

Singapore Management University

## Institutional Knowledge at Singapore Management University

---

Research Collection School Of Information Systems

School of Information Systems

---

5-2019

### Bilateral liability-based contracts in information security outsourcing

Kai-Lung HUI

Ping Fan KE

Singapore Management University, [pfke@smu.edu.sg](mailto:pfke@smu.edu.sg)

Yuxi YAO

Wei Thoo YUE

Follow this and additional works at: [https://ink.library.smu.edu.sg/sis\\_research](https://ink.library.smu.edu.sg/sis_research)



Part of the [Information Security Commons](#)

---

#### Citation




HUI, Kai-Lung; KE, Ping Fan; YAO, Yuxi; and YUE, Wei Thoo. Bilateral liability-based contracts in information security outsourcing. (2019). *Information Systems Research*. 30, (2), 411-429. Research Collection School Of Information Systems.

Available at: [https://ink.library.smu.edu.sg/sis\\_research/4885](https://ink.library.smu.edu.sg/sis_research/4885)

This Journal Article is brought to you for free and open access by the School of Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email [libIR@smu.edu.sg](mailto:libIR@smu.edu.sg).

# Bilateral Liability-Based Contracts in Information Security Outsourcing

Kai-Lung Hui,<sup>a</sup> Ping Fan Ke,<sup>a</sup> Yuxi Yao,<sup>b</sup> Wei T. Yue<sup>c</sup>

<sup>a</sup> Department of Information Systems, Business Statistics, and Operations Management, School of Business and Management, Hong Kong University of Science and Technology, Hong Kong, China; <sup>b</sup> Department of Economics, University of Western Ontario, London, Ontario N6A 5C2, Canada; <sup>c</sup> Department of Information Systems, College of Business, City University of Hong Kong, Hong Kong, China  
**Contact:** klhui@ust.hk,  <https://orcid.org/0000-0002-7074-1176> (K-LH); pfke@connect.ust.hk,  <https://orcid.org/0000-0002-4205-7801> (PFK); yyao226@uwo.ca (YY); wei.t.yue@cityu.edu.hk,  <https://orcid.org/0000-0002-1344-153X> (WTY)

**Received:** September 10, 2014

**Revised:** January 26, 2016; September 21, 2017

**Accepted:** July 9, 2018

**Published Online in Articles in Advance:**  
May 23, 2019

<https://doi.org/10.1287/isre.2018.0806>

**Copyright:** © 2019 INFORMS

**Abstract.** We study the efficiency of bilateral liability-based contracts in managed security services (MSSs). We model MSS as a collaborative service with the protection quality shaped by the contribution of both the service provider and the client. We adopt the negligence concept from the legal profession to design two novel contracts: threshold-based liability contract and variable liability contract. We find that they can achieve the first best outcome when postbreach effort verification is feasible. More importantly, they are more efficient than a multilateral contract when the MSS provider assumes limited liability. Our results show that bilateral liability-based contracts can work in the real world. Hence, more research is needed to explore their properties. We discuss the related implications.

**History:** Alok Gupta and Il-Horn Hann, Senior Editors; Sabyasachi Mitra, Associate Editor.

**Funding:** This work was supported by the Research Grants Council of Hong Kong [Grant GRF 642411].

**Supplemental Material:** The online appendix is available at <https://doi.org/10.1287/isre.2018.0806>.

**Keywords:** managed security service • liability-based contracts • negligence • auditing error • limited liability

## 1. Introduction

The managed security services (MSSs) market has grown by 10% in 2016, reaching an annual revenue of \$9.6 billion (Gartner 2017). Industry forecasts predict that the MSS market may grow at a cumulative average growth rate of 12% per year until 2020 (Technavio 2016). However, outsourcing security protection via MSS does not completely shield a firm from cyberattacks and intrusions. For example, Target suffered from a massive data breach in 2013, losing more than 100 million customer records that cost the company \$148 million (Abrams 2014). Apparently, Target's vendor, FireEye, detected the security attack and alerted Target, but Target failed to take action (Riley et al. 2014). This incident and countless other security breaches involving MSSs highlight the challenges and risks of sharing security protection responsibility across multiple parties.

Despite these security incidents, the relationship between firms and MSS providers will likely move toward a more integrated partnership instead of just an outsourcing vendor-client relationship (Chuvakn 2014). This closely knit collaborative relationship raises questions. How do we ensure that the client and the MSS provider will both invest the necessary efforts to protect the client's system? What are the optimal pricing and liability terms in MSS contracts?

Under a collaborative setting, the client and the MSS provider naturally want each other to assume more

liability. The views on liability can differ greatly depending on the perspective. Some practitioners hold the view that the MSS provider should be held fully accountable for the losses suffered by a client when there is failure in protection (Bahirwani 2015). However, the Target incident suggests that, in some cases, the client should share part of the responsibility as well.

To explore the MSS landscape and practices, we survey some popular security service outsourcing contracts in Table 1. Several features are common in these contracts. All of them are bilateral between the client and the MSS provider without involving any other parties. Furthermore, they include some liability terms under the service-level agreements (SLAs), which specify the compensation to the client in the event of a security breach. Some of these compensations are provided on the condition that the client takes prespecified actions, such as complying with configuration guidelines or maintaining the connectivity of the security devices. Obviously, to meet these conditions, the MSS provider must be able to assess the client's effort after a security breach incident.

The MSS contracts in Table 1 are consistent with the growing consensus on using liability terms to achieve accountability (Hurley 2004, Lichtman and Posner 2006, Chandler 2010, Fisher 2013, Fryer et al. 2013). The liability in these MSS contracts resembles the role of warranty typically provided for durable products. The difference here is that the quality of the service

**Table 1.** MSS Contract Examples

Provider	Service	SLA remedy	Details
IBM <sup>a</sup>	Managed protection service	Loss based	Premium incident prevention: compensate at prenegotiated amount; others: compensate a part of monthly fee
	Network IDPS	Threshold based	Compensate a part of monthly fee only when the client provides accurate contact and network/server information
	Network firewall		
	Security event and log management		
	Unified threat management	Threshold based	Compensate a part of monthly fee only when the client's system configuration complies with the provided configuration guideline
	Vulnerability management		
	Web security		
Email security			
Dell SecureWorks <sup>b</sup>	Managed firewall	Threshold based	Compensate 1/30th of monthly charge only when the client complies with the stated customer requirements, such as maintaining the health and connectivity of the security device
	Managed IPS		
	Security monitoring service		
Symantec <sup>c</sup>	Policy compliance	Loss based	Compensate 1/30th of monthly charge
	Vulnerability management	N/A	
	External penetration testing	N/A	
Verizon <sup>d</sup>	MSS	Loss based	Offer limited warranty
	Managed web content service	Threshold based	Compensate one service credit, which is a percentage of daily charge
	Managed email content service		
	Managed intrusion protection	Loss based and threshold based	Compensate a percentage of monthly recurring charge only when the security service failure is not caused by client-side fault, such as customer-approved change in hardware or software, or inaccurate contact information
	Managed PKI for remote access		
	DOS defense		
	Managed firewall		
Trustwave <sup>e</sup>	MSS	Threshold based	Availability: compensate one-day credit
	MSS	Threshold based	Proactive notification: compensate one-day credit only when client's contact information is accurate
BT <sup>f</sup>	MSS	Threshold based	Compensate one-day charge only when the client meets the stated obligation set forth
CenturyLink <sup>g</sup>	MSS	Threshold based	Compensate at most 50% of monthly charge only when the incident is not caused by the client
Orange Business Services <sup>h</sup>	Web protection suite	Loss based	Compensate two-day charge only when the service failure is not caused by the acts or omissions of the client
			Compensate a percentage of monthly service charge

*Note.* DOS, denial-of-service; IDPS, intrusion detection and prevention systems; IPS, intrusion prevention systems; N/A, not available; PKI, public key infrastructure.

<sup>a</sup>See IBM's contract documents: [http://www-935.ibm.com/services/us/iss/html/contracts\\_worldwide\\_landing.html](http://www-935.ibm.com/services/us/iss/html/contracts_worldwide_landing.html).

<sup>b</sup>See Dell's security services contract documents: <http://www.dell.com/learn/us/en/04/service-contracts-security-services>.

<sup>c</sup>See Symantec's contract documents: <http://www.symantec.com/business/support/index?page=content&id=TECH131855>.

<sup>d</sup>See Verizon's security services contract documents: <http://www.verizonenterprise.com/terms/us/products/security/>.

<sup>e</sup>See Trustwave's MSS SLA: [https://www3.trustwave.com/SLA/Ver001\\_Trustwave\\_MSS\\_SLA.PDF](https://www3.trustwave.com/SLA/Ver001_Trustwave_MSS_SLA.PDF).

<sup>f</sup>See BT's Convergent Solutions Contract: [https://www2.bt.com/static/i/media/pdf/ip\\_converge\\_service\\_schedule.pdf](https://www2.bt.com/static/i/media/pdf/ip_converge_service_schedule.pdf).

<sup>g</sup>See CenturyLink's MSS SLA: <http://www.centurylink.com/legal/docs/Managed-Security-Service.pdf>.

<sup>h</sup>See Orange Business Service's Web Protection Suite SLA: [http://www.orange-business.com/files/media/contributor\\_en/sla.web\\_protection\\_suite.gbl\\_06-13.pdf](http://www.orange-business.com/files/media/contributor_en/sla.web_protection_suite.gbl_06-13.pdf).

(i.e., the client's state of security) is highly dependent on both the client's efforts and the MSS provider's efforts.

To incentivize both the client and the MSS provider to work hard via a bilateral contract, we need to verify either the client's effort or the MSS provider's effort after a security breach. This could be a costly undertaking even with the proviso that advances in storage and networking technologies and security auditing have greatly enhanced the feasibility of tracking the activities of the involved parties. With this backdrop,

it is important to design bilateral MSS contracts that minimize the need for verification while encouraging effort contribution by both the client and the MSS provider.

In this paper, we explore the optimal design of bilateral liability-based contracts. We start with a simple loss-based contract, which requires the MSS provider to compensate the client fully in case of a security breach. We then design other liability-based contracts with different verification requirements. In particular, the legal profession assesses damage using the calculus of

negligence (the “Hand rule”) from the tort literature (Rustad and Koenig 2007, Naldi et al. 2013). *Comparative negligence* allocates liability on the basis of the proportion of damage caused by the plaintiff and defendant, whereas *contributory negligence* allocates liability to the plaintiff when he or she is deemed to have contributed to the damage (Cooter and Ulen 1986). Using these two negligence concepts, we design two liability-based contracts: variable liability contract and threshold-based liability contract.

The *variable liability* contract follows the spirit of comparative negligence and assigns the liability based on the effort invested by the client. In other words, the compensation received by the client in the event of a security breach is proportional to the effort that she invests. By contrast, the *threshold-based liability* contract follows the spirit of contributory negligence. Under this contract, the client will receive compensation if and only if her effort exceeds a certain threshold.

These two types of contracts involve different assessment and verification requirements before and after security breaches. A variable liability contract requires the MSS provider to have a full account of the client’s protection effort after a breach has occurred. Hence, it is demanding in terms of postbreach verification. A threshold-based liability contract does not require such extensive verification. Instead, it only requires judging whether the client’s effort has exceeded a predefined threshold, which is simpler in terms of postbreach verification (compared with a detailed audit of all actions undertaken by the client). However, to construct a threshold-based liability contract, the client and the MSS provider have to predetermine the threshold effort needed from the client. This is not a trivial task.

