease.*

The condition $\underline{q} > av/c_s$ in Proposition 1b corresponds to a situation where the client deliberately shifts the compliance responsibility to the MSSP by security outsourcing. The client knows that the MSSP will shirk and underprovide security quality relative to the mandatory security requirement, $\underline{q}$, but she is willing to pay for his service because she knows that her threat from a hacker attack is not high enough to justify developing $\underline{q}$ internally. In other words, the client simply pays others to help her satisfy the mandated requirement. As is clear from Lemma 1 and Proposition 1, $u_s^* + \pi^* = \breve{u}_s^* + \breve{\pi}^*$. So, the mandatory security requirement does not affect social welfare.

Finally, the model presented here can be easily generalized to n clients if the clients are homogeneous and independent, the MSSP's cost of serving multiple clients exhibits constant economies of scale, and there is no resource constraint. The independence assumption ensures that the MSSP's optimization problem is separable among the n clients. The homogeneity and the lack of resource constraint assumptions ensure that

the MSSP will offer the same contract to all the clients. Then, Lemma 1 and Proposition 1 can be extended directly; the MSSP's profit is simply the sum of the profit gained from serving each of the n clients.

Multiple Interdependent Clients

In a networked economy, computer systems are interdependent [33]. A compromise in one part of a network can spill over to other computers in the same network. For example, a successful attack at one client's system may cause the MSSP to halt his entire network to ensure that the problem does not propagate. Other clients may also need to check their log files to ensure that there has not been any unauthorized access/damage to their data. To capture this negative spillover, we modify Assumptions 1, 2, 3, and 4:

Assumption 1′: There are n clients and one MSSP. Each client values her system at v. The clients' systems become interdependent if they outsource to the MSSP. If one client's system is compromised, then each of the other MSSP's clients will incur a loss of ev, where e is a small constant.[8]

Assumption 2′: A hacker will attack A out of the n clients, where $0 \le A \le n$. *The A attacks are independent and uniformly distributed among the n clients. Hence, the probability for each client to be attacked is* $a = A/n$, $0 \le a \le 1$.

Assumption 3′: The SLA between the clients and the MSSP includes a compensation term ("liability"), $\beta \in [0, 1]$. *A client whose system is directly compromised ("hacked") will receive a compensation of* βv. *Each of the other MSSP's clients who indirectly suffer harm due to system interdependency will receive* βev.

Assumption 4′: Each client's cost of developing security protection is an increasing convex function, $(1/2)c_k q^2$. *The corresponding cost for the MSSP is* $(1/2)c_s q^2$, $c_s < c_k$. *The MSSP incurs a separate cost to protect each client.*[9]

As before, a client's expected utility from in-house development is given by Equation (1). Due to the system interdependency, the MSSP may choose not to serve all n clients. Let there be $m \le n$ clients using the MSSP's service.[10] Suppose that client j, $j = 1, ..., m$, outsourced her protection to the MSSP. Her expected utility is

$$u_{s,j} = \left(1 - L_j\right)v + L_j \beta_j v - p_j, \tag{9}$$

where

$$L_j \equiv a\left(1 - q_{s,j}\right) + e\left[\frac{a(na-1)\sum_{i=1,i\neq j}^{m}\left(1-q_{s,i}\right)}{n-1} + \frac{(1-a)(na)\sum_{i=1,i\neq j}^{m}\left(1-q_{s,i}\right)}{n-1}\right]$$

$$= a\left(1 - q_{s,j}\right) + ea\sum_{i=1,i\neq j}^{m}\left(1-q_{s,i}\right)$$

denotes the expected loss of client j. The first term in L_j is the probability that the hacker directly and successfully hacked client j's system. The second term in L_j is

the expected number of security breaches among the other $m - 1$ MSSP's clients, multiplied by the spillover (externality) factor, e.[11]

Given m clients, the MSSP's total profit would be

$$\pi = \sum_{j=1}^{m}\left(p_j - L_j\beta_j v - \frac{1}{2}c_s q_{s,j}^2\right). \tag{10}$$

To attract the clients to use his service, the prices and liabilities have to satisfy $u_{s,j} \geq u_k^*$, that is,

$$p_j \leq \left(a - L_j\right)v + L_j\beta_j v - \frac{1}{2}\frac{(av)^2}{c_k}.$$

The MSSP's problem then becomes

$$\max_{p_j, q_{s,j}, \beta_j, m} \sum_{j=1}^{m}\left(p_j - L_j\beta_j v - \frac{1}{2}c_s q_{s,j}^2\right)$$

$$\text{s.t. } p_j \leq \left(a - L_j\right)v + L_j\beta_j v - \frac{1}{2}\frac{(av)^2}{c_k} \quad \forall\, j = 1,\ldots,m.$$

The following lemma characterizes the solution to this problem:

Lemma 2: In equilibrium, the MSSP will set price and liability such that

$$p_j^* - Ta\beta_j^* v\left(1 - \frac{Tav}{c_s}\right) = \frac{(Tav)^2}{c_s} - \frac{1}{2}\frac{(av)^2}{c_k} - av(T-1), \quad j = 1,\ldots,m^*,$$

where $T \equiv 1 + e(m^* - 1)$. He will exert the same effort, $q_s^* = Tav/c_s$, for all the clients, where m^* and q_s^* solve

$$m^* = \frac{1}{2} + \frac{avq_s^* - \frac{1}{2}c_s\left(q_s^*\right)^2 - \frac{1}{2}\frac{(av)^2}{c_k}}{2eav\left(1 - q_s^*\right)} \tag{11}$$

and

$$q_s^* = \frac{av}{c_s}\left[1 + e\left(m^* - 1\right)\right]. \tag{12}$$

m^* clients will outsource. Their expected utility is the same as in Equation (4), that is, $u_s^* = (1 - a)v + (1/2)((av)^2/c_k)$. The other $n - m^*$ clients will stay out but obtain the same utility as the m^* clients of the MSSP, that is, $u_k^* = u_s^*$. The MSSP's equilibrium profit is

$$\pi^* = m^*\left[\frac{1}{2}\frac{(Tav)^2}{c_s} - \frac{1}{2}\frac{(av)^2}{c_k} - av(T-1)\right]. \tag{13}$$

Comparing Lemma 2 with Lemma 1, with system interdependency, the clients' utility does not change but the MSSP earns a lower profit per client. System interdependency increases the threat faced by the MSSP's clients. In order to attract the clients, the MSSP has to ensure that they get at least the in-house development reservation utility, u_k^*. So, the MSSP has to internalize the losses arising from system interdependency, which can be achieved by compensating clients whose systems are not directly hacked for harms that they suffer due to spillovers from others.

Further, because the MSSP has to internalize the expected losses due to system interdependency, he will raise the quality of security protection for his clients. Ironically, despite the fact that system interdependency increases the MSSP's clients' threats, it also enhances their protection against *direct hacking*. The MSSP's clients may suffer from others' security breaches, but their own systems will be less likely to be directly hacked now.[12]

We next investigate the implications of imposing a mandatory security requirement. With Assumptions 7 and 8, Lemma 2 will continue to hold if $\underline{q} \le q_k^* = av/c_k$. If $\underline{q} > av/c_k$, the clients' reservation utility is again given by Equation (6). The prices and liabilities must satisfy $p_j \le (a - L_j)v + L_j\beta_j v - av\underline{q} + (1/2)c_k\underline{q}^2$. The MSSP's problem becomes

$$\max_{p_j, q_{s,j}, \beta_j, m} \sum_{j=1}^{m} \left(p_j - L_j\beta_j v - \frac{1}{2}c_s q_{s,j}^2 \right),$$

$$\text{s.t. } p_j \le \left(a - L_j\right)v + L_j\beta_j v - av\underline{q} + \frac{1}{2}c_k\underline{q}^2 \ \ \forall\ j = 1,\ldots,m.$$

The procedure to derive the solution to the above problem is similar to that leading to Proposition 1 and Lemma 2. The following proposition characterizes the equilibrium:

Proposition 2: In the presence of system interdependency among the MSSP's clients, when there is a mandatory security requirement, $\underline{q}$:

(a) If $\underline{q} \le av/c_k$, the results in Lemma 2 apply. The MSSP will supply the security quality stated in the service contract, $q_s^* = Tav/c_s$.

(b) If $\underline{q} > av/c_k$, the MSSP will supply $\breve{q}_s^* = \breve{T}av/c_s$ and set price and liability such that

$$\breve{p}_j^* - \breve{T}a\breve{\beta}_j^* v\left(1 - \frac{\breve{T}av}{c_s}\right) = \frac{\left(\breve{T}av\right)^2}{c_s} - av\left(\breve{T} - 1\right) - av\underline{q} + \frac{1}{2}c_k\underline{q}^2, \quad j = 1,\ldots,\breve{m}^*,$$

where $\breve{T} \equiv 1 + e(\breve{m}^* - 1)$, $\breve{m}^*$ and $\breve{q}_s^*$ solve

$$\breve{m}^* = \frac{1}{2} + \frac{av\breve{q}_s^* - \frac{1}{2}c_s\left(\breve{q}_s^*\right)^2 - av\underline{q} + \frac{1}{2}c_k\underline{q}^2}{2eav\left(1 - \breve{q}_s^*\right)} \tag{14}$$

and

$$\breve{q}_s^* = \frac{av}{c_s}\left[1 + e\left(\breve{m}^* - 1\right)\right]. \tag{15}$$

The utility of the $\breve{m}^*$ clients is the same as in Equation (7), that is, $\breve{u}_s^* = (1-a)v + av\underline{q} - (1/2)c_k\underline{q}^2$. The other $n - \breve{m}^*$ clients will stay out but obtain the same utility as the $\breve{m}^*$ clients of the MSSP, that is, $\breve{u}_k^* = \breve{u}_s^*$. The MSSP's equilibrium profit is

$$\breve{\pi}^* = \breve{m}^*\left[\frac{1}{2}\frac{\left(\breve{T}av\right)^2}{c_s} + \frac{1}{2}c_k\underline{q}^2 - av\underline{q} - av\left(\breve{T} - 1\right)\right]. \tag{16}$$

Similar to the single client case, if $\underline{q} \le \breve{T}av/c_s$, the equilibrium service quality will exceed the mandatory requirement and the MSSP will be truthful. If $\underline{q} > \breve{T}av/c_s$, the MSSP will claim to supply $\underline{q}$ when in fact supplying only $\breve{q}_s^*$. The $\breve{m}^*$ clients again know that the MSSP will shirk, but they will nevertheless use his service.