We analytically compare the performance of loss-based contract, variable liability contract, and threshold-based liability contract in terms of the ability to induce effort investments from the client and the MSS provider. We find that only variable liability contract and threshold-based liability contract can lead to socially optimal outcomes. We then assess the performance of these two contracts under different real-world constraints (viz the presence of postbreach verification errors and the assumption of limited liability). We find that threshold-based liability contract performs better than variable liability contract in these settings. We conclude the analysis by comparing these two liability-based contracts with a multilateral loss-based contract, which also leads to socially optimal effort investments without the need for postbreach verification (Lee et al. 2013). We show that the two liability-based contracts suffer less effort distortion than the multilateral loss-based contract under limited liability.

This study makes three important contributions. First, it incorporates the negligence concept from the

legal profession in designing novel bilateral contracts that can help induce socially optimal outcomes in MSS settings. Second, it illustrates that, even with postbreach effort verification, nuanced design of the contract terms could still lead to different extents of inefficiency when the market encompasses realistic constraints, such as limited liability or verification errors. Third, it provides a theoretical basis for exploring the optimal design of MSS contracts in other complex settings, such as the presence of strategic hackers or collaborative multiparty security protection (Cavusoglu et al. 2009).

The rest of this paper is organized as follows. Section 2 reviews the related literature. Section 3 presents the model, particularly the two bilateral liability-based contracts. It also considers the scenario with effort verification errors. Section 4 checks the robustness of our results with interdependent clients. Section 5 applies our model to several security configurations and breach scenarios. Section 6 considers the scenario with limited liability and compares the performance of the bilateral liability-based contracts with a multilateral loss-based contract. Section 7 discusses and concludes the paper.

## 2. Literature Review

This research is related to prior studies on pricing models in information systems outsourcing contracts (Gopal et al. 2003, Dey et al. 2010, Mani et al. 2012). In general, we can consider loss-based contract as one type of fixed price contract that is contingent on service outcome, whereas variable liability contract and threshold-based liability contract are similar to variable price contracts (Roels et al. 2010). For these pricing contracts, adding nonprice provisions, such as an extendibility clause, could be an effective means of promoting efficiency (Susarla et al. 2010). Our setting deviates from these pricing studies in that both the client’s efforts and the MSS provider’s efforts contribute to shaping the security of the system (compared with a typical outsourcing contract, where the outcome depends only on the service provider’s effort).

In particular, our focus on bilateral protection efforts follows the same spirit as previous studies on collaborative contributions, such as software engineering (Jayanth et al. 2011), collaborative services (Roels et al. 2010), product design (Bhattacharya et al. 2014), and information security outsourcing (Lee et al. 2013). A common feature in these settings is the presence of information asymmetry on both sides of the market, giving rise to double moral hazard (Cooper and Ross 1985, Bhattacharyya and Lafontaine 1995). It is well known that first best outcomes are not achievable when the efforts from the two involved parties are not contractible. To induce the client and the service provider to exert socially optimal efforts, we need to add additional features or requirements to the context.

One way is to add some third parties. Lee et al. (2013) propose a multilateral contract where the MSS provider has to compensate some third parties, such as other MSS clients or designated beneficiaries, when a focal client's system is compromised. With this contract, the breached client will not receive any compensation, whereas the MSS provider has to pay a compensation for security breaches. Hence, both of them have incentives to invest in protection. This solution is theoretically sound and follows the same spirit as the "nonbalanced" or surplus loss schemes in the principal agent model (Kambhu 1982, Emons 1988). However, negotiating for such multilateral arrangements is not trivial in the real world, especially when it requires the MSS provider to compensate other parties unrelated to the security incident. None of the contracts surveyed in Table 1 involve multilateral arrangements.

Another way to encourage protection is to increase the uncertainty of the payoff. In particular, the use of liability schemes can induce efficient outcomes when the client needs to incur a loss even with compensation. The intuition is that the threat of incurring a loss because of the uncertain compensation would incentivize the principal (in our case, the MSS client) from shirking. However, previous analysis has shown that too much or too little uncertainty in the compensation does not induce the efficient outcomes (Mann and Wissink 1988).

Our research differs from these two streams of work in that we focus on bilateral instead of multilateral contracts and do not incorporate a random component in the outcome. Instead, we base our contract design on the negligence concept from the tort literature. The essential idea is that a fault determination mechanism can induce the potential injurer and victim to take precaution against a crime (Green 1976, Cooter and Ulen 1986, Rubinfeld 1987). For our bilateral contracts to work, we need one extra assumption: namely, the client's effort is verifiable after the security breach. This assumption is similar to the auditing requirement in Bhattacharya et al. (2014), where ex post knowledge facilitates the choice of contracts with different compensations. We further compare the efficiency of different bilateral liability-based contracts with varying verification requirements and under real-world constraints, such as limited liability and effort verification errors, and with multilateral contracts similar to the one proposed by Lee et al. (2013).

More broadly, this research is related to prior works on MSS design and configuration, such as the optimal ways to outsource prevention and detection functions (Cezar et al. 2014), when outsourcing security is better than cyber insurance (Zhao et al. 2013), choice of MSS networks or consortia (Gupta and Zhdanov 2012), pricing of MSSs in relation to transaction costs (Ding and Yurcik 2005), and how a client's outsourcing decision relates to the risks of the MSS provider going

bankrupt (Ding and Yurcik 2006) or the performance of the outsourcing contract (Ding et al. 2005). We extend this literature by studying the economic efficiency of a specific tool (viz bilateral liability-based contracts).

### 3. The Model

We consider an MSS provider offering a service contract to a client. The client will protect her system jointly with the provider if she accepts the contract. Otherwise, she has to undertake the protection herself. The contract lasts for a fixed period (often one year in the industry). The client's system faces a probability of security breach, which depends on three factors: the attack rate  $a \in [0, 1]$ , the client's protection effort  $q_k \in [0, 1]$ , and the provider's protection effort  $q_s \in [0, 1]$ . Let the breach probability be  $\mathcal{B}(a, q_k, q_s) \in [0, 1]$ , which is nonincreasing and convex in the client's efforts and the MSS provider's efforts (i.e.,  $\partial \mathcal{B} / \partial q_k \leq 0$ ,  $\partial \mathcal{B} / \partial q_s \leq 0$ ,  $\partial^2 \mathcal{B} / \partial q_k^2 \geq 0$ , and  $\partial^2 \mathcal{B} / \partial q_s^2 \geq 0$ ). The convexity in breach probability captures diminishing marginal returns in security protection (Moitra and Konda 2000, Gordon and Loeb 2002).

The client's and the MSS provider's costs of protection,  $\mathcal{C}_k(q_k) \geq 0$  and  $\mathcal{C}_s(q_s) \geq 0$ , are increasing and convex in effort (i.e.,  $\partial \mathcal{C}_k / \partial q_k > 0$ ,  $\partial \mathcal{C}_s / \partial q_s > 0$ ,  $\partial^2 \mathcal{C}_k / \partial q_k^2 \geq 0$ , and  $\partial^2 \mathcal{C}_s / \partial q_s^2 \geq 0$ ). For example, the client needs to deploy more workers if she wants to monitor a security operations center 24 hours a day and seven days a week instead of only during the office hours. The MSS provider also needs to incur a higher cost if it provides real time incident response service. We do not consider fixed cost because it may depend on the size of the client firm or the market or on the progress of technological development, none of which are the focus of this study.

The client enjoys a utility,  $v > 0$ , if her system is not breached and zero utility otherwise. The contract includes a compensation term,  $\beta \in [0, 1]$ , in the SLA. The MSS provider will compensate the client by  $\beta v$  if the client has contracted its service and her system is breached within the contract period. We study a static game where the client and the MSS provider make a single set of decisions—whether to collaborate in the protection, how much effort to invest in protecting the client's system, and the price and compensation terms involved. With a static game, we can interpret all functions and parameters as summary measures of what the client and the MSS provider expect throughout the game (Varian 2004, Grossklags et al. 2008, Lee et al. 2013). Table 2 lists the notations used in this paper.

We assume that all model functions and parameters are public knowledge, which is customary in the economics of information security literature (Gordon and Loeb 2002, Lee et al. 2013). Before investing in information security, firms often conduct risk assessment to estimate their vulnerabilities and measure



**Table 2.** Notations

Symbol	Definition
$m$	Number of clients in the market
$a$	Attack rate to a client's system
$v$	Payoff of a client's system
<b>Functions</b>	
$\mathcal{B}$	Breach probability
$\mathcal{C}_k$	Client's protection cost
$\mathcal{C}_s$	MSS provider's protection cost
<b>Decisions</b>	
$q_k$	Client's protection effort
$p$	Contract price
$\hat{\beta}$	Conditional compensation rate
$\bar{\beta}$	Variable liability constant
$q_s$	MSS provider's protection effort
$\beta$	Compensation rate
$T$	Effort requirement (threshold)
<b>Objectives</b>	
$w$	Social welfare
$u_0$	Client's utility from in-house protection
$u_1$	Client's utility from outsourcing
$\pi$	MSS provider's profit
<b>Benchmarks</b>	
$W^*$	First best social welfare
$U_0^*$	Client's reservation utility
$Q_k^*$	First best protection effort for client
$Q_s^*$	First best protection effort for MSS provider
<b>Extensions</b>	
$e$	Interdependency risk coefficient
$\lambda_k$	Client's weight of protection
$c_k$	Client's unit cost of protection
$\gamma$	Liability upper bound
$Q_k^{sb}$	Second best protection effort for the client
$\mathcal{L}_i$	Loss function with interdependency risk
$\lambda_s$	MSS provider's weight of protection
$c_s$	MSS provider's unit cost of protection
$\phi$	Price cap
$Q_s^{sb}$	Second best protection effort for the MSS provider

the costs and benefits of protection (Czarnik 2014, van Kessel and Allan 2014). For instance, they may determine breach probability by assessing the likelihood of threat event occurrence based on adversary intent, capability, and targeting together with the likelihood of nonadversarial threat event occurrence based on historical evidence and empirical data (NIST 2012). Note that our objective is to compare different liability-based MSS contracts. As is customary in economic analyses of outsourcing (Aksin et al. 2008, Dey et al. 2010, Jain et al. 2013), the precise measurement of the parameters and the construction of the contract terms are of secondary importance.

We first establish two benchmarks, the social planner's problem and in-house protection, that help assess the performance of the liability-based contracts later.

### 3.1. Social Planner's Problem

The social planner's objective function is

$$w = [1 - \mathcal{B}(a, q_k, q_s)]v - [\mathcal{C}_k(q_k) + \mathcal{C}_s(q_s)], \quad (1)$$

where  $[1 - \mathcal{B}(a, q_k, q_s)]v$  is the expected value of the system with protection and  $[\mathcal{C}_k(q_k) + \mathcal{C}_s(q_s)]$  is the total cost of protection. The first-order conditions are

$$\frac{\partial w}{\partial q_k} = -\frac{\partial \mathcal{B}}{\partial q_k}v - \frac{\partial \mathcal{C}_k}{\partial q_k} = 0, \quad (2)$$

$$\frac{\partial w}{\partial q_s} = -\frac{\partial \mathcal{B}}{\partial q_s}v - \frac{\partial \mathcal{C}_s}{\partial q_s} = 0. \quad (3)$$

We consider only interior solutions,  $Q_k^*$  and  $Q_s^*$ , which represent the client's and the MSS provider's first best efforts. Realistically, perfect security is unachievable. The cost of attaining an extreme level of security can outweigh the system's benefit, which is perhaps why information security professionals advocate balancing the portfolio of risk control strategies to include risk mitigation and transference in addition to risk reduction and prevention (Tipton and Krause 2007, Goldstein and Sood 2014).

With an interior solution, the first best efforts must satisfy Equations (2) and (3); that is,

$$-v \frac{\partial \mathcal{B}}{\partial q_k} \Big|_{(Q_k^*, Q_s^*)} = \frac{\partial \mathcal{C}_k}{\partial q_k} \Big|_{Q_k^*}, \quad (4)$$

$$-v \frac{\partial \mathcal{B}}{\partial q_s} \Big|_{(Q_k^*, Q_s^*)} = \frac{\partial \mathcal{C}_s}{\partial q_s} \Big|_{Q_s^*}. \quad (5)$$

Equations (4) and (5) suggest that the optimal social welfare is attained when the marginal benefit of protection equals marginal cost of protection. One notable challenge here is that the marginal benefit of protection involves another party's effort, meaning that coordination is necessary.