Here again, if the mandatory security requirement is high ($\underline{q} > av/c_k$), the clients' utility will decrease (see Figure 2) because the cost needed to attain such a high requirement exceeds the threat from the hacker. Unlike the single client case, however, the mandatory security requirement will also change the equilibrium service quality when the MSSP's clients' systems are interdependent, as summarized in the following proposition:

Proposition 3: In the presence of system interdependency among the MSSP's clients, a high mandatory security requirement, $\underline{q} > av/c_k$, will increase the equilibrium security service quality and the number of clients outsourcing to the MSSP. It is more likely for the MSSP to truthfully meet the mandatory security requirement.

Figures 4 and 5 illustrate how the security service quality, $\breve{q}_s^*$, and the number of clients outsourcing to the MSSP, $\breve{m}^*$, vary with $\underline{q}$.

The mandatory security requirement increases the effort needed for in-house development, and so it decreases the clients' bargaining power against the MSSP. The MSSP's profit from serving each client would increase, and so he will serve more clients. This increases the overall risk to the MSSP's network due to system interdependency. To ensure that the compensation for security breaches is not excessive, the MSSP will increase his security protection efforts. Hence, the mandatory security requirement will cause more clients to suffer indirect harms from others' security breaches ($\breve{m}^* > m^*$), but it will reduce the probability of their systems being directly hacked ($\breve{q}^* > q^*$). Interestingly, the mandatory security requirement makes the MSSP work harder not because he has an incentive to fulfill the requirement, but because it increases his liability by sending him more clients.

By Proposition 2, the clients who outsource to the MSSP may be variously better or less well protected relative to $\underline{q}$. Although a high $\underline{q}$ increases the protection of some clients (and more clients) against direct hacking ($\breve{q}_s^*$ and $\breve{m}^*$ increase when $\underline{q} > av/c_k$), it decreases the expected net utility of *all* clients. From the MSSP's clients' perspective, the gain from the MSSP's protection is offset by the additional threat from the negative

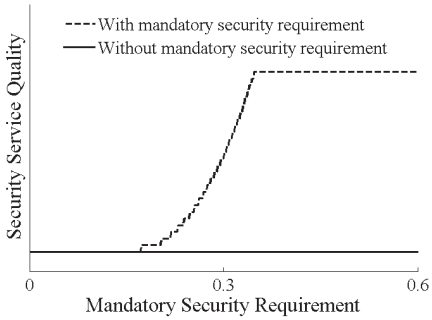

Figure 4. Security Service Quality

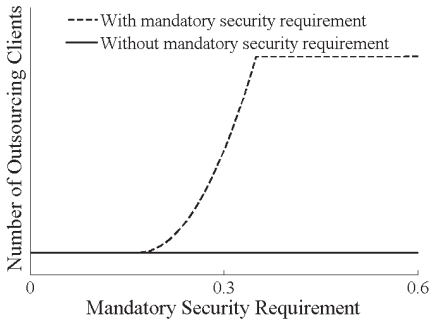

Figure 5. Number of Outsourcing Clients

spillovers arising from joining an interdependent system. The next proposition shows that such a high mandatory security requirement decreases social welfare too:[13]

> *Proposition 4: A high mandatory security requirement, $\underline{q} > av/c_k$, decreases social welfare when the MSSP's clients are interdependent.*

Figure 6 illustrates how the social welfare varies with $\underline{q}$. When $\underline{q} > av/c_k$, by Proposition 2, $n - \breve{m}^*$ clients will not be able to outsource and so the high mandatory security requirement would force them to spend more in-house effort. Such extra efforts are socially excessive. Further, by Proposition 3, the high mandatory security requirement would motivate the MSSP to serve more clients. Although more clients can now enjoy the MSSP's superior cost efficiency, they also increase the size of the MSSP's network and so increase the system interdependency risks to *all outsourcing clients.* The MSSP must work harder to protect his clients. This increases the MSSP's cost and so decreases social welfare as well.

Intuitively, one might think that a high mandatory security requirement should enhance social welfare because it induces the clients and the MSSP to work harder. Propositions 2 and 4, however, indicate otherwise: if the mandatory security requirement is low, it will not affect the equilibrium behaviors; if it is high, then it will expand the MSSP's clientele, which increases the system interdependency risk and

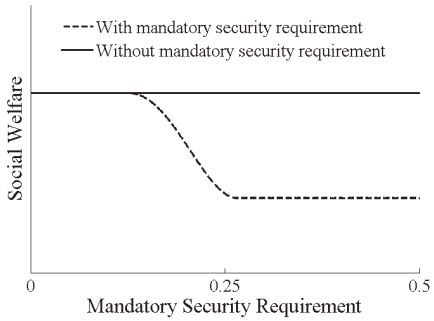

Figure 6. Equilibrium Social Welfare

causes wastage in protection efforts. Such a high mandatory security requirement is *welfare reducing.*

Proposition 4 further characterizes the *negative* interaction between system interdependency and the mandatory security requirement. By the analysis of the basic model, specifically, Lemma 1 and Proposition 1, without system interdependency, the MSSP will always serve all the clients by supplying the same quality of service. Imposing a mandatory security requirement will only affect the payment from the clients to the MSSP, and it will not affect the equilibrium outcomes. However, when the MSSP's network exhibits system interdependency, the threat from the hacker to his clients will be amplified. To limit the expected losses of his clients (and to maximize his price), the MSSP will restrict his "output" (i.e., serve fewer clients), which tends to decrease the harm due to spillovers of security breaches. Imposing a high mandatory security requirement, however, will provide a wrong incentive—it encourages the MSSP to serve more clients, which increases the system interdependency risks. The MSSP then has to work harder to address such risks, therefore social welfare decreases. Accordingly, if system interdependency is prevalent (e.g., when an MSSP uses a common set of technology or platform to serve all the clients), imposing a high security requirement is generally not advised.[14]

Verifiability

So far our analysis has assumed that the clients cannot verify the MSSP's protection efforts. Prior studies have shown that verifiability plays an instrumental role in facilitating efficient service quality and social welfare [19]. We now investigate if a mandatory security requirement would affect this conclusion. In particular, if the clients can verify the MSSP's effort, then the MSSP will not be able to shirk and must supply the quality of service specified in the service contract. We modify Assumption 8 as follows:

> *Assumption 8′: The client must invest up to $\underline{q}$ if she develops the protection in-house. The client can verify the MSSP's effort if she outsources the protection.*

Referring to Proposition 2b, when the mandatory security requirement, $\underline{q} \leq \check{T}av/c_s$, the MSSP will always truthfully supply the optimal service quality, and so verifiability has no impact on the equilibrium outcome. When $\underline{q} > \check{T}av/c_s$ and the MSSP *cannot* shirk, he must now supply $\check{q}_s^* = \underline{q}$ instead of $\check{T}av/c_s$. Perhaps not surprisingly, the inability of the MSSP to choose an optimal $\check{q}_s^*$ implies a reduction in profit as well as social welfare. The next proposition summarizes the outcome of this scenario:

> *Proposition 5: With verifiability, if $\underline{q} \leq \check{T}av/c_s$, the results in Proposition 2 apply; imposing verifiability does not affect the equilibrium outcomes. If, however, $\underline{q} > \check{T}av/c_s$, then in the equilibrium with verifiability, the MSSP's profit and social welfare will decrease, but his clients will be better protected against direct hacking.*

Without verifiability, when $\underline{q} > \check{T}av/c_s$, by Proposition 2, the MSSP will shirk by supplying a lower quality service, $\check{q}_s^* = \check{T}av/c_s$. This decreases the MSSP's costs and so increases his profit. With verifiability, the MSSP could no longer exploit his clients by shirking. Instead, the MSSP must diligently supply $\underline{q}$, which increases his cost and erodes his profit. The MSSP's effort will be socially excessive because the threat faced by the clients does not call for $\check{q}_s^* = \underline{q}$. Accordingly, imposing verifiability would cause the MSSP to work *too hard,* which decreases social welfare.

Hence, from a social welfare perspective, it is not advisable for the clients to verify or audit the MSSP's effort. Shirking *could be good* for the society when the security risk is low and when the clients are mandated to have a higher level of security protection. Figure 7 summarizes the equilibrium outcomes with/without verifiability under different mandatory security requirements. The shaded areas correspond to the setting with social welfare losses. Figure 8 plots the social welfare outcomes. It is clear that only our main configuration, without verifiability, would achieve the social optimum for all levels of $\underline{q}$.[15]

Because of asymmetric information, clients often cannot ascertain whether the MSSP will work hard. To address such uncertainty, an increasingly popular practice is to engage security service auditing [39]. Our analysis shows that such auditing may in fact decrease social welfare when there exists a high mandatory security requirement.

We conclude this section by stating the impact if the MSSP cannot commit to compensating the clients in the event of security breaches. Without the compensation, the MSSP will always shirk after the clients have decided to outsource the protection to him. The clients rationally expect this, and so in most cases they would rather choose to develop the security protection in-house. Nevertheless, when the mandatory security requirement is excessively high, the clients may find that it is cheaper to engage the MSSP to satisfy the requirement. Hence, the clients may even be willing to pay the MSSP despite knowing that he will not work hard to protect them. Overall, the social welfare always *decreases* when the MSSP cannot commit to compensate his clients. Hence, in information security outsourcing, liability (e.g., by including damage-tied compensation terms in the SLA) may play a more important role than auditing.

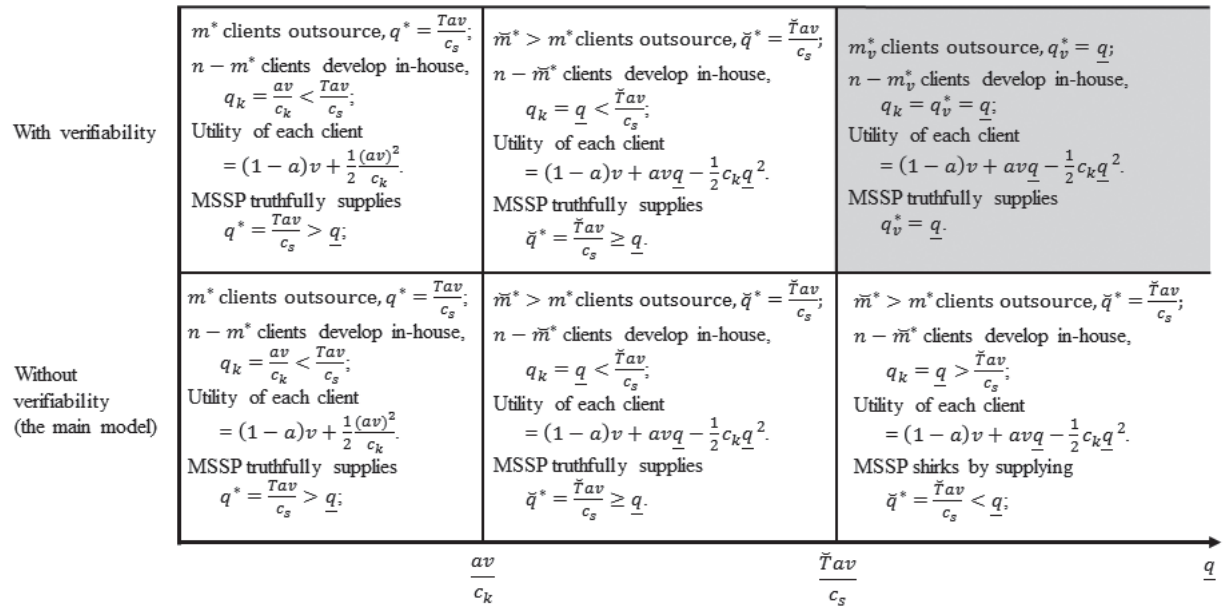

Figure 7. Equilibrium Outcomes

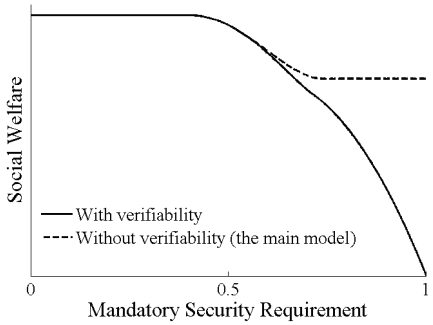

Figure 8. Social Welfare with Different Contracting Instruments

Extensions

We assess the robustness of our findings by relaxing several assumptions in the above analysis. For each of the following extensions we use the model with system interdependency, e, and mandatory security requirement, $\underline{q}$, as the benchmark.

Heterogeneous Clients

We first consider the case with heterogeneous clients. Specifically, we modify Assumptions 1′ and 5 as follows:

> *Assumption 1″: There are n_1 high-type and n_0 low-type clients, and one MSSP. The high types value their system at v_1. The low types value their system at $v_0 < v_1$. The clients' systems become interdependent if they use the MSSP's service. If one client's system is compromised, then each of the other MSSP's clients will incur a loss of ev_t, $t = 0, 1$, where e is an arbitrarily small constant.*
>
> *Assumption 5′: v_0, v_1, c_k, c_s, and a are public information. Further, the MSSP can accurately diagnose and separate the high-type and low-type clients.*

Assumption 5′ ensures that the MSSP could assess the reservation utility of the clients, so he does not need to practice indirect price discrimination (e.g., segmenting the clients with incomplete information about their valuations) [41]. Considering indirect price discrimination will complicate the analysis without giving much insight into the influence of a mandatory security requirement. In any case, the MSSP often needs to conduct on-site preassessments before committing to serving the clients.[16] So, it is reasonable to assume that the MSSP knows the clients' values.

Similar to the analysis in the previous section, if client type t, $t = 0, 1$, developed the security protection in-house, her net utility would be $u_{k,t} = (1 - a)v_t + (1/2)((av_t)^2/c_k)$ if $\underline{q} < av_t/c_k$ and $u_{k,t} = (1 - a)v_t + av_t\underline{q} - (1/2)c_k\underline{q}^2$ otherwise. Suppose that in equilibrium the MSSP would serve m_1 high-type and m_0 low-type clients. Then, if client j of type t outsources the protection to the MSSP, her expected net utility would be

$$u_{s,t,j} = \left(1 - L_{t,j}\right) v_t + L_{t,j}\beta_{t,j} v_t - p_{t,j},$$

where

$$L_{t,j} \equiv a\left(1 - q_{s,t,j}\right) + ea\sum_{i=1, i\neq j}^{m_t}\left(1 - q_{s,t,i}\right) + ea\sum_{i=1}^{m_{1-t}}\left(1 - q_{s,1-t,i}\right).$$

For the clients to outsource to the MSSP, we must have $u_{s,t,j} \geq u_{k,t}$, that is, $p_{t,j} \leq (1 - L_{t,j})v_t + L_{t,j}\beta_{t,j}v_t - u_{k,t}$. The MSSP's problem becomes

$$\max_{p_{t,j}, q_{s,t,j}, \beta_{t,j}, m_t} \sum_{t=0,1}\sum_{j=1}^{m_t}\left(p_{t,j} - L_{t,j}\beta_{t,j}v_t - \frac{1}{2}c_s q_{s,t,j}^2\right)$$

$$\text{s.t. } p_{t,j} \leq \left(1 - L_{t,j}\right)v_t + L_{t,j}\beta_{t,j}v_t - u_{k,t} \quad \forall\ t = 0,1 \text{ and } j = 1,\ldots,m_t.$$

It is straightforward to show that, in equilibrium,

$$q_{s,t,j}^* = q_{s,t}^* = \frac{a\left[1 + e\left(m_t^* - 1\right)\right]v_t + eam_{1-t}^* v_{1-t}}{c_s} \tag{17}$$

and

$$m_t^* = \frac{1}{2} + \frac{\left(1-a\right)v_t + av_t q_{s,t}^* - u_{k,t} - \frac{1}{2}c_s\left(q_{s,t}^*\right)^2}{2eav_t\left(1 - q_{s,t}^*\right)} - \frac{m_{1-t}^*}{2}\left(\frac{v_{1-t}}{v_t} + \frac{1 - q_{s,1-t}^*}{1 - q_{s,t}^*}\right), \tag{18}$$

$t = 0, 1$. Hence, the two types of clients will receive a different quality of service. Similar to the case with homogeneous clients, the MSSP's clients will receive better protection against direct hacking because the MSSP will work extra hard to internalize the losses that arise from system interdependency. By Equation (17), the MSSP's extra effort is a function of the number of each type of clients that he serves, weighted by their valuations for their systems, v_t. Further, by Equation (18), the two types of clients are substitutes for the MSSP; if he serves more type t clients, then he will serve fewer $1 - t$ type clients.

Note that Equations (17) and (18) are direct generalizations of the solutions in Lemma 2 and Proposition 2, and so our basic conclusions remain unchanged. If the mandatory security requirement is sufficiently high to the extent that $\underline{q} > av_1/c_k$, then both m_0^* and m_1^* will increase, that is, the MSSP will serve *more* clients of both types. By Equation (17), the service quality, $q_{s,t}^*$, is a positive function of m_0^* and m_1^*, and so it will unambiguously *increase too.*[17]

Because a high security requirement, $\underline{q} > av_1/c_k$, would motivate the MSSP to serve more clients, which is the key reason driving the expected social losses arising from spillovers, and hence, the results in Proposition 4, the incorporation of client heterogeneity will not change our conclusions. A high mandatory security requirement will decrease social welfare, particularly with system interdependency.

Competition

We next explore the consequence of introducing competition. We modify Assumption 1′ by allowing for z identical MSSPs in the market and keep all the other assumptions. We use the Bertrand–Nash equilibrium concept.

Suppose that z is sufficiently large to the extent of perfect competition. Then, the MSSPs must price their service at marginal cost [19] and therefore earn zero profit. In this case, the MSSPs will not be able to exploit their clients even when there is a high mandatory security requirement. Accordingly, for each MSSP, $\pi = p_j - L_j\beta_j v - (1/2)c_s q_{sj}^2 = 0$, and so $p_j - L_j\beta_j v = (1/2)c_s q_{sj}^2$. Substituting p_j into Equation (9) and maximizing, all MSSPs will choose $q_c^* = (av/c_s)[1 + e(m_c^* - 1)]$. Since the expected loss due to system interdependency increases in m, without other sources of heterogeneity, we will have the same $m_c^* = n/z$ among all z MSSPs.[18] All the clients will outsource their security protection. Social welfare will be maximized.

Next, if the market is an oligopoly with only a few MSSPs to the extent that $z\check{m}^* \le n$, then the results in Proposition 2 apply. Each MSSP will serve an "island" of $\check{m}^*$ clients. The MSSPs will fully exploit the pricing power granted to them by a high mandatory security requirement, and so they will serve *too many* clients, which escalates the system interdependency risks. Relative to the case with one MSSP, social welfare will increase because more MSSPs could make a profit. But it will still be lower than that in perfect competition because some excluded clients will work too hard, whereas the outsourcing clients will face excessive risks of system spillovers.

Finally, if $z\check{m}^* > n$ but the competition is not keen enough (i.e., z is not so large) to drive the MSSPs' price down to marginal cost, then the equilibrium may feature mixed strategies over m, p (and so β), and q, and all the clients will outsource to the MSSPs. We leave the exploration of such a mixed strategy equilibrium to future research. Nevertheless, as long as the MSSPs cannot fully exploit their pricing power, the social welfare in this scenario should lie between the perfect competition and the oligopoly cases. Overall, competition tends to weaken the (negative) social welfare impact of a high mandatory security requirement, but it may not completely undo the "damage" of such a requirement.[19]

Strategic Hacking

We now endogenize the hacker's choice of attack coverage, A [11, 15, 35, 42]. We follow the structure in Hausken [26] and Png and Wang [42] and modify Assumption 2′ as follows:

> *Assumption 2″: A hacker attacks A out of the n clients, $0 \le A \le n$. The total cost of attacking A clients is an increasing convex function, $(1/2)c_h A^2$, where c_h is an arbitrary cost coefficient. The hacker obtains a benefit, b, from each successful attack. The A attacks are independent and uniformly distributed among the n clients. Hence, the probability of each client being attacked, $a = A/n$, $0 \le a \le 1$. The hacker moves simultaneously with the clients and the MSSP.*

We separate the analysis into two cases:

Case (i): $\underline{q} \le av/c_k$. The equilibrium choices of the clients and MSSP follow Lemma 2. The hacker's utility function becomes

$$\begin{aligned} u_h &= b\left[A\left(\frac{m}{n}\right)\left(1-q_s\right)+A\left(\frac{n-m}{n}\right)\left(1-q_k\right)\right]-\frac{1}{2}c_hA^2 \\ &= Ab\left[\left(1-q_k\right)-\frac{m}{n}\left(q_s-q_k\right)\right]-\frac{1}{2}c_hA^2. \end{aligned} \tag{19}$$

The first term in Equation (19) is the expected number of clients, including those who are variously using/not using the MSSP's service, whose systems were successfully compromised by the hacker, multiplied by the hacker's benefit, b. The second term is the hacker's cost of launching the A attacks. Differentiating with respect to A,

$$A^* = \frac{b}{c_h}\left[\left(1-q_k\right)-\frac{m}{n}\left(q_s-q_k\right)\right]. \tag{20}$$

Together with Equations (11) and (12), and $q_k^* = av/c_k$, we could solve for the equilibrium m^*, q_s^*, q_k^*, and $a^* = A^*/n$. Note that since the equilibrium a^* is endogenous, the constraint $\underline{q} \le av/c_k$ is no longer absolute but depends on the strategic actions of the hacker, the MSSP, and the clients.