### 3.2. In-House Protection

If the client declines the MSS provider's service, then she has to develop the security protection in house.  $q_s$  becomes zero, and her expected utility from in-house protection is

$$u_0 = [1 - \mathcal{B}(a, q_k, 0)]v - \mathcal{C}_k(q_k). \quad (6)$$

The client's reservation utility  $U_0^*$  is the maximum value of  $u_0$  (i.e.,  $U_0^* = \max_{q_k} u_0$ ). This reservation utility serves as the reference for the client to decide whether to outsource.

### 3.3. Liability-Based Contracts

We now analyze the contractual agreement between the client and the MSS provider. The MSS provider first decides the contract price  $p$  and compensation rate  $\beta$ . If the client accepts the offer, then both she and the provider will put in efforts independently without knowing each other's effort. This resembles the case in the real world because, ex ante, before any security incident occurs, firms may lack the expertise or resources to verify the MSS provider's security effort or

quality (Schneier 2002, Ashford 2012). The expected utility from outsourcing for the client is

$$u_1 = [1 - \mathcal{B}(a, q_k, q_s)(1 - \beta)]v - \mathcal{C}_k(q_k) - p. \quad (7)$$

The MSS provider's profit from serving the client is

$$\pi = p - \mathcal{B}(a, q_k, q_s)\beta v - \mathcal{C}_s(q_s). \quad (8)$$

Because both  $u_1$  and  $\pi$  are concave, the client will maximize her utility based on the first-order condition of (7):

$$\frac{\partial u_1}{\partial q_k} = -\frac{\partial \mathcal{B}}{\partial q_k}v - \frac{\partial \mathcal{C}_k}{\partial q_k} + \frac{\partial(\mathcal{B}\beta)}{\partial q_k}v = 0. \quad (9)$$

Similarly, the MSS provider will maximize its profit based on the first-order condition of (8):

$$\frac{\partial \pi}{\partial q_s} = -\frac{\partial(\mathcal{B}\beta)}{\partial q_s}v - \frac{\partial \mathcal{C}_s}{\partial q_s} = 0. \quad (10)$$

By comparing with the social planner's problem in Section 3.1 (i.e., juxtaposing (2) with (9) and (3) with (10)), the sufficient conditions for a contract to induce socially optimal efforts are

$$\frac{\partial(\mathcal{B}\beta)}{\partial q_k} = 0, \quad (11)$$

$$\frac{\partial(\mathcal{B}\beta)}{\partial q_s} = \frac{\partial \mathcal{B}}{\partial q_s}. \quad (12)$$

Equation (11) says that the expected compensation rate  $\mathcal{B}\beta$  must be independent of the client's effort. Equation (12) says that the expected compensation rate and breach probability must have the same rate of change with respect to the MSS provider's effort. These conditions align the client's and the MSS provider's incentives by imposing liability for security breach on the MSS provider and restricting the compensation to the client. They form the cornerstone in designing optimal MSS contracts when the client and the MSS provider need to join effort in protecting the client's system.

Unlike the compensation rate, the contract price does not affect the equilibrium efforts. This is because the price is simply a means of rent allocation between the client and the MSS provider, which is not important for social welfare consideration. Because the MSS provider is offering a monopoly service, it will extract all surplus from the client. However, for the client to outsource, her expected utility must not be smaller than her reservation utility; therefore, we must have  $u_1 = U_0^*$ , which is a constant. Because social welfare is the sum of the client's and the MSS provider's utility (i.e.,  $w = \pi + u_1$ ), the MSS provider's problem is identical to the social planner's problem, giving rise to the following result.<sup>1</sup>

**Lemma 1.** *The MSS provider will choose a contract that maximizes the social welfare.*

Lemma 1 is consistent with previous studies (Lee et al. 2013, Zhao et al. 2013). Although the MSS provider's and social planner's interests are aligned, we may not get the first best outcome because the client may not choose the efficient protection after outsourcing. We next analyze three bilateral liability-based contracts and show that only two of them can lead to the first best outcome.

**3.3.1. Loss-Based Liability.** With a loss-based liability contract, the MSS provider compensates the client by a constant rate,  $\beta \in [0, 1]$ , if the client's system is breached after contracting its service. Referring to Table 1, this type of contract is common in the information security industry, where the MSS provider assumes an *unconditional* liability for the breach of the client's system. It is akin to the "no questions asked" type of warranty or insurance services offered in some conventional markets (e.g., rental car insurance).

The compensation rate is determined by the MSS provider and hence becomes a constant by the time that the client decides how much effort to invest. The sufficient conditions for optimal social welfare, (11) and (12), require  $\beta = 0$  or  $\partial \mathcal{B} / \partial q_k = 0$  and  $\beta = 1$  or  $\partial \mathcal{B} / \partial q_s = 0$ . Suppose that  $\partial \mathcal{B} / \partial q_k = 0$ . From (2),  $\partial w / \partial q_k$  becomes  $-\partial \mathcal{C}_k / \partial q_k < 0$ , meaning that social welfare is decreasing in the client's effort. Hence, the optimal client effort  $Q_k^* = 0$ . Similarly, suppose that  $\partial \mathcal{B} / \partial q_s = 0$ . From (3),  $\partial w / \partial q_s$  becomes  $-\partial \mathcal{C}_s / \partial q_s < 0$ , meaning that the optimal MSS provider effort  $Q_s^* = 0$ . This implies that the client will not outsource to the MSS provider. These results violate our assumption of interior first best efforts. In fact, if  $\partial \mathcal{B} / \partial q_k = 0$  or  $\partial \mathcal{B} / \partial q_s = 0$ , the protection can be optimally handled by a single agent. Such a problem has been well studied in the prior literature (Dey et al. 2010, Fitoussi and Gurbaxani 2012). Hence, we do not consider the case with either  $\partial \mathcal{B} / \partial q_k = 0$  or  $\partial \mathcal{B} / \partial q_s = 0$ . The social welfare maximization conditions, (11) and (12), then require  $\beta = 0$  and  $\beta = 1$ , which are obviously contradictory. This implies that a loss-based liability contract is always inefficient. Our first proposition follows.

**Proposition 1.** *When it is optimal for the client and the MSS provider to invest in security protection, the first best social welfare is not achievable with a loss-based liability contract.*

Proposition 1 is consistent with the literature showing that a loss-based liability contract is not efficient in a collaborative security protection setting (Lee et al. 2013). This is because assigning liability to only one party cannot induce the other party to work hard. Here, a high compensation rate encourages the client to shirk, but a low compensation rate encourages the MSS provider to shirk.

Nevertheless, when either  $Q_k^* = 0$  or  $Q_s^* = 0$ , a loss-based liability contract can be efficient. An example is the “best shot” protection, with which the breach probability (e.g.,  $\mathcal{B} = a[1 - \max(q_k, q_s)]$ ) depends only on the highest effort put in by the two involved parties (Varian 2004, Grossklags et al. 2008). The first best outcome can be achieved by letting the party with the highest benefit-cost ratio do all of the protection. For example, if the MSS provider has a cost advantage, a loss-based liability contract with  $\beta = 1$  is socially efficient. With this kind of configuration, however, the problem again reduces to a single-agent protection problem without involving collaboration.

Given the inefficiency of a loss-based liability contract, how can we incentivize the client and the MSS provider to contribute first best efforts? One solution is to introduce a third party. This is the spirit of the multilateral contract proposed by Lee et al. (2013), which requires the MSS provider to pay *other* clients but not the one whose system is breached. In the model by Lee et al. (2013), the clients will receive a “subsidy” from the MSS provider and the breached client if their own systems are not breached. This way, the MSS provider’s compensation is redistributed to some other third parties, but the clients have to work hard because their payoff is directly tied to the security of their own systems. Another example of a multilateral solution is “reverse insurance,” where a third party (usually the government) gives a lump sum payment amounting to the expected loss from a security breach to the client first; then the MSS provider compensates the third party when a security breach occurs.

Although a multilateral solution can induce optimal efforts in a collaborative setting, the need for a third party and transfer payments between the involved players is demanding. The transfer payments may also incur transaction costs and therefore could be socially costly. Here we explore if we can induce optimal efforts from the client and the MSS provider without enlisting a third party.

**3.3.2. Variable Liability.** We now consider a contract that distributes the liability between the MSS provider and the victim based on the extent of the victim’s negligence (or effort). This type of liability allocation is related to the concept of comparative negligence in tort law. The compensation function is usually a monotonic transformation of the client’s effort. The higher effort the client has invested, the more compensation she will receive. This type of contract is commonly used in insurance (e.g., Shavell 1979), and it adheres to the principle of proportionality in legal practice. The idea is akin to the use of variable rewards in security management. Nowadays, many firms offer “bug bounty” programs to reward white hat hackers for reporting security loopholes and patches. The reward is mostly

tied to the severity of the vulnerability and complexity of the solution. For example, Google runs a Patch Rewards Program that offers \$5,000 for moderately complex patches and \$10,000 for sophisticated improvements in security (Kirk 2014).

Note that to distribute the liability between the MSS provider and the client, we need to assume that the client’s effort is observable *after* the security breach. This is a realistic assumption because many organizations today keep detailed audit trails that can facilitate postbreach investigation using computer forensic techniques. It is also consistent with real-world observations. For example, the Target incident indicates that postbreach investigation can pin down the negligence of the outsourcing client. Premera Blue Cross, one of the largest health insurance providers in the state of Washington, was sued after a data breach incident in 2014 (Viebeck 2015). Federal auditors had warned the company three weeks before the breach about inadequate security procedures. The evidence could eventually determine whether Premera Blue Cross was negligent in its own protection.

When  $\beta$  depends on  $q_k$ , Equation (11) expands to  $\mathcal{B}\partial\beta/\partial q_k + \beta\partial\mathcal{B}/\partial q_k = 0$ , which is a first-order linear ordinary differential equation with solution  $\beta = \tilde{\beta}/\mathcal{B}$ , where  $\tilde{\beta}$  is a constant. By Lemma 1, the MSS provider prefers the first best outcome. Hence, it would choose  $q_s = Q_s^*$  and then incentivize the client to exert the first best effort through a proper construction of the function  $\beta = \tilde{\beta}/\mathcal{B}(a, q_k, Q_s^*)$  that satisfies Equations (11) and (12). This inverse proportionality between the compensation rate and breach probability follows the insurance literature, which addresses the moral hazard problem by designing an insurance coverage that equals the premium divided by the probability of having an accident (Shavell 1979). With this design, the expected coverage, which is the probability of having an adverse incident times the coverage, is always a constant.

Following a similar spirit, by Equation (12),  $\beta = 1$ , meaning that the MSS provider simply needs to set  $\tilde{\beta} = \mathcal{B}(a, Q_k^*, Q_s^*)$  to induce the first best effort from the client. Accordingly, the optimal compensation rate that satisfies Equations (11) and (12) at  $(Q_k^*, Q_s^*)$  is

$$\beta = \frac{\mathcal{B}(a, Q_k^*, Q_s^*)}{\mathcal{B}(a, q_k, Q_s^*)}, \quad (13)$$

where the numerator is the breach probability with efficient protection and the denominator is the breach probability given that  $q_s = Q_s^*$  and the client’s *actual* effort. Our next proposition follows.