Case (ii): $\underline{q} > av/c_k$. The equilibrium choices of the clients and MSSP follow Proposition 2b. The hacker's utility function is

$$u_h = Ab\left[\left(1-\underline{q}\right)-\frac{m}{n}\left(q_s-\underline{q}\right)\right]-\frac{1}{2}c_hA^2. \tag{21}$$

Differentiating with respect to A, we have

$$\breve{A}^* = \frac{b}{c_h}\left[\left(1-\underline{q}\right)-\frac{m}{n}\left(q_s-\underline{q}\right)\right]. \tag{22}$$

Together with Equations (14) and (15), we could solve for the equilibrium, $\breve{m}^*$, $\breve{q}_s^*$, $\breve{q}_k^*$, and $\breve{a}^* = \breve{A}^*/n$.

The explicit solutions to the above problems are intractable. However, from the implicit functions, we could draw the following conclusions:[20]

a. $\partial A^*/\partial q_s < 0$, $\partial \breve{A}^*/\partial q_s < 0$, $\partial A^*/\partial q_k < 0$, and $\partial \breve{A}^*/\partial q_k = 0$. So, the hacker's attack would generally decrease with the clients' and MSSP's protection efforts.
b. $\partial A^*/\partial m < 0$ and $\partial \breve{A}^*/\partial m < 0$ if and only if $q_s \ge \underline{q}$. In other words, the likelihood of the hacker's attack decreases with the size of the clientele of the MSSP only if the MSSP works hard. If the MSSP shirks by undersupplying quality relative to $\underline{q}$, the hacker would actually tend to launch more attacks as *more* clients outsource to the MSSP.

c. When $\underline{q} \leq av/c_k$, that is, the mandatory security requirement is not binding, $(\partial/\partial A)(\partial u_k/\partial q_k) > 0$ and $(\partial/\partial A)(\partial \pi/\partial q_s) > 0$. In other words, the MSSP's and the clients' efforts increase with the hacker's attack. The sign of $(\partial/\partial A)(\partial \pi/\partial m)$ is, however, ambiguous.
d. When $\underline{q} > av/c_k$, that is, the mandatory security requirement is binding, $(\partial/\partial A)(\partial \breve{u}_k/\partial q_k) = 0$ and $(\partial/\partial A)(\partial \breve{\pi}/\partial q_s) > 0$. The clients who are not outsourcing will not be affected by a marginal change in A because they have to choose $\underline{q}$ anyway. The MSSP's effort increases with the hacker's attack. Further, $(\partial/\partial A)(\partial \breve{\pi}/\partial m) > 0$. Therefore, the number of clients served by the MSSP also increases with the hacker's attack.
e. When $\underline{q} > av/c_k$, $\partial \breve{A}^*/\partial \underline{q} < 0$. That is, if the mandatory security requirement is binding, further increasing it could indeed *decrease* the hacker's attack.

The effect characterized in (e) tends to counteract the welfare-reducing effect of $\underline{q}$ in Proposition 4. A high mandatory security requirement may decrease social welfare because of the strategic responses of the MSSP and of the clients to deploy excessive protections. These strategic behaviors, however, do decrease the success rate of attacks, and hence will dissuade the hacker from launching more attacks, which may increase social welfare. The net effect of such a high $\underline{q}$ on social welfare is ambiguous.

However, the above analysis rests on the assumption that the hacker can choose to attack any number of clients. What if the hacker faces a binding resource constraint (e.g., time taken to study the clients' systems and network configurations) so that there is an upper limit of number of clients that it can attack, $\overline{A}$, $A \leq \overline{A} \ll n$? If $\overline{A}$ is binding, then the hacker's strategic responses in Equations (20) and (22) become irrelevant. It will always choose the maximum attack intensity, $\overline{A}$. The welfare-enhancing effect of a reduced A due to the MSSP's and the clients' strategic responses to the mandatory security requirement, $\underline{q}$, that we characterized in (e) above will become moot. Then, obviously, Proposition 4 applies. Imposing a high $\underline{q}$ will decrease social welfare particularly when the MSSP's clients' systems are interdependent. A high mandatory security requirement *may* enhance social welfare only when the hacker has slack resources.[21]

Finally, what if the hacker is thrill-seeking in the sense that it attacks the clients' systems for pleasure, and it responds by *more* attacks if the defense put up at the MSSP's/clients' side is stronger [26]? In this case, A^* would increase with q_s^* and q_k^*, or $\breve{q}_s^*$ and $\breve{q}_k^*$, which would obviously decrease social welfare. It will be undesirable to impose a high mandatory security requirement, $\underline{q}$, in the presence of such a hacker.

Shirking Clients

We have assumed that the MSSP can shirk but the clients cannot. What if it is the opposite, that is, the clients can shirk but the MSSP cannot? Obviously, if $\underline{q} \leq av/c_k$, then Lemma 2 applies because $\underline{q}$ is not binding. The MSSP will supply the optimal service quality, $q_s^* = Tav/c_s > av/c_k \geq \underline{q}$. If $\underline{q} > av/c_k$ and the clients can shirk, then the clients will simply ignore the mandatory security requirement. So, by Equation (1), their

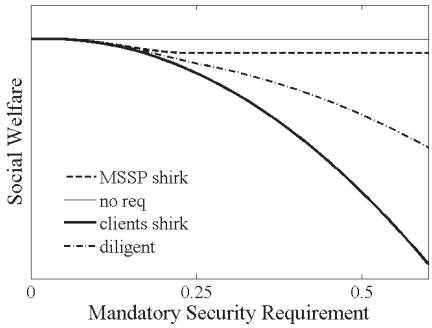

Figure 9. Comparison of Social Welfare

reservation utility becomes $u_k^* = (1-a)v + (1/2)((av)^2/c_k)$ for *all* levels of $\underline{q}$, and by Equations (1) and (9), the pricing constraint is always $p_j \le (a - L_j)v + L_j\beta_j v - (1/2)((av)^2/c_k)$. Accordingly, Lemma 2 will also apply for all $av/c_k < \underline{q} \le Tav/c_s$.

Next, if $\underline{q} > Tav/c_s$, that is, the mandatory security requirement exceeds what the MSSP will supply voluntarily, then the situation is similar to the setting with verifiability (where the MSSP must also work hard), except that the MSSP's price for serving each client is subject to a tighter constraint because the clients now have a higher reservation utility, u_k^*. So, as in Proposition 5, if there is a high mandatory security requirement, $\underline{q} > Tav/c_s$, and the MSSP cannot shirk but the clients can, then the MSSP's profit and social welfare will decrease.

Finally, if we allow both the MSSP and the clients to shirk, then the mandatory security requirement is immaterial. The results in Lemma 2 apply directly.

In fact, our analysis can be conceptually organized as follows: the basic setting with no mandatory security requirement (denote that setting as "no req") gives rise to Lemma 2, which also gives the first-best social welfare. Proposition 2 builds on "no req" by imposing $\underline{q}$ and allowing the MSSP to shirk (denote it as "MSSP shirk"). The analysis of verifiability (Proposition 5) builds on "MSSP shirk" by removing the shirking option from the MSSP (denote it as "diligent"). The analysis here also builds on "MSSP shirk" by removing the shirking option from the MSSP and giving it to the clients (denote this setting as "clients shirk"). Then, Proposition 4 states that the social welfare in "no req" ≥ that in "MSSP shirk." Proposition 5 says that the social welfare in "MSSP shirk" ≥ that in "diligent," and the result in this section indicates that the social welfare in "no req" ≥ that in "clients shirk." Figure 9 shows how the social welfare may vary with $\underline{q}$ in these four scenarios.[22] Clearly, the social welfare is highest if we do not impose a high mandatory security requirement.

Implications

OUR MAIN RESULTS INDICATE THAT WHEN CLIENTS ARE LESS CAPABLE of information security protection, and when they are mandated to enhance their protection, they may outsource

to an MSSP despite knowing that he will shirk and underprovide quality. The benefit of such outsourcing, however, may be offset by the interdependency risks [33] that arise when the MSSP serves multiple clients. With system interdependency, a mandatory security requirement may distort the clients' and the MSSP's equilibrium behaviors and cause undue social welfare losses.

We found that a stringent mandatory security requirement would shift the surplus from clients to the MSSP, which would cause the MSSP to expand his service coverage to more clients. This could be socially detrimental when the clients' systems become interconnected after outsourcing to the MSSP. To some extent, the MSSP's network becomes a "single point of failure"—any security breach of a node may spill over to others.[23] Although the MSSP would exert more effort to protect each of his clients when the size of his network grows, the benefit of such additional efforts will be offset by the increased threat from system spillovers.

There has been a greater call for mandatory security requirements to stem the tide of widespread security concerns. For instance, the Chinese government had proposed that every personal computer (PC) sold in China should be preinstalled with the GDYE software, which was designed to filter content downloaded to the PC. The way GDYE works is similar to antivirus software. Once installed, it will automatically download a list of prohibited sites from an online database and record users' data. However, it has been found that GDYE itself introduces "remotely exploitable vulnerabilities" [57]. It contains programming errors, which "allow malicious sites to steal private data, send spam, or enlist the PC in a botnet" [57]. The proposed requirement was subsequently eliminated for all home computers because of widespread objections.

Another mandatory security initiative proposed by the industry was to apply the public health model to the Internet [14, 44]. The idea is that computing devices should be granted access to the Internet only if consumers can demonstrate that they are "healthy" (i.e., free of viruses, spyware, and other security vulnerabilities). Consumers must use well-accepted protection mechanisms to secure their computing resources. An infrastructure of "health certificates" can be used to notarize the security check. It is further suggested that "access providers and other organizations must have a way to request health certificates and take appropriate action based upon the information provided" [14, p. 6].

Our analysis suggests that these initiatives should be exercised with caution. Although mandatory security requirements such as the GDYE or "certification of inoculation" may force more clients to outsource and thus help realize cost savings and a higher level of protection, it also opens them to interdependency risks. *It is important to recognize system interdependency as a countervailing factor in security outsourcing.*

We also examined the impact of a commonly used measure in information security outsourcing—verifiability [19]. Auditing MSSPs' behaviors (verifiability) has often been regarded as being important for clients. Although verifiability has been found to ensure social efficiency in the contexts of many other credence goods such as medical treatments or mechanical repairs [19], our analysis suggests that we should not impose it in managed security services. The point of departure here is that the "treatment"—a high level of security protection—is mandatory, which will cause excessive protection

and outsourcing. The irony is that verifiability would then remove any room for an MSSP to shirk, which generates socially excessive protection.

Our analysis shows that a carefully examined liability, one that is determined according to the expected risk of the clients, would suffice to motivate the MSSP to serve clients efficiently. Ex post compensations may outperform auditing in facilitating security outsourcing.[24]

Finally, we have extended our model by including a heterogeneous mixture of clients, competition, strategic hacking, and shirking clients, and showed that our main conclusions are robust with respect to these variations.

Conclusions

INFORMATION TECHNOLOGY OUTSOURCING IS INHERENTLY COSTLY—the outsourcer typically needs to invest significant efforts to search for, contract with, and continuously manage a service provider [8]. Notwithstanding these obvious cost considerations, in the case of information security, encouraging too much outsourcing by imposing mandatory security requirements may not be good for the society. It is important to understand the motivations and implications of information security outsourcing before we could devise a proper environment to realize its potential benefits. This study serves just such a purpose.

Our analysis can be extended in multiple ways. We have assumed a monopoly security outsourcing market. Although we have examined the implications of competition, it would be more general to consider heterogeneous MSSPs in terms of their cost structure or security expertise, or perhaps their reputations. Also, we have assumed that the clients can estimate their own risks and therefore know the level of security protection that they need. A full analysis of information security as a credence good should consider settings whereby the clients *do not know* what they need. It would be important to incorporate the quality of diagnosis in such a setting. It would be interesting to see if a mandatory security requirement and liability would produce similar conclusions in such a setting, too.

Lastly, the success of information security outsourcing arguably rests not only on the MSSPs' but also on the clients' efforts. For example, if the clients do not properly secure their internal computer accounts or transmission media, which connect their systems to an MSSP's network, then their systems will be vulnerable regardless of how much effort the MSSP invests to strengthen security. How the strategic interaction between the MSSP and his clients shapes the quality of a security system, and how the threats posed by malicious hackers affect such strategic interaction, are important questions for future research.

Acknowledgments: Author names appear in alphabetical order. This research was supported in part by the Research Grants Council (RGC) of Hong Kong, Project 642411. The authors thank the seminar participants at the Institute of High Performance Computing, Agency for Science, Technology and Research at Singapore, and Ivan Png and Qiuhong Wang for valuable comments and suggestions.

NOTES

1. This result is consistent with industry observations that firms often expend little effort to monitor the MSSP. In particular, only 20 percent of firms in the technology, media, and telecommunications industries would audit their outsourcing service providers' activities [36]. Two-fifths of large organizations do not include security provisions in their outsourcing contracts *at all,* including many whose MSSPs are hosting highly confidential information [29].

2. In fact, anecdotal evidence has shown that security outsourcing may not necessarily lead to better security. A recent industry report has indicated that many firms in the United Kingdom believe that their security has neither improved nor deteriorated after using the external services [29]. The Australian Business Assessment of Computer User Security (ABACUS) survey has found that businesses that outsource their computer security are more likely to report breach of security incidents [45]. In this paper, social welfare is defined as the sum of client utility and MSSP's profit.

3. The literature has also considered cyber insurance as a means to manage information security risks but has mostly concluded that it is ineffective [9]. For a detailed discussion, see Bandyopadhyay et al. [7].

4. Our formulation of client utility, which characterizes the expected loss as the product of the threat of attack, a, security vulnerability, $1 - q_k$, and monetary value, v, is similar to that in Gordon and Loeb [24]. Throughout this paper we use the subscripts k for the client and s for the MSSP.

5. Mandatory security requirement is now quite common among organizations. For example, the European Union Data Protection Directive 95/46/EC requires firms to take reasonable measures to secure data from potential abuses. In the United States, the Federal Information Security Management Act of 2002 requires each federal agency to provide appropriate security protection for its systems. The Gramm–Leach–Bliley Act requires financial institutions to protect the security of customer data. The Health Insurance Portability and Accountability Act requires health care providers to adopt appropriate administrative and technical protections of consumers' health information. In the private sector, the ISO 27000 series requires firms to design and implement good information security management systems. Some professional associations, such as the ISM3 Consortium, are now promoting security maturity models (SMMs) that encompass various sets of security performance targets and systems configurations. In the Shirking Clients extension below we consider the scenario when the client can also shirk with in-house development.

6. We add a breve, $\breve{}$, for all results with a mandatory security requirement.

7. We used the following parameters to generate Figures 2 and 3: $c_s = 1$, $c_k = 2$, and $v = 10$. Further, for Figures 4–6, we added $n = 15$, $A = 0.5$, and $e = 0.01$ (refer to the discussion in the next section).

8. We assume that e is sufficiently small and that security outsourcing is feasible in the presence of system interdependency. Specifically, $e < (1/(n-1))((c_s/av) - 1)$, which, as we shall see below, ensures that $q \leq 1$.

9. For example, the MSSP needs to study each client's system and devise corresponding procedures and/or adjustments to integrate the security protection functions.

10. Since the clients and the MSSP have common knowledge on all the model parameters, in equilibrium the clients will rationally expect the MSSP's service coverage, m, and the MSSP will fulfill such an expectation.

11. We model the hacker's attack as random draws *without replacement*. So, the expected number of systems (excluding j) compromised by the hacker is the proportion of clients effectively protected by the MSSP, $\Sigma_{i=1,i\neq j}^{m}(1-q_i)/(n-1)$, multiplied by the hacker's attack coverage, which is, ex post, $na - 1$ when client j was attacked and na when client j was not attacked. We assume that the client population is sufficiently large relative to the hacker's attack coverage, A (which, given n, determines a), the number of MSSP's clients, m, and the spillover, e, to the extent that $L_j \leq 1$. An alternative approach to model this problem is to assume that client j suffers at most once from other clients' security breaches, which would then ensure that $L_j \leq 1$. Such a model is, however, analytically intractable. The key contribution of our analysis lies in accounting for spillover among the MSSP's clients due to security interdependency. The functional form of such spillover is of secondary importance (see also [55]).

12. By Equation (12), because the equilibrium q_s^* increases in m^*, the chance for the MSSP's clients' systems to be directly hacked, $a(1-q_s^*)$, decreases with multiple interdependent clients. Their utility in Lemma 2 stays the same as that in Lemma 1 because of the negative spillovers from others.

13. We define social welfare as the sum of all n clients' utilities and the MSSP's profit.

14. It is straightforward to prove the "dual" version of Proposition 4—that is, the decrease in social welfare due to system interdependency is particularly large when the mandatory security requirement is high, $\underline{q} > av/c_k$. The implication is that with a high mandatory security requirement, it is better to encourage the MSSP to "disconnect" his clients. This could be achieved by, for example, using separate server management systems and segmented or independent service platforms. In practice, however, it seems easier to adjust the security requirement level than to change the technology for managed security services.

15. We used the following parameters to generate Figure 8: $n = 10$, $c_s = 1$, $c_k = 1.25$, $v = 50$, $A = 0.05$, $e = 0.08$.

16. For example, both the IBM Payment Card Industry (PCI) solution and Motorola's security assessment solution highlight assessment service as a key feature of their solutions.

17. If, however, $av_0/c_k < \underline{q} \le av_1/c_k$, then $u_{k,0}$ will decrease but not $u_{k,1}$. Because of the substitution between high-type and low-type clients, the net effect of such a $\underline{q}$ on the equilibrium m_t^* and $q_{s,t}^*$, $t = 0, 1$, and the total number of clients, $m_0^* + m_1^*$, is ambiguous. Also, it is obvious that when $\underline{q} \le av_0/c_k$, then the mandatory security requirement is immaterial.

18. If $z \ge n$, each MSSPs will serve one client, and $q_s^* = av/c_s$.

19. Our analysis treats z as an exogenous parameter, and so in the oligopoly setting the MSSPs may still earn an abnormal profit. Realistically, as long as the MSSPs could make a positive profit, the market may continue to evolve with new entrants entering to share the profits. Hence, without other "frictions" or entry barriers, the managed security service market may degenerate into a perfectly competitive one, which, as we have mentioned, is generally good for social welfare. However, factors such as proprietary technology, transaction costs between the MSSP and clients, MSSPs' reputation, and so forth, may prevent clients from freely switching from one MSSP to another and facilitate an oligopoly.

20. We could only draw the implications based on a partial equilibrium analysis. A complete equilibrium analysis is tedious and analytically intractable.

21. Empirically, using an international panel of attack data, Png et al. [43] has found that the number of information security attacks is not affected by domestic enforcements or unemployment rates. This seems to be consistent with limited hacker resources, that is, a binding $\bar{A}$. For further evidence, see Gershwin [22].

22. We used the following parameters to generate Figure 9: $n = 10$, $c_s = 1$, $c_k = 2$, $v = 10$, $A = 0.05$, $e = 0.05$.

23. In the CardSystems' failure example that we cited in the Introduction, one wonders if the Merrick Bank would have lost its customers' credit card numbers had it not outsourced the payment processing to CardSystems. Also, the "clustering" of clients in an MSSP network, such as a cloud-based security platform or the use of common security protocols, naturally makes the network a bigger target for hackers.

24. A related issue is privacy audit. There has been a growing concern about consumer privacy on the Internet (see, e.g., [1, 25, 28, 38]). The European Union and some other countries have enforced the use of privacy protection by data collectors. Many trust seal issuers, such as Truste and BBBOnLine, profess to notarize organizations' data practices. Our research implies that if the government mandates organizations to protect consumer privacy, then auditing the practices of trust seal issuers may not be advisable. However, the governments should ensure that these trust seal issuers assume a liability ex ante in case of data breaches. This is not commonly practiced at the moment.

References

1. Acquisti, A., and Gross, R. Predicting social security numbers from public data. *PNAS, 106,* 27 (2009), 10975–10980.

2. Akerlof, G.A. Quality uncertainty and the market mechanism. *Quarterly Journal of Economics, 84,* 3 (1970), 488–500.

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

4. Armour, J., and Humphrey, W.S. Software product liability. Technical Report no. CMU/SEI-93-TR-13, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 1993.

5. August, T., and Tunca, T.I. Network software security and user incentives. *Management Science, 52,* 11 (2006), 657–670.

6. August, T., and Tunca, T.I. Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Science, 57,* 5 (2011), 934–959.

7. Bandyopadhyay, T.; Mookerjee V.; and Rao, R.C. Why IT managers don't go for cyber-insurance products. *Communications of the ACM, 52,* 11 (2009), 68–73.

8. Barthelemy, J. The hidden costs of IT outsourcing. *Sloan Management Review, 42,* 3 (2001), 60–69.

9. Bohme, R., and Schwartz, G. Modeling cyber-insurance: Towards a unifying framework. Paper presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), Harvard University, Cambridge, 2010 (available at http://weis2010.econinfosec.org/papers/session5/weis2010_boehme.pdf).

10. Burson, S. Outsourcing information security. CIO.com, January 19, 2010 (available at www.cio.com/article/518513/Outsourcing_Information_Security/).

11. 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.