**Proposition 2.** *The first best social welfare is achievable with a variable liability contract by setting the optimal-to-actual breach probability ratio as the compensation rate.*

The expected compensation rate  $\mathcal{B}\beta$  equals the breach probability with efficient protection, which is



a constant. This means that the client will not get extra benefit by reducing her effort because the MSS provider can penalize her according to the extent of her underinvestment. However, it may be difficult to implement a variable liability contract in practice because detailed assessment of security effort could be unduly complex. This is especially the case when the client is desperate in fighting the attack—useful data could be lost during the process, and the MSS provider may have little time to audit the client’s effort. Recent analysis suggests that some distributed denial-of-service (DDoS) attacks are launched to distract the incident response team so that it cannot discover other hidden and more sophisticated attacks (Kolochenko 2015). Such attack tactics make postbreach effort verification an even more difficult task.

**3.3.3. Threshold-based Liability.** Supposing that postbreach verification is difficult or costly, we next consider another contract that allocates the breach liability based on whether the client has invested enough effort (the “threshold”) to protect her system. This idea is similar to the concept of contributory negligence in tort law, which denies a victim from getting compensation if her damage is partly caused by her own negligence. Such threshold contracts seem to be common in the information technology (IT) industry. Referring to Table 1, IBM’s SLA stipulates that if the client’s contact information, network, or server was changed without notifying IBM in advance, any failure in detecting and reporting security incidents could be taken as an omission of the client and void the compensation (IBM 2008).

Formally, in a threshold-based liability contract, a compensation is provided only when the client’s effort exceeds a prespecified threshold  $T \in (0, 1]$ . Specifically,

$$\beta = \hat{\beta} \mathbf{1}_{q_k \geq T} = \begin{cases} \hat{\beta} & q_k \geq T, \\ 0 & q_k < T, \end{cases} \quad \hat{\beta} \in (0, 1], \quad (14)$$

where  $\hat{\beta}$  is the compensation rate conditional on the client meeting the threshold. If a security breach occurs and the client’s effort is found to be smaller than  $T$ , then the compensation rate  $\beta = 0$ . The MSS provider’s first-order condition in Equation (10) then becomes  $\partial\pi/\partial q_s = -\partial\mathcal{L}_s/\partial q_s < 0$ , meaning that it will invest zero effort. This means that the client will be better off choosing in-house protection. Hence, if the client chooses to outsource, she should invest at least  $T$  effort. Then Equation (12) will reduce to  $\hat{\beta} = 1$ , meaning that the MSS provider should offer full compensation. This, however, violates Equation (11) because  $\partial\mathcal{B}/\partial q_k \neq 0$ . Furthermore, following Equation (9),  $\partial u_1/\partial q_k$  will reduce to  $-\partial\mathcal{L}_k/\partial q_k < 0$ , and hence, the client’s utility will decrease with her effort. Therefore, the client will invest exactly  $T$  and not more than  $T$  effort. Taken together, the threshold-based liability contract is efficient with

$T = Q_k^*$  and  $\hat{\beta} = 1$ , conditional on the client meeting the threshold effort (i.e.,  $Q_k^*$ ).

**Proposition 3.** *The first best social welfare is achievable with a threshold-based liability contract by setting the client’s first best effort as the threshold and providing conditional full compensation.*

With loss-based liability, a high compensation would induce the MSS provider but not the client to work hard. With threshold-based liability, other than the compensation (which incentivizes the MSS provider to work hard), a threshold is used to force the client to put in the first best effort. Essentially, the MSS provider sets up the protection efforts for itself and the client. For such a contract to work, we need to add an additional contract term specifying the minimum protection from the clients.

### 3.4. Effort Verification Error

In the analysis in Sections 3.3.2 and 3.3.3, we assume that the MSS provider can verify the client’s effort after the security breach. Realistically, this effort verification could be costly and hence, erroneous because of strategic behavior of the attacker or the quality of the auditor. For example, the attacker may deliberately remove the log files and all traces of the attack and protection to cover their paths (Graves 2010). In such a case, the client’s effort may be understated in the audit report if the security configurations or policies are modified. To critically compare the performance of the variable liability contract and the threshold-based liability contract, we introduce an error so that the audited client’s effort after the breach  $\tilde{q}_k$  follows a uniform distribution with limit  $[q_k - \varepsilon, q_k]$ , where  $\varepsilon$  is a small error. Note that we assume the audited effort does not exceed the actual effort because effort estimation is often conservative. For instance, the auditor may verify only the security operations contained in a checklist. It may omit the efforts invested beyond the checklist, leading to underestimation of the invested effort.

Recall from Section 3.3.2 that to achieve the efficient outcome with a variable liability contract, the expected compensation rate  $\mathcal{B}\beta$  must equal the breach probability with the efficient protection, which is a constant. With verification errors, for  $q_k \geq \varepsilon$ , the expected compensation rate accounting for breach probability is

$$\begin{aligned} E(\mathcal{B}\beta) &= \int_{q_k - \varepsilon}^{q_k} \frac{\mathcal{B}(a, q_k, q_s)\beta(\tilde{q}_k)}{\varepsilon} d\tilde{q}_k \\ &= \frac{\mathcal{B}}{\varepsilon} [G(q_k) - G(q_k - \varepsilon)], \end{aligned} \quad (15)$$

where

$$G(q_k) = \int \beta(\tilde{q}_k) d\tilde{q}_k \quad (16)$$

and  $\partial G/\partial q_k = \beta$ . Equation (15) results because the actual breach probability  $\mathcal{B}(a, q_k, q_s)$  and the error limit  $\varepsilon$  do not depend on the audited client effort  $\tilde{q}_k$ ; hence, they can be taken out of the integral. In most cases, the term  $\mathcal{B}[G(q_k) - G(q_k - \varepsilon)]$  in Equation (15) depends on  $q_k$ , which means that the client's effort will always influence the expected compensation rate. This violates the necessary condition for efficiency in Equation (13). Accordingly, the variable liability contract will mostly not give the efficient outcome when effort verification errors exist.<sup>2</sup>

With threshold-based liability, the expected compensation rate with effort verification errors is

$$E(\beta) = S \int_{q_k - \varepsilon}^{q_k} 1_{\tilde{q}_k \geq T} \frac{\hat{\beta}}{\varepsilon} d\tilde{q}_k. \quad (17)$$

If we apply the outcome from the case without verification errors (i.e.,  $T = Q_k^*$ ,  $\hat{\beta} = 1$ , and  $q_k = Q_k^*$ ), the expected compensation will become zero. This will change the outcome because the MSS provider will always shirk when it expects to pay zero compensation. To address this, we can reduce the threshold to some  $T = Q_k^* - \varepsilon$  so that the expected compensation rate will remain 100% at  $q_k = Q_k^*$ . In this case, the client may still get compensation when the audited effort  $\tilde{q}_k > Q_k^* - \varepsilon$ . Specifically, given  $T = Q_k^* - \varepsilon$ ,  $\hat{\beta} = 1$ , and  $q_k \in [Q_k^* - \varepsilon, Q_k^*]$ , the expected compensation rate will become

$$E(\beta) = \int_{q_k - \varepsilon}^{q_k} 1_{\tilde{q}_k \geq Q_k^* - \varepsilon} \frac{1}{\varepsilon} d\tilde{q}_k = 1 - \frac{Q_k^* - q_k}{\varepsilon}. \quad (18)$$

To ensure that the client does not deviate from the efficient effort, her utility should be increasing in  $q_k \in [Q_k^* - \varepsilon, Q_k^*]$ . Note that the client's utility is concave in this region,

$$\frac{\partial^2 u_1}{\partial q_k^2} = - \left( \frac{Q_k^* - q_k}{\varepsilon} \right) \frac{\partial^2 \mathcal{B}}{\partial q_k^2} v - \frac{\partial^2 \mathcal{C}_k}{\partial q_k^2} + \frac{\partial \mathcal{B}}{\partial q_k} \frac{v}{\varepsilon} < 0, \quad (19)$$

and it is always increasing beyond  $q_k = Q_k^* - \varepsilon$ ,

$$\frac{\partial u_1}{\partial q_k} \Big|_{(Q_k^* - \varepsilon)^+} = - \frac{\partial \mathcal{B}}{\partial q_k} v - \frac{\partial \mathcal{C}_k}{\partial q_k} + \frac{\mathcal{B}v}{\varepsilon} > 0. \quad (20)$$

Now consider the first-order derivative of the utility below  $q_k = Q_k^*$ ,

$$\frac{\partial u_1}{\partial q_k} \Big|_{(Q_k^*)^-} = - \frac{\partial \mathcal{C}_k}{\partial q_k} + \frac{\mathcal{B}v}{\varepsilon}, \quad (21)$$

the sign of which depends on the error. When this derivative is also positive, the client's utility will always increase in  $q_k \in [Q_k^* - \varepsilon, Q_k^*]$ , meaning that she will choose  $q_k = Q_k^*$ . Therefore, the socially optimal condition in a

threshold-based liability contract with effort verification errors is

$$\varepsilon < \frac{\mathcal{B}v}{\partial \mathcal{C}_k / \partial q_k} \Big|_{(Q_k^*, Q_k^*)} = \frac{\mathcal{B}}{-\partial \mathcal{B} / \partial q_k} \Big|_{(Q_k^*, Q_k^*)} \equiv \hat{\varepsilon}. \quad (22)$$

The upper bound  $\hat{\varepsilon}$  that maintains the client's incentive to contribute  $q_k = Q_k^*$  depends on the scale of the breach probability relative to the client's protection efficiency at the socially optimal level of protection. If the breach probability is high or the client's protection is less efficient, then  $\hat{\varepsilon}$  will increase, meaning that the threshold-based liability contract can tolerate more error because the client's effort is less influential. In the extreme case, if  $\hat{\varepsilon} \geq Q_k^*$ , the threshold-based liability contract is efficient even if the error is large. The MSS provider can simply grant a compensation when the client's effort is positive.

Note that the effort verification error introduces payoff uncertainty to the client. Prior research has shown that such payoff uncertainty could incentivize the client to contribute effort and lead to socially optimal outcomes in some settings (Mann and Wissink 1988). Here we show that this is indeed the case with threshold-based liability contract but not with variable liability contract.

To conclude this section, we find that threshold-based liability contract is more resilient to error in the sense that it can still lead to the socially optimal outcome when the realized verification error is not excessively large. It is also easier to implement than a variable liability contract because it requires less postbreach verification. It is perhaps not surprising that it is more preferred as shown in Table 1. In the remaining analysis, we focus on the threshold-based liability contract. The corresponding analysis for the variable liability contract is available in the online appendix.

#### 4. Interdependent Clients

We now examine the performance of the variable liability contract and the threshold-based liability contract in another extension (viz when the clients are interconnected because of the outsourcing) (Hui et al. 2013). Realistically, when multiple computer systems are connected to a single hub, additional risks may arise because the hub introduces a single point of failure. The damage from the breach of one system may propagate to the other systems on the same network. An example is the Dark Seoul incident on March 20, 2013, in Korea. The attacker spread a malware via the patch management system of AhnLab, a security software provider, with compromised user accounts to AhnLab's other clients (Schwartz 2013). In general, collaborative MSSs may create negative externalities among the clients because the compromise of any one client's system may cause inconvenience to the entire network because of postbreach investigation and system reconciliation. This type of propagated risk is also prevalent in software

as a service (August et al. 2014) or, more broadly, any connected systems (Zhao et al. 2013).