12. Cezar, A.; Cavusoglu, H.; and Raghunathan, S. Competition, speculative risks, and IT security outsourcing. In T. Moore, D. Pym, and C. Ioannidis (eds.), *Economics of Information Security and Privacy.* New York: Springer, 2010, pp. 301–320.

13. Cezar, A.; Cavusoglu, H.; and Raghunathan, S. Outsourcing information security: Contracting issues and security implications. Paper presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), Harvard University, Cambridge, 2010 (available at http://weis2010.econinfosec.org/papers/session1/weis2010_cezar.pdf).

14. Charney, S. Collective defense: Applying public health models to the Internet. Microsoft, Redmond, WA, 2010.

15. 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.

16. Dey, D.; Fan, M.; and Zhang, C. Design and analysis of contracts for software outsourcing. *Information Systems Research, 21,* 1 (2010), 93–114.

17. Ding, W., and Yurcik, W. Outsourcing Internet security: The effect of transaction costs on managed service providers. Paper presented at the International Conference on Telecommunication Systems—Modeling and Analysis, Dallas, TX, November 17–20, 2005.

18. Ding, W.; Yurcik, W.; and Yin, X. Outsourcing Internet security: Economic analysis of incentives for managed security service providers. In X. Deng and Y. Ye (eds.), *Internet and Network Economics.* Lecture Notes in Computer Science, vol. 3828. Berlin: Springer, 2005, pp. 947–958.

19. Dulleck, U., and Kerschbamer, R. On doctors, mechanics, and computer specialists: The economics of credence goods. *Journal of Economic Literature, 44,* 1 (2006), 5–42.

20. Emons, W. Credence goods and fraudulent experts. *RAND Journal of Economics, 28,* 1 (1997), 107–119.

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

22. Gershwin, L.K. Cyber threat trends and U.S. network security. Central Intelligence Agency, Washington, DC, June 21, 2001 (available at www.cia.gov/news-information/speeches-testimony/2001/gershwin_speech_06222001.html).

23. Ghose, A., and Rajan, U. The economic impact of regulatory information disclosure on information security investments, competition, and social welfare. Paper presented at the Fifth Workshop on Economics of Information Security (WEIS 2006), Cambridge University, Cambridge, 2006 (available at http://weis2006.econinfosec.org/docs/37.pdf).

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

25. Hann, I.H.; Hui, K.L.; Lee, T.S.Y.; and Png, I.P.L. Overcoming online information privacy concerns: An information processing theory approach. *Journal of Management Information Systems, 42,* 2 (Fall 2007), 13–42.

26. Hausken, K. Strategic defense and attack for series and parallel reliability systems. *European Journal of Operational Research, 186* (2008), 856–881.

27. 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.

28. Hui, K.L.; Teo, H.H.; and Lee, T.S.Y. The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31,* 1 (2007), 19–33.

29. Information security breaches survey 2010. Technical Report, PriceWaterhouseCoopers, London, 2010.

30. IT outsourcing statistics 2010/2011. Computer Economics, Irvine, CA, October 2010.

31. Kim, B.C.; Chen, P.-Y.; and Mukhopadhyay, T. The effect of liability and patch release on software security: The monopoly case. *Production and Operations Management, 20,* 4 (2011), 603–617.

32. 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), 241–279.

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

34. Lee, C.H.; Geng, X.; and Raghunathan, S. Security standardization in the presence of unverifiable control. Paper presented at the Tenth Workshop on Economics of Information Security (WEIS 2011), George Mason University, Washington, DC, 2011 (available at http://weis2011.econinfosec.org/papers/Security%20Standardization%20in%20the%20Presence%20of%20Unverifiable%20Co.pdf).

35. Liu, P.; Zang, W.; and Yu, M. Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Transactions on Information and System Security, 8,* 1 (2005), 1–41.

36. Losing ground: 2009 TMT global security survey. Deloitte, Rotterdam, 2009 (available at www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/dtt_TMT-Security-Survey09-full.pdf).

37. MacArthur, K. McDonald's says hacker broke into customer database; FBI investigating. *Crain's Chicago Business,* December 13, 2010 (available at www.chicagobusiness.com/article/20101213/NEWS07/101219975/).

38. Mai, B.; Menon, N.M.; and Sarkar, S. No free lunch: Price premium for privacy seal-bearing vendors. *Journal of Management Information Systems, 27,* 2 (Fall 2010), 189–212.

39. Moeller, Robert. *IT Audit, Control and Security.* Hoboken, NJ: John Wiley & Sons, 2010.

40. Outpacing change: Ernst & Young's 12th annual global information security survey. Ernst & Young, New York, 2009.

41. Png, I.P.L., and Lehman, D. *Managerial Economics.* New York: Blackwell, 2002.

42. Png, I.P.L., and Wang, Q.-H. Information security: Facilitating user precautions vis-à-vis enforcement against attackers. *Journal of Management Information Systems, 26,* 2 (Fall 2009), 97–121.

43. Png, I.P.L.; Wang, C.-Y.; and Wang, Q.-H. The deterrent and displacement effects of information security enforcement: International evidence. *Journal of Management Information Systems, 25,* 2 (Fall 2008), 125–144.

44. Rice, M.; Butts, J.; Miller, R.; and Shenoi, S. Applying public health strategy to the protection of cyberspace. *International Journal of Critical Infrastructure Protection, 3,* 3–4 (2010), 118–127.

45. Richards, K., and Davis, B. Computer security incidents against Australian businesses: Predictors of victimisation. Australian Institute of Criminology, *Trends & Issues in Crime and Criminal Justice,* no. 399, September 2010 (available at www.aic.gov.au/documents/6/9/F/%7B69FC108B-D437-47E0-9C17-93B5DEFC8D96%7Dtandi399.pdf).

46. Rothschild, M., and Stiglitz, J.E. Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. *Review of Economic Studies, 44,* 3 (1977), 407–430.

47. Ryan, D.J. Two views on security software liability: Let the legal system decide. *IEEE Security & Privacy, 1,* 1 (2009), 70–72.
48. Sawyer, J. Tech insights: When to pull the outsourcing trigger. *Dark Reading,* April 23, 2010 (available at www.darkreading.com/security-services/167801101/security/securitymanagement/224600304/index.html).
49. Schneier, B. The case of outsourcing security. *Computer, 35,* 4 (2002), 20–26.
50. Schwartz, M.J. More firms outsourcing security to MSSPs. *InformationWeek,* June 17, 2010 (available at www.informationweek.com/security/management/more-firms-outsourcing-security-to-mssps/225700537/).
51. Spence, M. Consumer misperceptions, product failure and producer liability. *Review of Economic Studies, 44,* 3 (1977), 561–572.
52. Stiglitz, J.E. Monopoly, non-linear pricing and imperfect information: The insurance market. *Review of Economic Studies, 44,* 3 (1977), 407–430.
53. Use of IT security outsourcing low but rising as threats grow. Computer Economics, Irvine, CA, June 2009 (available at www.computereconomics.com/custom.cfm?name=postPaymentGateway.cfm&id=1459/).
54. Varian, H.R. System reliability and free riding. In L.J. Camp and S. Lewis (eds.), *Economics of Information Security.* Novell, MA: Kluwer Academic, 2004, pp. 1–15.
55. Vijayan, J. Outsourcers rush to meet security demand. *IT World,* March 8, 2001 (available at www.itworld.com/CWSTO57980/).
56. Whitman, M.E., and Mattord, H.J. *Principles of Information Security.* Boston: Course Technology, Cengage Learning, 2009.
57. Wolchok, S.; Yao, R.; and Halderman, J.A. Analysis of the Green Dam Censorware System. Working paper, Computer Science and Engineering Division, University of Michigan, Ann Arbor, 2009.
58. Wolinsky, A. Competition in markets for credence goods. *Journal of Institutional and Theoretical Economics, 151,* 1 (1995), 117–131.
59. Yue, W.T.; Cakanyildirim, M.; Ryu, Y.U.; and Liu, D. Network externalities, layered protection and IT security risk management. *Decision Support Systems, 44,* 1 (2007), 1–16.
60. Zetter, K. In legal first, data-breach suit targets auditor. *WIRED,* June 2, 2009 (available at www.wired.com/threatlevel/2009/06/auditor_sued/).

Appendix

Proof of Lemma 1

The Lagrangian function is

$$\Lambda = p - a\beta v\left(1-q_s\right) - \frac{1}{2}c_s q_s^2$$
$$-\lambda\left[p - avq_s - a\beta v\left(1-q_s\right) + \frac{1}{2}\frac{\left(av\right)^2}{c_k}\right].$$

The constraints are:

$$p \le avq_s + a\beta v\left(1-q_s\right) - \frac{1}{2}\frac{\left(av\right)^2}{c_k} \tag{A1}$$

$$\lambda \ge 0. \tag{A2}$$

Differentiating with respect to p, q_s, and β, we have

$$\frac{\partial \Lambda}{\partial p} = 1 - \lambda \tag{A3}$$

$$\frac{\partial \Lambda}{\partial q_s} = a\beta v - c_s q_s + \lambda a v - \lambda a \beta v \tag{A4}$$

$$\frac{\partial \Lambda}{\partial \beta} = -av\left(1 - q_s\right) + \lambda av\left(1 - q_s\right). \tag{A5}$$

Solving the Equations (A3), (A4), and (A5), we have $\lambda = 1$, $q_s^* = av/c_s$, and $p^* - a\beta^* v(1 - (av/c_s)) = ((av)^2/c_s) - (1/2)((av)^2/c_k)$. Substitute them into Equations (2) and (3), the client's utility and MSSP's profit follow.

Proof of Proposition 1

Proposition 1a is obvious because $\underline{q}$ is not binding. For Proposition 1b, the Lagrangian function is now

$$\Lambda = p - a\beta v\left(1 - q_s\right) - \frac{1}{2} c_s q_s^2$$
$$-\lambda\left[p - av\left(q_s - \underline{q}\right) - a\beta v\left(1 - q_s\right) + \frac{1}{2} c_k \underline{q}^2\right].$$

The constraints are

$$p \le av\left(q_s - \underline{q}\right) + a\beta v\left(1 - q_s\right) - \frac{1}{2} c_k \underline{q}^2 \tag{A6}$$

$$\lambda \ge 0. \tag{A7}$$

Differentiating with respect to p, q_s, and β, the first-order conditions are identical to Equations (A3), (A4), and (A5). Solving the equations, we have $\lambda = 1$, $\breve{q}_s^* = av/c_s$, and $\breve{p}^* - a\breve{\beta}^* v(1 - (av/c_s)) = ((av)^2/c_s) - av\underline{q} + (1/2)c_k\underline{q}^2$. Substitute them into Equations (2) and (3), the client's utility and MSSP's profit follow.

Finally, because the MSSP always chooses $\breve{q}_s^* = av/c_s$, his effort will match/exceed $\underline{q}$ whenever $\underline{q} \le av/c_s$. The MSSP will underprovide his service quality relative to $\underline{q}$ when $\underline{q} > av/c_s$.

Proof of Lemma 2

The Lagrangian function is

$$\Lambda = \sum_{j=1}^{m}\left(p_j - L_j\beta_j v - \frac{1}{2} c_s q_{s,j}^2\right)$$
$$-\sum_{j=1}^{m}\lambda_j\left[p_j - \left(a - L_j\right)v - L_j\beta_j v + \frac{1}{2}\frac{(av)^2}{c_k}\right].$$

The constraints are

$$p_j \le \left(a - L_j\right)v + L_j\beta_j v - \frac{1}{2}\frac{(av)^2}{c_k}, \quad j = 1,...,m, \tag{A8}$$

$$\lambda_j \ge 0, \quad j = 1,...,m. \tag{A9}$$

For simplicity, we treat m as if it were continuous (alternatively, we could redefine m to be a fraction of n, which must be continuous). Differentiating Λ with respect to p_j, $q_{s,j}$, and β_j, $j = 1,...,m$:

$$\frac{\partial \Lambda}{\partial p_j} = 1 - \lambda_j \tag{A10}$$

$$\frac{\partial \Lambda}{\partial q_{s,j}} = a\left[1 + e\left(m-1\right)\right]\left(\beta_j v + \lambda_j v - \lambda_j \beta_j v\right) - c_s q_{s,j} \tag{A11}$$

$$\frac{\partial \Lambda}{\partial \beta_j} = -L_j v + \lambda_j L_j v \tag{A12}$$

$$\begin{aligned}\frac{\partial \Lambda}{\partial m} &= \frac{\partial}{\partial m}\sum_{j=1}^{m}\left[p_j\left(1-\lambda_j\right) - \lambda_j\beta_j v\left(1-\lambda_j\right)\right] \\ &+ \frac{\partial}{\partial m}\sum_{j=1}^{m}\left[\lambda_j\left(a - L_j\right)v - \frac{1}{2}c_s q_{s,j}^2 + \frac{1}{2}\frac{\lambda_j (av)^2}{c_k}\right].\end{aligned} \tag{A13}$$

By Equations (A10) and (A12), $\partial\Lambda/\partial p_j = 0$ and $\partial\Lambda/\partial\beta_j = 0$ imply $\lambda_j = 1$, and so by Equation (A11), the MSSP will select the same quality, $q_{s,j}^* = q_s$ for all the clients. Equation (A13) then simplifies to

$$\frac{\partial \Lambda}{\partial m} = eav + av\left(1-e\right)q_s - 2eavm\left(1-q_s\right) - \frac{1}{2}c_s\left(q_s\right)^2 - \frac{1}{2}\frac{(av)^2}{c_k}. \tag{A14}$$

Solving all the first-order conditions, we have

$$m^* = \frac{1}{2} + \frac{avq_s^* - \frac{1}{2}c_s\left(q_s^*\right)^2 - \frac{1}{2}\frac{(av)^2}{c_k}}{2eav\left(1-q_s^*\right)},$$

$$q_{s,j}^* = q_s^* = \frac{Tav}{c_s},$$

and

$$p_j^* - Ta\beta_j^* v\left(1 - \frac{Tav}{c_s}\right) = \frac{(Tav)^2}{c_s} - \frac{1}{2}\frac{(av)^2}{c_s} - av\left(T-1\right),$$

where $T \equiv 1 + e(m^* - 1) > 1$. It is straightforward to show that if e is sufficiently small, the second term in m^* will be positive, and $q_s^* < 1$. Further, with a sufficiently large

number of clients, n, m^* will be bounded between 1 and n. These conditions guarantee that an interior solution exists.

Suppose that the solution characterized by m^* and q_s^* is unique. Substituting these results into Equations (9) and (10), we can obtain the clients' utility in Equation (4) and the MSSP's profit in Equation (13). Note that because m^* maximizes π, and, by Equation (13), $\pi = (1/2)(av)^2((1/c_s) - (1/c_k)) > 0$ if $m^* = 1$, the equilibrium $\pi^* \geq (1/2)(av)^2((1/c_s) - (1/c_k)) > 0$.

It remains to be proved that the solution characterized by m^* and q_s^* is unique. First, observe that $dq_s^*/dm^* = eav/c_s$, which is a positive constant. So, q_s^* increases linearly in m^*. Similarly,

$$\frac{dm^*}{dq_s^*} = \frac{av - c_s q_s^* + \frac{1}{2} c_s \left(q_s^*\right)^2 - \frac{1}{2}\frac{(av)^2}{c_k}}{2eav\left(1 - q_s^*\right)^2}.$$

When $q_s^* = 0$, $dm^*/dq_s^* > 0$. As q_s^* increases, the numerator in dm^*/dq_s^* decreases, but, up to $q_s^* = Tav/c_s$, $dm^*/dq_s^* > 0$. Next, it is straightforward to show that the sign of $d^2m^*/d(q_s^*)^2$ has the sign of $2av - c_s - (1/2)((av)^2/c_k)$, which, given v, c_k, c_s, and a, is always a constant. Hence, m^* is either strictly convex or strictly concave in q_s^*. Since q_s^* is linear and increasing in m^*, and m^* is either strictly convex or strictly concave in q_s^*, other than the corner solution whereby $m^* = 1$ and $q_s^* = av/c_s$ (i.e., the outcome in the single-client case), the $m^*(q_s^*)$ curve and the $q_s^*(m^*)$ curve could intersect at most once, which implies that given selected v, c_k, c_s, and a, the solution characterized by m^* and q_s^* must exist and is unique.

Proof of Proposition 2

The Lagrangian function is

$$\breve{\Lambda} = \sum_{j=1}^{m}\left(p_j - L_j\beta_j v - \frac{1}{2}c_s q_{s,j}^2\right)$$
$$-\sum_{j=1}^{m}\lambda_j\left[p_j - \left(a - L_j\right)v - L_j\beta_j v + av\underline{q} - \frac{1}{2}c_k\underline{q}^2\right].$$

The first-order conditions with respect to p_j, $q_{s,j}$, and β_j are identical to Equations (A10), (A11), and (A12), and so, again, the MSSP will select the same service quality, $\breve{q}_{s,j}^* = \breve{q}_s^*$ for all clients who use his service. The first-order condition with respect to m is then

$$\frac{\partial\breve{\Lambda}}{\partial m} = eav + av\left(1 - e\right)q_s - 2eavm\left(1 - q_s\right) - \frac{1}{2}c_s\left(q_s\right)^2 - av\underline{q} + \frac{1}{2}c_k\underline{q}^2. \qquad \text{(A15)}$$

Solving all the first-order conditions, we have

$$\breve{m}^* = \frac{1}{2} + \frac{av\breve{q}_s^* - \frac{1}{2}c_s\left(\breve{q}_s^*\right)^2 - av\underline{q} + \frac{1}{2}c_k\underline{q}^2}{2eav\left(1-\breve{q}_s^*\right)},$$

$$\breve{q}_{s,j}^* = \breve{q}_s^* = \frac{\breve{T}av}{c_s},$$

and

$$\breve{p}_j^* - \breve{T}a\breve{\beta}_j^* v\left(1-\frac{\breve{T}av}{c_s}\right) = \frac{\left(\breve{T}av\right)^2}{c_s} - av\left(\breve{T}-1\right) - av\underline{q} + \frac{1}{2}c_k\underline{q}^2,$$

where $\breve{T} \equiv 1 + e(\breve{m}^* - 1) > 1$. Here again, if e is sufficiently small and n is sufficiently large, $\breve{q}_s^* < 1$ and $\breve{m}^*$ is bounded between 1 and n, which guarantee the existence of an interior solution. The proof of uniqueness then follows a similar procedure as outlined in Lemma 2.

Substitute the above results into Equations (9) and (10), we can obtain the clients' utility in Equation (7) and the MSSP's profit in Equation (16). Because $\breve{m}^*$ maximizes $\breve{\pi}$, and

$$\breve{\pi} = \frac{1}{2}(av)^2\left(\frac{1}{c_s} - \frac{1}{c_k}\right) + \frac{1}{2}c_k\left(\underline{q} - \frac{av}{c_k}\right)^2 > 0$$

if $\breve{m}^* = 1$, the equilibrium $\breve{\pi}^* > 0$.

Finally, because the MSSP always chooses $\breve{q}_s^* = \breve{T}av/c_s$, his effort will match/exceed $\underline{q}$ whenever $\underline{q} \le \breve{T}av/c_s$. The MSSP will underprovide service quality relative to $\underline{q}$ when $\underline{q} > \breve{T}av/c_s$.

Proof of Proposition 3

Differentiating Equations (A14) and (A15) with respect to m, $\partial^2\Lambda/\partial m^2 = \partial^2\breve{\Lambda}/\partial m^2 = -2eav(1 - q_s) < 0$, which implies that Λ and $\breve{\Lambda}$ are strictly concave in m. Now, by Equations (A14) and (A15),

$$\frac{\partial\breve{\Lambda}}{\partial m} - \frac{\partial\Lambda}{\partial m} = \frac{1}{2}c_k\left(\underline{q} - \frac{av}{c_k}\right)^2 > 0, \tag{A16}$$

and so, given any pairs of m and q_s, $\partial\breve{\Lambda}/\partial m > \partial\Lambda/\Delta m$. Equation (A16) implies that at the m^* and q_s^* which maximizes Λ we must have

$$\left.\frac{\partial\breve{\Lambda}}{\partial m}\right|_{m=m^*, q_s=q_s^*} > \left.\frac{\partial\Lambda}{\partial m}\right|_{m=m^*, q_s=q_s^*} = 0.$$

Since $\breve{\Lambda}$ is strictly concave in m,

$$\left.\frac{\partial \breve{\Lambda}}{\partial m}\right|_{m=m^*, q_s=q_s^*} > 0$$

necessarily means that the equilibrium $\breve{m}^* > m^*$. This also implies that the optimal security quality,

$$\breve{q}_s^* = \frac{av}{c_s}\left[1+e\left(\breve{m}^*-1\right)\right] > q_s^* = \frac{av}{c_s}\left[1+e\left(m^*-1\right)\right].$$

Finally, by Proposition 2, the MSSP will shirk if and only if $\underline{q} > \breve{T}av/c_s$. If $\breve{m}^*$ increases, $\breve{T}$ also increases, and so it is less likely for $\underline{q} > \breve{T}av/c_s$, that is, the MSSP will be less likely to shirk.