To incorporate this system interdependency risk, we consider a market with  $m$  homogeneous clients. We assume that a breached client in the MSS provider's network will cause all other clients in the same network to incur an expected loss:  $ev$ ,  $e \leq 1$ . We further assume this loss to be sufficiently small so that the market is fully covered, which means that serving the  $m$ th client yields a nonnegative marginal profit to the MSS provider. The expected utility from in-house protection will remain the same as in (6) because clients who do not outsource will not be affected by the outsourcing clients and the MSS provider. Hence, the clients' reservation utility is still  $U_0^*$ . The social welfare now becomes

$$w = \sum_{i=1}^m [(1 - \mathcal{L}_i)v - \mathcal{C}_k(q_{ki}) - \mathcal{C}_s(q_{si})], \quad (23)$$

where  $\mathcal{L}_j = \mathcal{B}(a, q_{kj}, q_{sj}) + e \sum_{i=1, i \neq j}^m \mathcal{B}(a, q_{ki}, q_{si})$ . Similar to the baseline model in Section 3, the first best efforts with the externalities ( $Q_{ke}^*, Q_{se}^*$ ) should satisfy the first-order conditions of (23):

$$-[1 + e(m - 1)]v \frac{\partial \mathcal{B}}{\partial q_{kj}} \Big|_{(Q_{ke}^*, Q_{se}^*)} = \frac{\partial \mathcal{C}_k}{\partial q_{kj}} \Big|_{Q_{ke}^*}, \quad (24)$$

$$-[1 + e(m - 1)]v \frac{\partial \mathcal{B}}{\partial q_{sj}} \Big|_{(Q_{ke}^*, Q_{se}^*)} = \frac{\partial \mathcal{C}_s}{\partial q_{sj}} \Big|_{Q_{se}^*}. \quad (25)$$

Comparing these first-order conditions with those from the baseline model (i.e., (4) with (24) and (5) with (25)), the main difference is that the marginal benefit is now multiplied by  $[1 + e(m - 1)]$  when interdependency risk is present.

With outsourcing, client  $j$ 's expected utility is

$$u_{1j} = v - (1 - \beta_j)\mathcal{L}_j v - \mathcal{C}_k(q_{kj}) - p_j, \quad (26)$$

and the MSS provider's total profit from serving the  $m$  clients is

$$\pi = \sum_{i=1}^m [p_i - \beta_i \mathcal{L}_i v - \mathcal{C}_s(q_{si})]. \quad (27)$$

Here again, the client will maximize her utility based on the first-order condition of (26):

$$\frac{\partial u_{1j}}{\partial q_{kj}} = -(1 - \beta_j) \frac{\partial \mathcal{B}}{\partial q_{kj}} v + \mathcal{L}_j \frac{\partial \beta_j}{\partial q_{kj}} v - \frac{\partial \mathcal{C}_k}{\partial q_{kj}} = 0. \quad (28)$$

The MSS provider will maximize its profit based on the  $m$  first-order conditions of (27):

$$\frac{\partial \pi}{\partial q_{sj}} = -\left(\beta_j + e \sum_{i=1, i \neq j}^m \beta_i\right) \frac{\partial \mathcal{B}}{\partial q_{sj}} v - \mathcal{L}_j \frac{\partial \beta_j}{\partial q_{sj}} v - \frac{\partial \mathcal{C}_s}{\partial q_{sj}} = 0, \quad (29)$$

$$j = 1 \dots m.$$

By comparing (24) with (28) and (25) with (29), the liability contract leads to socially optimal outcomes when the following sufficient conditions are satisfied at ( $Q_{ke}^*, Q_{se}^*$ ):

$$\mathcal{L}_j \frac{\partial \beta_j}{\partial q_{kj}} = -[\beta_j + e(m - 1)] \frac{\partial \mathcal{B}}{\partial q_{kj}}, \quad (30)$$

$$\mathcal{L}_j \frac{\partial \beta_j}{\partial q_{sj}} = \left[ (1 - \beta_j) + e \sum_{i=1, i \neq j}^m (1 - \beta_i) \right] \frac{\partial \mathcal{B}}{\partial q_{sj}}. \quad (31)$$

Condition (31) depends on the compensations made to the other clients. With homogeneous clients, the MSS provider will offer the same contract to all clients (i.e.,  $\beta_i = \beta_j$ ). Equation (31) then simplifies to  $\mathcal{L}_j \partial \beta_j / \partial q_{sj} = (1 - \beta_j)[1 + e(m - 1)] \partial \mathcal{B} / \partial q_{sj}$ .

With a loss-based liability contract, Equations (30) and (31) can be simplified to  $\beta_j = -e(m - 1)$  and  $\beta_j = 1$  because the compensation rate  $\beta_j$  is a constant,  $\partial \mathcal{B} / \partial q_{kj} \neq 0$ , and  $\partial \mathcal{B} / \partial q_{sj} \neq 0$ . These two conditions are contradictory because  $-e(m - 1) < 0$ . This implies that loss-based liability contract continues to be inefficient with system interdependency risk.

Interestingly, condition (30) suggests that the client should pay compensation to the other clients when a breach occurs because  $\beta_j = -e(m - 1) < 0$ . This counterintuitive result arises because the client will only consider her own loss from security breach when deciding how much to invest in the protection. The loss owing to system interdependency is orthogonal to the client's effort (i.e.,  $\partial \mathcal{L}_j / \partial q_{kj} = \partial \mathcal{B} / \partial q_{kj}$ ). Therefore, the client will underprotect her system, even if no compensation is provided on security breach. By contrast, the MSS provider will internalize the system interdependency risk because its profit is directly tied to the security of *every* client. Hence, having full compensation should be sufficient to induce the MSS provider to exert first best efforts. This is similar to the case in Section 3.

With threshold-based liability, the outsourcing clients will invest at least  $T_j$  effort to prevent the MSS provider from shirking. By (31), the MSS provider will choose  $\hat{\beta}_j = 1$  and exert the socially efficient effort. Here again, the client will not invest more than  $T_j$  effort because, by (28),  $\partial u_{1j} / \partial q_{kj}$  will become  $-\partial \mathcal{C}_k / \partial q_{kj} < 0$ , meaning that her utility is decreasing in effort. Hence, the MSS provider will specify  $T_j = Q_{ke}^*$  in the contract to force the client to choose the first best effort, which collectively leads to the socially optimal outcome. This result is similar to the one from the basic model, except that now the threshold is changed from  $Q_k^*$  to  $Q_{ke}^*$  to account for the system interdependency risk.

Similarly, our analysis shows that the variable liability contract could also yield the socially optimal outcome. We present the proof in the online appendix. To sum up, our main findings from the baseline model

are robust to accounting for system interdependency risks. The following proposition summarizes the results with system interdependency.

**Proposition 4.** *In the presence of system interdependency risks, first best social welfare is not achievable with a loss-based liability contract. It is achievable with a threshold-based liability contract with conditional full compensation or a variable liability contract with the compensation rate equal to the optimal-to-actual breach probability ratio capped at 100% (i.e.,  $\beta_j = \min\{\mathcal{B}(a, Q_{ke}^*, Q_{se}^*)/\mathcal{B}(a, q_{kj}, Q_{se}^*), 1\}$ ).*

## 5. Security Breach Scenarios

In practice, the MSS provider's and the client's efforts may interact with each other. The efforts could be complementary or substitutes, which lead to different breach outcomes. In this section, we analyze the performance of the bilateral liability-based contracts under three common scenarios: total effort (Varian 2004, Grossklags et al. 2008) and serial and parallel configurations (Lee et al. 2016). In the total effort scenario, the client and the MSS provider are each responsible for protecting a separate part of the client's system. In other words, their efforts do not interact with each other. With a serial configuration, the attacker needs to penetrate both the client's and the MSS provider's protection to compromise the system. Hence, their protection efforts are substitutes. With a parallel configuration, the attacker needs to penetrate either the client's or the MSS provider's protection to breach the client's system. Hence, their protection efforts are complementary.

The total effort configuration reflects a scenario where the client and the MSS provider are applying independent controls to protect the system (e.g., when the system is partitioned). One example is when the client outsources the protection of nonsensitive data to the MSS provider and develops protection of sensitive data herself. Another example is the protection of mirrored systems (Grossklags et al. 2008). The MSS provider would save copies of the client's data and propagate them through its content delivery network. The usability, performance, and robustness of the entire system depend on the security of each of the mirrors in the network. One party's bandwidth is independent of the other party's bandwidth, and therefore, the attacker has to consume all bandwidths from all parties to disrupt the service entirely.

With total effort configuration, the breach function depends on the weighted sum of the client's and the MSS provider's efforts,

$$\mathcal{B}(a, q_k, q_s) = a(1 - \lambda_k q_k - \lambda_s q_s), \quad (32)$$

where  $\lambda_k$  and  $\lambda_s$  are the weights of protection for the client and the MSS provider, with  $\lambda_k + \lambda_s = 1$ ,  $\lambda_k, \lambda_s \neq 0$ . One characteristic of this configuration is that

the marginal benefit of protection is *independent* of the other party's effort (i.e.,  $\partial^2 \mathcal{B} / \partial q_k \partial q_s = 0$ ). This means that even if one party shirks, the other party's effort will remain effective. Hence, the client will exert first best effort during in-house protection, although the provider's effort is missing, and hence, the overall security is socially suboptimal. We compare the contract performance by applying (32) and a quadratic cost function (i.e.,  $\mathcal{C}_k(q_k) = c_k q_k^2 / 2$  and  $\mathcal{C}_s(q_s) = c_s q_s^2 / 2$ ) to our baseline model in Section 3. The first column of Table 3 presents the outcomes. Both the threshold-based liability contract and the variable liability contract are efficient, whereas the loss-based liability contract is not.

With a loss-based liability contract, the optimal compensation balances both parties' protection weights and unit costs. The optimal efforts are *fractions* of the first best efforts depending on the chosen compensation rate. In general, when the MSS provider has higher protection weight and cost advantage, the compensation rate will exceed 50%, and the client will shirk more than the MSS provider. For instance, when software vulnerability assessment is outsourced with a loss-based liability contract, the client-side security testers may shirk because they expect that the external testers will handle the job. However, the external testers will also tend to shirk because they do not bear the full liability for assessment failure. The client-side testers will work hard only if they cannot shift the blame to the MSS provider, which is the case with a threshold-based liability contract or a variable liability contract.

Interestingly, a loss-based liability contract is socially efficient under a specific scenario where the system is partitioned and the system's payoff is separable (i.e.,  $\lambda_k v$  if the client's part is not breached and  $\lambda_s v$  if the MSS provider's part is not breached). In such a case, the MSS provider should compensate  $\lambda_s v$  only if its part is breached, which is essentially the full compensation.

With serial configuration, the attacker needs to penetrate both the client's and the MSS provider's protection to compromise the system. Such a setting applies when controls from both parties serve similar purposes, such as the concept of "defense in depth," where the system is protected with multiple layers of redundant security controls. For example, to defend against phishing or malicious email attachments, the client could use email filtering services from the MSS provider and install antivirus software on her own system. To penetrate the client's system, the attacker would need to circumvent both the filtering system from the MSS provider and the antivirus software. However, adding antivirus software on top of the filtering system has lower marginal benefit than when the software is used alone because the MSS provider's filtering system should have already removed most malicious emails.



**Table 3.** Contract Performance Under Different Security Configurations

Breach function (cost function)	Total effort (quadratic)	Serial configuration (quadratic)	Parallel configuration (cubic)
Social planner's problem			
Client's effort $Q_k^*$	$\frac{\lambda_k av}{c_k}$	$\frac{av(c_s - av)}{c_k c_s - (av)^2}$	$\frac{av}{c_k^{2/3} c_s^{1/3}}$
MSS provider's effort $Q_s^*$	$\frac{\lambda_s av}{c_s}$	$\frac{av(c_k - av)}{c_k c_s - (av)^2}$	$\frac{av}{c_k^{1/3} c_s^{2/3}}$
Welfare $W^*$	$(1-a)v + \left[ \frac{(\lambda_k av)^2}{2c_k} + \frac{(\lambda_s av)^2}{2c_s} \right]$	$(1-a)v + \frac{(av)^2(c_k + c_s - 2av)}{2[c_k c_s - (av)^2]}$	$(1-a)v + \frac{(av)^3}{3c_k c_s}$
Bilateral loss-based liability			
Compensation rate $\beta^*$	$\frac{\lambda_s^2 c_k}{\lambda_k^2 c_s + \lambda_s^2 c_k}$	Solution of $\beta^* c_k (c_s - \beta^* av)^2 = (1 - \beta^*) c_s [c_k - (1 - \beta^*) av]^2$	$\frac{1}{2}$
Client's effort $q_k^*$	$(1 - \beta^*) Q_k^*$	$\frac{(1 - \beta^*) av (c_s - \beta^* av)}{c_k c_s - \beta^* (1 - \beta^*) (av)^2}$	$\frac{Q_k^*}{2}$
MSS provider's effort $q_s^*$	$\beta^* Q_s^*$	$\frac{\beta^* av [c_k - (1 - \beta^*) av]}{c_k c_s - \beta^* (1 - \beta^*) (av)^2}$	$\frac{Q_s^*}{2}$
Welfare loss $W^* - w^*$	$\frac{(\lambda_k \lambda_s av)^2}{2(\lambda_k^2 c_s + \lambda_s^2 c_k)}$	No explicit expression	$\frac{(av)^3}{6c_k c_s}$
Threshold-based liability			
Compensation rate $\beta^*$	$\mathbf{1} q_k \geq \frac{\lambda_k av}{c_k}$	$\mathbf{1} q_k \geq \frac{av(c_s - av)}{c_k c_s - (av)^2}$	$\mathbf{1} q_k \geq \frac{av}{c_k^{2/3} c_s^{1/3}}$
Client's effort $q_k^*$	$\frac{\lambda_k av}{c_k}$	$\frac{av(c_s - av)}{c_k c_s - (av)^2}$	$\frac{av}{c_k^{2/3} c_s^{1/3}}$
MSS provider's effort $q_s^*$	$\frac{\lambda_s av}{c_s}$	$\frac{av(c_k - av)}{c_k c_s - (av)^2}$	$\frac{av}{c_k^{1/3} c_s^{2/3}}$
Welfare loss $W^* - w^*$	0	0	0
Variable liability			
Compensation rate $\beta^*$	$\frac{c_k c_s - (\lambda_k^2 c_s + \lambda_s^2 c_k) av}{c_k c_s (1 - \lambda_k q_k) - \lambda_s^2 c_k av}$	$\frac{c_s (c_k - av)}{[c_k c_s - (av)^2] (1 - q_k)}$	$\frac{c_k c_s - av}{c_k c_s - c_k^{2/3} c_s^{1/3} av q_k}$
Client's effort $q_k^*$	$\frac{\lambda_k av}{c_k}$	$\frac{av(c_s - av)}{c_k c_s - (av)^2}$	$\frac{av}{c_k^{2/3} c_s^{1/3}}$
MSS provider's effort $q_s^*$	$\frac{\lambda_s av}{c_s}$	$\frac{av(c_k - av)}{c_k c_s - (av)^2}$	$\frac{av}{c_k^{1/3} c_s^{2/3}}$
Welfare loss $W^* - w^*$	0	0	0

Unlike total effort protection, the client's and the MSS provider's security controls are dependent in a serial configuration. The breach probability

$$\mathcal{B}(a, q_k, q_s) = a(1 - q_k)(1 - q_s). \quad (33)$$

In particular,  $\partial^2 \mathcal{B} / \partial q_k \partial q_s = \partial^2 \mathcal{B} / \partial q_s \partial q_k = a$ , meaning that the client's and the MSS provider's efforts are *strategic substitutes*. This implies that the marginal benefit from protection *decreases* in the other party's effort. In the extreme case, when one party exerts full effort, the other party will not need to do any protection because the breach probability will be zero.

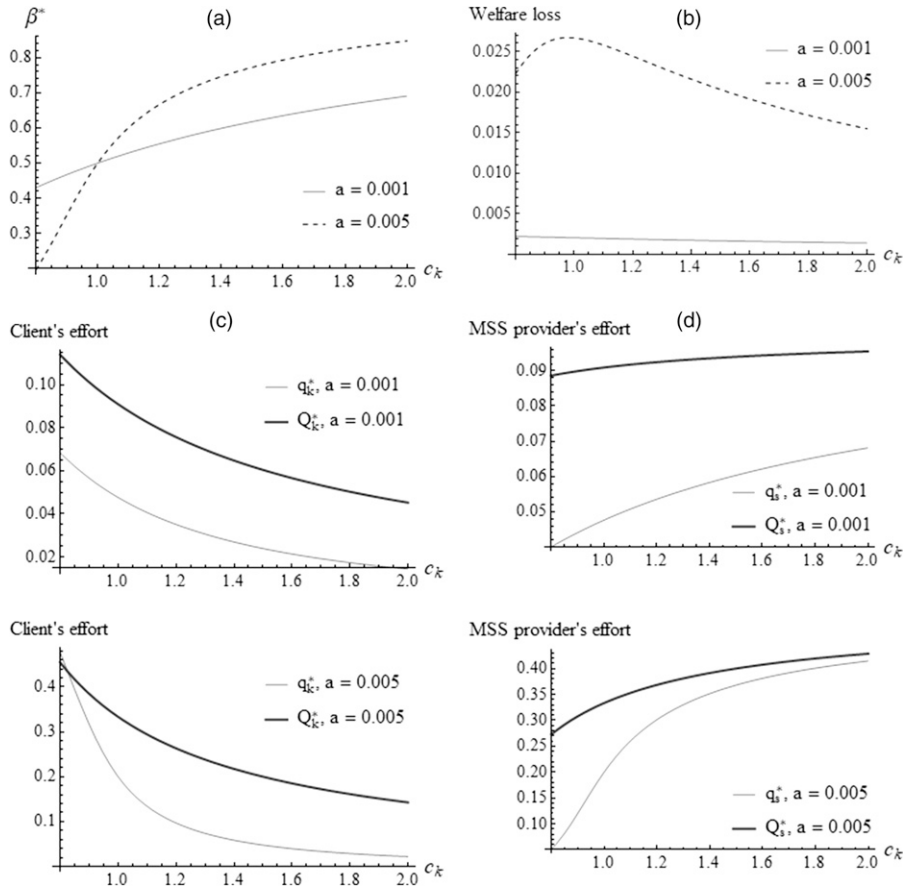
With (33), we compare the contract performance in Table 3. A loss-based liability contract is again inefficient, whereas the variable liability contract and the threshold-based liability contract yield first best outcomes. To illustrate this, we plot the variables from Table 3 with different  $a$  and  $c_k$  by fixing  $v = 100$  and  $c_s = 1$  in Figure 1. In many cases, both parties will underinvest protection under a loss-based liability contract. This underinvestment is more severe when one has some cost

disadvantage and the expected loss is high, which makes the other party more efficient in security protection.

To illustrate this inefficiency, consider a client adopting a cloud-based web application firewall (WAF) from the MSS provider to fulfill the Payment Card Industry Data Security Standard (PCI DSS) (Beaver 2011). The client may undertake other controls to protect her system. Because of expertise and experience, the MSS provider is likely to be better in managing security controls. Our result then suggests that because the client is less efficient than the MSS provider, it will more likely free ride on the WAF under a loss-based liability contract. This defeats the purpose of having redundant controls.

With parallel configuration, the attacker needs to penetrate *either* the client's or the MSS provider's protection to compromise the system. Realistically, a parallel configuration may exist when the system is subject to multiple attack paths. For example, to secure sensitive data in a system, the client could contract a network intrusion detection system from the MSS provider and introduce internal security policies, such as blocking

**Figure 1.** Loss-Based Liability Contracts in Serial Configuration



Note. Parameters:  $v = 100$ ,  $c_s = 1$ ,  $\mathcal{B} = a(1 - q_k)(1 - q_s)$ .

USB ports to restrict data access. However, when one of two controls is compromised, the attacker will gain full access to the system.

In this scenario, the breach probability depends on both parties' efforts:

$$\mathcal{B}(a, q_k, q_s) = a(1 - q_k q_s). \quad (34)$$

The efforts are *strategic complements* here because  $\partial^2 \mathcal{B} / \partial q_k \partial q_s = \partial^2 \mathcal{B} / \partial q_s \partial q_k = -a$ . Even if one party protects the system fully, the breach probability will remain positive if the other party does not work hard. If one party shirks, the protection will fail completely, and the breach probability will become identical to the attack rate. Hence, in-house protection becomes infeasible. The client's reservation utility is simply  $U_0^* = (1 - a)v$ .

We apply (34) and adopt a cubic cost function<sup>3</sup> (i.e.,  $\mathcal{C}_k(q_k) = c_k q_k^3 / 3$  and  $\mathcal{C}_s(q_s) = c_s q_s^3 / 3$ ) into the baseline model in Section 3. The results are shown in the last column of Table 3. Both the threshold-based liability contract and the variable liability contract are efficient with full compensation. The compensation rate in a loss-based liability contract is always 50%, which suggests that both parties should share the same amount of liability, even if one party's protection is less

cost-effective. This is because the security level in a parallel configuration is heavily influenced by the weakest link, and setting equal liability could minimize this impact. Similarly, the client's and the MSS provider's efforts in a loss-based liability contract are always one-half of their corresponding first best efforts.

In summary, the variable liability contract and threshold-based liability contract always give the first best outcomes under different security configurations. Loss-based liability contract does not perform as well except in the total effort configuration, where the system can be partitioned and breaching the outsourced part does not affect the in-house part. Table 4 summarizes these results.

## 6. Limited Liability

In practice, the MSS provider often cannot fully compensate for the value of a system to the client because the system can worth billions of dollars (e.g., a bank's system may contain millions of credit-card numbers and mission-critical transaction processing systems). In practice, many providers set a liability limit up to 12 months of the security service revenue (Overby 2012). To examine how the bilateral liability-based contracts

**Table 4.** Summary of Security Outsourcing Scenario

Breach function (effort interaction)	Total effort (independent)	Serial configuration (strategic substitute)	Parallel configuration (strategic complement)
Sample scenarios	Partition and outsource: outsource the protection of a subsystem (e.g., nonsensitive data) and protect the remaining part in house Mirrored system: both parties independently protect a mirrored system (e.g., a website), and the availability of this system depends on total effort	Defense in depth: both parties apply redundant controls to secure a system	Multiple attack paths: security breach occurs if either party's security control is compromised Acquire and configure: the client acquires a security appliance from the MSS provider, which is effective only if the client spends effort in proper configuration
Contract comparison			
Bilateral loss-based liability	Socially efficient if the system can be partitioned; inefficient otherwise	Socially inefficient: both parties shirk; the party with cost-disadvantage and high expected loss will shirk more	Socially inefficient: effort and social welfare are halved
Threshold-based liability	Socially efficient	Socially efficient	Socially efficient
Variable liability	Socially efficient	Socially efficient	Socially efficient

perform under such a limit, we introduce an exogenous constraint that caps the compensation rate,  $\gamma \in (0, 1)$ .<sup>4</sup> The MSS provider would only offer a compensation rate  $\beta$  between zero and  $\gamma$ . Referring to Propositions 2 and 3, both the threshold-based liability contract and the variable liability contract require full compensation to induce first best efforts. Therefore, the upper bound  $\gamma < 1$  will immediately lead to inefficiency, as implied in previous analyses (e.g., Lee et al. 2013).

The MSS provider often does not have full control of the liability upper bound. Otherwise, it will simply set  $\gamma = 1$  and provide full compensation to obtain the maximum profit. To reflect this constraint, we treat  $\gamma$  as an exogenous variable. One explanation of this limited liability is the MSS provider's budget constraint—it can afford to pay only a fixed amount to each client because the full outcome of the breach is simply unbearable. In this case, the liability upper bound will equal  $\gamma$ , and the compensation cap is  $\gamma v$ . As one real-world example, in IBM's premium MSS, the clients will be compensated by up to \$50,000 per month for any security breaches.