Proof of Proposition 4

To prove this proposition, it is instrumental to compute the first-best social welfare. Let there be $m \le n$ outsourcing clients. Substituting from Equations (1), (9), and (10), first-best social welfare,

$$W = (n-m)\left[(1-a)v + \frac{1}{2}\frac{(av)^2}{c_k}\right] + \sum_{j=1}^{m}\left[\left(1-L_j\right)v - \frac{1}{2}c_s q_{s,j}^2\right]. \qquad \text{(A17)}$$

The first term in Equation (A17) is the sum of utility that the "excluded" clients obtain by developing in-house protection (by the analysis in the basic model, the optimal decision of the clients who are not outsourcing is to select $q_k^* = av/c_k$, which gives the maximum utility $u_k^* = (1-a)v + (1/2)((av)^2/c_k)$). The second term in Equation (A17) is the net utility generated for the m outsourcing clients, which is simply the sum of Equations (9) and (10) (when computing social welfare, the transfer payment between the clients and the MSSP is irrelevant).

Differentiating Equation (A17) with respect to $q_{s,j}$ and m, and suppose that the MSSP chooses the same quality level for all clients, it is straightforward to show that the first-order conditions are identical to Equations (A11) and (A14). This implies that the optimal m and q_s that maximize social welfare are identical to Equations (11) and (12), that is, they are also the solution for the case with no mandatory security requirement.

Accordingly, the solution presented in Lemma 2 provides the first-best social welfare. By definition, any deviation of m or $q_{s,j}$ away from this solution, including the $\breve{m}^*$ and $\breve{q}_s^*$ in Proposition 2, that is, Equations (14) and (15), should reduce social welfare.

Next, by Lemma 1 and Proposition 1, with or without $\underline{q}$, the social welfare from serving each client is always $(1-a)v + (1/2)((av)^2/c_s)$. Hence, the social welfare from serving all n clients, $W_{-e} = n[(1-a)v + (1/2)((av)^2/c_s)]$. In other words, without system interdependency, the social welfare change due to $\underline{q}$, $\Delta W_{-e} = 0$.

With system interdependency, denote the social welfare with $\underline{q} > av/c_k$ as $\breve{W}$. Then, by Equation (A17) and the discussion thereafter, we must have $W > \breve{W}$, and so $W - \breve{W} > \Delta W_{-e} = 0$.

Proof of Proposition 5

By Proposition 2, when $\underline{q} \le \breve{T}av/c_s$, it is in the best interest of the MSSP to choose $\breve{q}_s^* = \breve{T}av/c_s$, and so imposing verifiability will not affect the equilibrium outcome.

Next, for any $\underline{q} > \breve{T}av/c_s$, the solution in Equations (14) and (15) yields the maximum profit for the MSSP, and so any deviation in $\breve{q}_s^*$ or $\breve{m}^*$ will necessarily reduce the MSSP's profit. Because all n clients will obtain utility $\breve{u}_s^* = \breve{u}_k^* = (1-a)v + av\underline{q} - (1/2)c_k\underline{q}^2$ with or without verifiability, a decrease in the MSSP's profit directly implies a decrease in social welfare. Finally, when $\underline{q} > \breve{T}av/c_s$, with verifiability, the MSSP's clients are better protected because they now get $\underline{q}$ from the MSSP instead of $\breve{q}_s^* = \breve{T}av/c_s$.

Proof of Results in Extension: Heterogeneous Clients

The Lagrangian function is

$$\Lambda = \sum_{t=0,1}\sum_{j=1}^{m_t}\left(p_{t,j} - L_{t,j}\beta_{t,j}v_t - \frac{1}{2}c_s q_{s,t,j}^2\right) - \sum_{t=0,1}\sum_{j=1}^{m_t}\lambda_{t,j}\left[p_{t,j} - \left(1-L_{t,j}\right)v_t - L_{t,j}\beta_{t,j}v_t + u_{k,t}\right].$$

The constraints are

$$p_{t,j} \le \left(1-L_{t,j}\right)v_t + L_{t,j}\beta_{t,j}v_t - u_{k,t}, \quad t=0,1,\ j=1,...,m \tag{A18}$$

$$\lambda_{t,j} \ge 0,\ t=0,1, \quad j=1,...,m. \tag{A19}$$

Differentiating Λ with respect to $p_{t,j}$, $q_{s,t,j}$, and $\beta_{t,j}$, $t=0,1$, $j=1,...,m$,

$$\frac{\partial\Lambda}{\partial p_{t,j}} = 1-\lambda_{t,j} \tag{A20}$$

$$\frac{\partial\Lambda}{\partial q_{s,t,j}} = a\left[1+e\left(m_t-1\right)\right]\left(\beta_{t,j}v_t + \lambda_{t,j}v_t - \lambda_{t,j}\beta_{t,j}v_t\right) + eam_{1-t}\left(\beta_{1-t,j}v_{1-t} + \lambda_{1-t,j}v_{1-t} - \lambda_{1-t,j}\beta_{1-t,j}v_{1-t}\right) - c_s q_{s,t,j} \tag{A21}$$

$$\frac{\partial\Lambda}{\partial\beta_{t,j}} = -L_{t,j}v_t + \lambda_{t,j}L_{t,j}v_t. \tag{A22}$$

By Equations (A20) and (A22), $\partial\Lambda/\partial p_{t,j} = 0$ and $\partial\Lambda/\partial\beta_{t,j} = 0$ imply $\lambda_{t,j} = 1$, and so by Equation (A21), the MSSP will select the same quality, $q_{s,t,j}^* = q_{s,t}$, for each type of client. Then,

$$\frac{\partial \Lambda}{\partial m_t} = (1-a)v_t + av_t q_{s,t} + eav_t\left(1-q_{s,t}\right) - 2eav_t m_t\left(1-q_{s,t}\right) - eam_{1-t}\left(1-q_{s,1-t}\right)v_t - u_{k,t} - \frac{1}{2}c_s q_{s,t}^2 - eam_{1-t}\left(1-q_{s,t}\right)v_{1-t}. \tag{A23}$$

Substituting $\lambda_{t,j} = 1$ and rearranging Equations (A21) and (A23):

$$q_{s,t}^* = \frac{a\left[1+e\left(m_t^*-1\right)\right]v_t + eam_{1-t}^* v_{1-t}}{c_s},$$

$$m_t^* = \frac{1}{2} + \frac{(1-a)v_t + av_t q_{s,t}^* - u_{k,t} - \frac{1}{2}c_s\left(q_{s,t}^*\right)^2}{2eav_t\left(1-q_{s,t}^*\right)} - \frac{m_{1-t}^*}{2}\left(\frac{v_{1-t}}{v_t} + \frac{1-q_{s,1-t}^*}{1-q_{s,t}^*}\right).$$

Because $(d/du_{k,t})(\partial\Lambda/\partial m_t) < 0$, if $\underline{q} > av_1/c_k > av_0/c_k$, then $u_{k,t}$ will decrease and $\partial\Lambda/\partial m_t$ will increase, which implies that the equilibrium m_t^*, $t = 0, 1$, will increase. In other words, the MSSP will tend to serve more clients of both types. By Equation (A21) and so Equation (17), the equilibrium $q_{s,0}^*$ and $q_{s,1}^*$ will increase too.

If, however, $av_0/c_k < \underline{q} \le av_1/c_k$, then $u_{k,0}$ will decrease but not $u_{k,1}$. The net effect of such a $\underline{q}$ on m_t^* depends on the relative magnitude of v_t^*, $t = 0, 1$, and so is ambiguous. Similarly, by Equation (17), $q_{s,t}^*$ is a function of m_t^*, and thus the impact of $\underline{q}$ on $q_{s,t}^*$ is ambiguous, too.

Proof of Results in Extension: Competition

The proofs of the first two cases, perfection competition and oligopoly, are already sketched in the text. We argue that for the last case, when $z\breve{m}^* > n$ but the market does not exhibit perfect competition, no pure strategy equilibrium exists. We sketch the idea below.

Suppose that there exists a pure strategy equilibrium in which the MSSPs choose some fixed prices and service quality. Because $z\breve{m}^* > n$, some MSSPs will have "excess capacity" relative to $\breve{m}^*$. Then, a marginal reduction in price or a marginal increase in liability would bring a first-order gain in number of clients but a second-order loss in revenue, and so would improve the MSSP's profit. Similarly, a marginal increase in service quality would bring a first-order gain in number of clients but only a second-order loss in service cost. So, the MSSPs will have incentives to bid down the prices or bid up the liability and service quality. However, they will not want to bid the prices, liabilities, and service quality all the way to the marginal cost because they could make a profit in some middle ranges. Hence, no pure strategy equilibrium exists when $z\breve{m}^* > n$, but the market does not exhibit perfect competition.

Proof of Results in Extension: Strategic Hacking

(a) By Equations (20) and (22),

$$\frac{\partial A^*}{\partial q_s} = \frac{\partial \breve{A}^*}{\partial q_s} = -\frac{b}{c_h}\frac{m}{n} < 0,$$

$$\frac{\partial A^*}{\partial q_k} = -\frac{b}{c_h}\left(1-\frac{m}{n}\right) < 0,$$

and, clearly, $\breve{A}^*$ is independent of q_k, and so $\partial \breve{A}^*/\partial q_k = 0$.

(b) By Equations (20) and (22),

$$\frac{\partial A^*}{\partial m} = -\frac{b}{c_h}\frac{\left(q_s - q_k\right)}{n} < 0$$

because, by Proposition 2 and Lemma 2, $q_s > q_k$. Further,

$$\frac{\partial \breve{A}^*}{\partial m} = -\frac{b}{c_h}\frac{q_s - \underline{q}}{n} < 0$$

if and only if $q_s > \underline{q}$, which, by Proposition 2, happens when the MSSP is honest.

(c)

$$\frac{\partial}{\partial A}\frac{\partial u_k}{\partial q_k} = \frac{v}{n} > 0$$

and

$$\frac{\partial}{\partial A}\frac{\partial \pi}{\partial q_s} = \frac{mv}{n}\left[1+e\left(m-1\right)\right] > 0.$$

(d) For the clients who are not outsourcing, they always have to choose $\underline{q}$, and so a marginal change in A would not affect their decisions. For the MSSP's clients,

$$\frac{\partial}{\partial A}\frac{\partial \breve{\pi}}{\partial q_s} = \frac{mv}{n}\left[1+e\left(m-1\right)\right] > 0.$$

For $q_s \le \underline{q}$,

$$\frac{\partial}{\partial A}\frac{\partial \breve{\pi}}{\partial m} = \frac{v}{n}\left(-\underline{q}+q_s\right) - \frac{ev}{n}\left(1-q_s\right)\left(2m-1\right) < 0.$$

(e) By Equation (22),

$$\frac{d\breve{A}^*}{dq} = -\frac{b}{c_h}\left(1-\frac{m}{n}\right) < 0.$$

Proof of Results in Extension: Shirking Clients

The proof follows that of Proposition 6 and so we omit it here.