Another explanation of limited liability is client-side budget constraint. As noted by Overby (2012), the service price with unlimited liability (i.e., full compensation) skyrockets, which discourages firms from outsourcing their security operations, especially when the budget is limited. Firms may negotiate for a lower price and accept the service only when the price is no greater than a certain value (e.g.,  $p \leq \phi$ ). This setting is compatible with the general liability upper bound  $\gamma \in (0, 1)$  because the service price is always set at such a level that  $u_1 = U_0^*$  to extract all surplus from the client. Specifically, by rearranging the terms in Equation (7), the equilibrium price is

$$p^* = [1 - \mathcal{B}(a, q_k^*, q_s^*)(1 - \beta^*)]v - \mathcal{C}_k(q_k^*) - U_0^*, \quad (35)$$

where  $q_k^*$  and  $q_s^*$  are functions of the compensation rate  $\beta^*$ . Therefore, the price is always a function of the compensation rate (i.e.,  $p^* = f(\beta^*)$  for some function). If the price cap is  $\phi$ , the liability upper bound will be a function of the price cap or  $\gamma = f^{-1}(\phi)$ . Hence, technically, imposing a price cap has the same effect as imposing a limited liability.

One special case of limited liability is compensation based on price, which is prevalent in practice as shown in Table 1. Because the price is a function of compensation rate, the liability upper bound will be the root of  $\beta v = p$  with respect to  $\beta$ . Unlike a simple limited liability or a price cap, the liability upper bound is always smaller than one with price-based compensation. Otherwise, if the compensation rate is one, the price should be set at  $v$  to fulfill  $\beta v = p$ . From Equation (7), the client's utility from outsourcing  $u_1$  will then become nonpositive, which cannot exceed the reservation utility  $U_0^* \geq 0$ .

In summary, we can consider limited liability as a constraint on the compensation rate or the price. For simplicity and without loss of generality, we model limited liability by the compensation upper bound  $\gamma$ , which is qualitatively similar to a price cap.

In general, the MSS provider's problem is the same as the social welfare maximization problem, with the compensation rate being the key decision variable

$$\max_{\beta} [1 - \mathcal{B}(a, q_k(\beta), q_s(\beta))]v - [\mathcal{C}_k(q_k(\beta)) + \mathcal{C}_s(q_s(\beta))], \quad (36)$$

where the efforts are functions of the compensation rate. Suppose that the social welfare function in (36) is quasiconcave in  $\beta$ , which is the case for the total effort, serial, and parallel configurations. If the liability upper bound is higher than the optimal compensation rate (i.e.,  $\gamma \geq \beta^*$ ), then the MSS provider will simply choose  $\beta^*$ .

Otherwise, it will choose  $\beta = \gamma$ . Then its profit maximization problem is governed by the first-order condition of (8) with  $\beta = \gamma$ ; that is,

$$\frac{\partial \pi}{\partial q_s} = -\gamma \frac{\partial \mathcal{B}}{\partial q_s} v - \frac{\partial \mathcal{L}_s}{\partial q_s} = 0. \quad (37)$$

This additional constraint restricts the choice of  $q_s(\beta)$  in Equation (36), preventing the MSS provider from choosing  $q_s = Q_s^*$  because Equation (37) is different from the first-order condition in the social planner's problem, as stated in (3) when  $\gamma < 1$ . We define  $q_k = Q_k^{sb}$  and  $q_s = Q_s^{sb}$  as the second best efforts, which are the optimal efforts of the social welfare maximization problem in (36) given that the MSS provider's best response is constrained by (37).

However, the client will maximize its utility given the compensation rate, which should follow the first-order condition in (9). With a threshold-based liability contract, this condition is not binding because the client will exert effort at least at the threshold level to prevent the MSS provider from shirking. The MSS provider can choose  $q_k(\beta)$  freely by a properly constructed threshold-based liability contract. In particular, it can set  $T = Q_k^{sb}$  to force the client to exert the second best effort. As explained earlier, the client will not exert less than  $Q_k^{sb}$  because otherwise the MSS provider will shirk. Also, she will not exert more than  $Q_k^{sb}$  when the following incentive compatibility condition holds:

$$\left. \frac{\partial u_1}{\partial q_k} \right|_{q_k=Q_k^{sb+}} = (1-\gamma) \frac{\partial q_s}{\partial q_k} \frac{\partial \mathcal{B}}{\partial q_s} v + \gamma \frac{\partial \mathcal{B}}{\partial q_k} v \leq 0, \quad (38)$$

which implies that further increasing effort from  $Q_k^{sb}$  will decrease her utility. If Equation (38) does not hold,  $Q_k^{sb}$  will not be the client's equilibrium effort. Note that as long as the client's and the MSS provider's efforts are not strategic substitutes (i.e.,  $\partial q_s / \partial q_k \geq 0$ ), Equation (38) will always hold.

With variable liability contract, we find that the MSS provider can still regulate the client's effort with conditional compensation. Therefore, similar to threshold-based liability contract, the distortion is only initiated from the underinvestment of the MSS provider. By contrast, the efforts will be further distorted in a multilateral contract or a reverse insurance contract because the MSS provider cannot fully regulate the client's behavior without a compensation linked to her effort (compare with the bilateral liability-based contracts, where the postbreach compensation to the client is directly linked to her effort). Specifically, the client will maximize her utility based on the first-order condition

$$\frac{\partial u_1}{\partial q_k} = -\frac{\partial \mathcal{B}}{\partial q_k} v - \frac{\partial \mathcal{L}_k}{\partial q_k}. \quad (39)$$

Equation (39) is similar to the client's problem in (9) without the compensation from the MSS provider. It is similar to the client's problem in the first best scenario in (2). However, because of the distortion by the MSS provider's constraint (37), having this additional constraint would reduce welfare.

Intuitively, with the bilateral liability-based contracts, the client's effort is directly tied to the MSS provider's decision through the design of the compensation function. This facilitates the client to "work" with the MSS provider in arriving at the second best outcome. With multilateral or reverse insurance contracts, the client does not receive any compensation after the breach. Hence, her decision is detached from that of the MSS provider, meaning that her effort will be distorted from the second best.

In general, how the client reacts to limited liability depends on the security setting. In a security operations center where the state of security is obtained from or shared with the MSS provider, the client may overinvest in threat intelligence because protection efforts are substitutes, and she knows that the MSS provider may underinvest because of the limited liability. However, in systems with multiple access points (such as the point-of-sale systems in the Target incident), with limited liability, every party may underinvest in protection because the efforts are complements. We provide a detailed discussion of these breach scenarios and the associated analysis in the online appendix.

To summarize, our analysis of limited liability suggests that all liability-based contracts are socially inefficient. This means that it is difficult to achieve the first best outcome in the real world when there are liability constraints or price caps. However, the bilateral liability-based contracts (viz variable liability contract and threshold-based liability contract) perform better than third-party contracts, such as multilateral or reverse insurance contracts.

## 7. Discussion and Conclusions

Table 5 presents a high-level overview of the various contracts considered in this paper. The two bilateral liability-based contracts—threshold-based liability contract and variable liability contract—are viable alternatives to the multilateral contract proposed in the literature (Lee et al. 2013). Our findings can be extended to cases where there are interdependent clients and apply to commonly used security control configurations. Furthermore, we critically assess the relative performance of these contracts under real-world constraints, such as verification errors and limited liability.

This research explains an intriguing discrepancy between prior theoretical analysis and industry practice. In a setting involving collaborative service between a client and a service provider, it is difficult to incentivize both of them to work hard when effort is not



**Table 5.** Contract Comparison

Contract	Bilateral loss-based liability	Threshold-based liability	Variable liability	Third-party contracts
Socially efficient	No	Yes	Yes	Yes
Minimum number of parties in the contract	2	2	2	3
Observability of the breach event	Required	Required	Required	Required
Receiver of breach compensation	The breached client	The breached client	The breached client	Some third party (e.g., other client)
Audit of breached client's effort	Not required	Required: check if effort exceeds a threshold	Required: check all efforts	Not required
Additional clause to address the presence of interdependency risk	Penalize the breached client	No additional action needed	Introduce 100% limited liability	Penalize the breached client
Distortions caused by limited liability	MSS provider and client: constraints (9) and (10)	MSS provider only: constraint (37)	MSS provider only: constraint (37)	MSS provider and client: constraints (37) and (39)

contractible. Hence, we must add either a third party or some uncertainty in the outcome function to facilitate the choice of efficient efforts (Mann and Wissink 1988, Lee et al. 2013). However, as is evident in Table 1, none of these solutions are deployed in the security industry. Instead, the industry mostly uses bilateral contracts with some compensation terms. The compensations are often tied to customer behavior, implying that the service providers expect to observe (at least partially) the clients' effort after a security incident. Our research aligns the theory and practice by proving that bilateral liability-based contracts can indeed be efficient when the effort is verifiable after the breach.

Most importantly, we find that *this effort verification need not be complete*. In fact, a threshold-base liability contract (which does not require a full audit of the client's effort) performs even better than a variable liability contract (which requires a detailed assessment of the client's effort) when postbreach effort verification is erroneous. Both of these contracts work better than a multilateral (third-party) contract in the presence of limited liability. These findings are novel, and they have important implications for research. Although effort verification can address the underprovision problem in a collaborative setting (Cooper and Ross 1985, Bhattacharyya and Lafontaine 1995, Lee et al. 2013), the design of contract terms can have nuanced impacts on efficiency in the real world. Our findings should revitalize the interest in studying the design of IT service contracts amid the proliferation of collaborative innovations, such as internet of things or Blockchain-based industry consortia (Iansiti and Lakhani 2017).

Practically, this study suggests that we should promote bilateral liability-based contracts when postbreach effort verification is practicable. In reality, MSS providers often provide periodic audit reports on their service quality (van der Walt 2003). In banking, the Federal Financial Institutions Examinations Council, which oversees information security practices in financial institutions,

recommends detailed and comprehensive assessment and management of MSS risks, including the right to audit and monitor MSS providers.<sup>5</sup> These auditing initiatives focus on service providers, which may not be the party suffering the main consequences of a security breach. Hence, unique to the MSS setting where collaborative protection is important, we think that auditing the client's contribution should receive more attention when the contract stipulates compensation from the MSS provider to the client.

Indeed, the payment card industry engages qualified security assessors to check client firms' compliance with the PCI DSS. Development of new technologies, such as Blockchain, that facilitate the storage of tamper-proof data and immutable security logs (Cucurull and Puiggali 2016) would certainly help propel such client-side effort verification forward.

The efficiency of the bilateral liability-based contracts depends on the quality of the postbreach verification. Obviously, there are challenges in auditing effort. For example, it is not easy to define the scope, manage the costs, and agree on the key determinants on compliance with the PCI DSS (Rees 2012). Many audit processes rely on data sampling to determine past actions. Such sampling could introduce errors owing to, for example, omission and mismeasurement. When auditing or postbreach verification error is unavoidable, we suggest using a threshold-based liability contract. The MSS provider can estimate the potential range of audit errors and incorporate it in the threshold to incentivize efficient effort from the client. Variable liability contract will mostly not yield efficient efforts here.

We also find that the provision of limited liability makes all contracts, including the multilateral contract, inefficient. The question, then, is why such provision is often made, especially when it hurts the MSS provider's profit. We believe that it is because in reality, the client's loss may extend well beyond the actual loss in the system. For example, there could be litigation costs

from consumers (including the loss of productivity, breach of personal information, and identity theft), opportunity losses caused by suspension of service, and reputation losses. In our model, we subsume all of these losses in  $v$ , in which case then it will be difficult for the MSS provider to shoulder all of these liability. Even if the MSS provider is willing to bear all liability, it will likely set an extremely high price that is not acceptable to the client because most client firms tend to underestimate the consequences of cyberattacks (Lloyd's 2017). For these reasons, limited liability will likely prevail. Our research shows that the bilateral liability-based contracts are more efficient than multilateral contracts in the presence of limited liability, but they are not fully efficient either. Future research should explore other efficient contracts in this context.

Before we can resolve the limited liability problem using contractual solutions, the client may enhance her protection using cyber insurance (Lloyd's 2017). For example, she can separate assets into different clusters and collaborate with the MSS provider to control some well-defined risks. She can cover other clusters' risks by cyber insurance. This is akin to the setting of total effort configuration analyzed in Section 5. However, better transparency on risk exposure could also alleviate the problem caused by limited liability. Top-tier MSS providers today possess state-of-the-art systems to track attacks at a global scale. We encourage the sharing of such intelligence so that all parties are better informed about risk exposure. Information sharing can reduce overall security risks through more investments in security (Gal-Or and Ghose 2005). In our case, the inefficiency resulting from price distortion could be minimized when all parties are better informed about the overall risk exposure.

There are several limitations in our study. First, we analyze a monopoly MSS. This is a common assumption in the literature for the ease of tractability, but it is restrictive. Future research should extend the analysis to an oligopoly. Second, we treat information security as a single service. In reality, there are different security services, such as prevention, detection, and real-time incident response. Not all of these services involve collaborative efforts. Furthermore, it may not be optimal to outsource all security services to a single MSS provider (Cezar et al. 2014). Future research should consider a more flexible model that can accommodate separate security controls with different levels of collaboration between the MSS provider and the client.

Finally, other forms of information asymmetry exist. The MSS provider may overstate the client's risk to sway the client into purchasing more protection than needed. The client may not have the ability to judge whether the provider's advice is accurate, which has been seen in other settings, such as software development (Jayanth et al. 2011) and medical services (Dulleck

and Kerschbamer 2006). Future research should consider the optimal contract design in these related settings.

## Acknowledgments

The authors gratefully thank the senior editors, the associate editor, and anonymous reviewers for their constructive advice and guidance. They also thank the seminar participants at the Hong Kong University of Science and Technology and the University of Texas at Dallas for their helpful comments and suggestions.

## Endnotes

- <sup>1</sup> The proofs of all results are available in the online appendix.
- <sup>2</sup> The only exceptional case for Equation (15) to evaluate to a constant (which is the necessary condition for the variable liability contract to be efficient) is when  $\mathcal{B}[G(q_k) - G(q_k - a)]$  is independent of  $q_k$ . This could happen in some limited functional forms for  $\mathcal{B}(\cdot)$  and  $G(\cdot)$ , and even so, they have to follow some restricted parametric forms. This seems highly unlikely in the real world.
- <sup>3</sup> We consider a cubic cost function for the parallel configuration because a quadratic cost function will lead to zero first best efforts, meaning that everyone should not protect the system. Lee et al. (2016) also use different cost functions when analyzing the serial and parallel configurations.
- <sup>4</sup> We thank an anonymous reviewer for suggesting the analysis of limited liability.
- <sup>5</sup> Please refer to the Federal Financial Institutions Examination Council's (FFIEC) website for details: <http://ithandbook.ffiec.gov/it-booklets/outourcing-technology-services/appendix-d-managed-security-service-providers/mssp-examination-procedures.aspx>.

## References

- Abrams R (2014) Target puts data breach costs at \$148 million, and forecasts profit drop. *New York Times* (August 5), <http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html>.
- Aksin OZ, de Véricourt F, Karaesmen F (2008) Call center outsourcing contract analysis and choice. *Management Sci.* 54(2):354–368.
- Ashford W (2012) Best practice in outsourcing security. *Comput. Weekly* (July 16), <http://www.computerweekly.com/feature/Best-practice-in-outsourcing-security>.
- August T, Niculescu MF, Shin H (2014) Cloud implications on software network structure and security risks. *Inform. Systems Res.* 25(3):489–510.
- Bahirwani K (2015) Should security providers be held liable for data breaches? *Daily News Anal.* (April 6), <http://www.dnaindia.com/scitech/report-should-security-providers-be-held-liable-for-data-breaches-2075017>.
- Beaver K (2011) Do Web application firewalls complicate enterprise security strategy? *TechTarget* (February 9), <http://searchnetworking.techtarget.com/tip/Do-Web-application-firewalls-complicate-enterprise-security-strategy>.
- Bhattacharyya S, Lafontaine F (1995) Double-sided moral hazard and the nature of share contracts. *RAND J. Econom.* 26(4):761–781.
- Bhattacharya S, Gupta A, Hasija S (2014) Joint product improvement by client and customer support center: The role of gain-share contracts in coordination. *Inform. Systems Res.* 25(1): 137–151.
- Cavusoglu H, Raghunathan S, Cavusoglu H (2009) Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems. *Inform. Systems Res.* 20(2):198–217.

- Cezar A, Cavusoglu H, Raghunathan S (2014) Outsourcing information security: Contracting issues and security implications. *Management Sci.* 60(3):638–657.
- Chandler J (2010) Information security, contract and liability. *Chicago-Kent Law Rev.* 84(1):841–849.
- Chuvakn A (2014) MSSP: Integrate, NOT outsource! *Gartner* (November 5), <http://blogs.gartner.com/anton-chuvakin/2014/11/05/mssp-integrate-not-outsource/>.
- Cooper R, Ross TW (1985) Product warranties and double moral hazard. *RAND J. Econom.* 16(1):103–113.
- Cooter RD, Ulen TS (1986) An economic case for comparative negligence. *New York Univ. Law Rev.* 61(6):1067–1110.
- Cucurull J, Puiggali J (2016) Distributed immutabilization of secure logs. Barthe G, Markatos E, Samarati P, eds. *Proc. 12th Internat. Workshop Security Trust Management* (Heraklion, Crete, Greece), 122–137.
- Czarnik A (2014) How to justify risk-based security investments. *Tripwire* (July 10), <http://www.tripwire.com/state-of-security/featured/justifying-security-investments/>.
- Dey D, Fan M, Zhang C (2010) Design and analysis of contracts for software outsourcing. *Inform. Systems Res.* 21(1):93–114.
- Ding W, Yurcik W (2005) Outsourcing Internet security: The effect of transaction costs on managed service providers. *Proc. Internat. Conf. Telecomm. Systems—Model. Anal., Dallas*.
- Ding W, Yurcik W (2006) Economics of Internet security outsourcing: Simulation results based on the Schneier model. *Proc. Workshop Econom. Securing Inform. Infrastructure, Washington, DC*.
- Ding W, Yurcik W, Yin X (2005) Outsourcing Internet security: Economic analysis of incentives for managed security service providers. Deng X, Ye Y, eds. *Internet and Network Economics—WINE 2005, Lecture Notes in Computer Science*, vol. 3828 (Springer, Berlin), 947–958.
- Dulleck U, Kerschbamer R (2006) On doctors, mechanics, and computer specialists: The economics of credence goods. *J. Econom. Literature* 44(1):5–42.
- Emons W (1988) Warranties, moral hazard, and the lemons problem. *J. Econom. Theory* 46(1):16–33.
- Fisher JA (2013) Secure my data or pay the price: Consumer remedy for the negligent enablement of data breach. *William Mary Bus. Law Rev.* 4(1):215–239.
- Fitoussi D, Gurbaxani V (2012) IT outsourcing contracts and performance measurement. *Inform. Systems Res.* 23(1):129–143.
- Fryer H, Moore R, Chown T (2013) On the viability of using liability to incentivise Internet security. *Proc. Workshop Econom. Inform. Security (WEIS 2013), Washington, DC*.
- Gal-Or E, Ghose A (2005) The economic incentives for sharing security information. *Inform. Systems Res.* 16(2):186–208.
- Gartner (2017) Market share analysis: Managed security services, worldwide, 2016. *Gartner* (May 23), <https://www.gartner.com/doc/3726517/market-share-analysis-managed-security>.
- Goldstein M, Sood A (2014) Dispelling the myths of cyber security. *Dark Reading* (May 14), <http://www.darkreading.com/risk/dispelling-the-myths-of-cyber-security/a/d-id/1251171>.
- Gopal A, Sivaramakrishnan K, Krishnan MS, Mukhopadhyay T (2003) Contracts in offshore software development: An empirical analysis. *Management Sci.* 49(12):1671–1683.
- Gordon LA, Loeb MP (2002) The economics of information security investment. *ACM Trans. Inform. System Security* 5(4):438–457.
- Graves K (2010) *CEH Certified Ethical Hacker Study Guide* (John Wiley & Sons, Indianapolis).
- Green J (1976) On the optimal structure of liability laws. *Bell J. Econom.* 7(2):553–574.
- Grossklags J, Christin N, Chuang J (2008) Security investment (failures) in five economic environments: A comparison of homogeneous and heterogeneous user agents. *Proc. Workshop Econom. Inform. Security (WEIS 2008), Hanover, NH*.
- Gupta A, Zhdanov D (2012) Growth and sustainability of managed security services networks: An economic perspective. *MIS Quart.* 36(4):1109–1130.
- Hui KL, Hui W, Yue WT (2013) Information security outsourcing with system interdependency and mandatory security requirement. *J. Management Inform. Systems.* 29(3):117–156.
- Hurley E (2004) Cyberspace security liability lawsuits on the rise? *TechTarget* (February 1), <http://searchsecurity.techtarget.com/Cyberspace-security-liability-lawsuits-on-the-rise>.
- Iansiti M, Lakhani KR (2017) The truth about Blockchain. *Harvard Bus. Rev.* 95(1):118–127.
- IBM (2008) IBM managed security services for network intrusion detection and intrusion prevention. *IBM Global Services*. Retrieved September 21, 2017, <http://www-935.ibm.com/services/us/igs/pdf-iss-contracts/uk-7805-00.pdf>.
- Jain N, Hasija S, Popescu DG (2013) Optimal contracts for outsourcing of repair and restoration services. *Oper. Res.* 61(6):1295–1311.
- Jayanth R, Jacob VS, Radhakrishnan S (2011) Vendor and client interaction for requirements assessment in software development: Implications for feedback process. *Inform. Systems Res.* 22(2):289–305.
- Kambhu J (1982) Optimal product quality under asymmetric information and moral hazard. *Bell J. Econom.* 13(2):483–492.
- Kirk J (2014) Google expands bug bounty program, ups patch reward. *PC World* (February 5), <https://www.pcworld.idg.com.au/article/537538/>.
- Kolochenko I (2015) DDoS attacks: A perfect smoke screen for APTs and silent data breaches. *CSO Magazine* (September 28), <http://www.csoonline.com/article/2986967>.
- Lee CH, Geng X, Raghunathan S (2013) Contracting information security in the presence of double moral hazard. *Inform. Systems Res.* 24(2):295–311.
- Lee CH, Geng X, Raghunathan S (2016) Mandatory standards and organizational information security. *Inform. Systems Res.* 27(1):70–86.
- Lichtman D, Posner E (2006) Holding Internet service providers accountable. *Supreme Court Econom. Rev.* 14:221–259.
- Lloyd's (2017) Closing the gap: Insuring your business against evolving cyber threats. Retrieved September 21, 2017, <https://www.lloyds.com/lloyds/about-us/what-do-we-insure/what-lloyds-insures/cyber/cyber-risk-insight/closing-the-gap>.
- Mani D, Barua A, Whinston AB (2012) An empirical analysis of the contractual and information structures of business process outsourcing relationships. *Inform. Systems Res.* 23(3):618–634.
- Mann DP, Wissink JP (1988) Money-back contracts with double moral hazard. *RAND J. Econom.* 19(2):285–292.
- Moitra SD, Konda SL (2000) The survivability of network systems: An Empirical analysis. Technical Report CMU/SEI-2000-TR-021, Carnegie Mellon Software Engineering Institute, Pittsburgh.
- Naldi M, Flamini M, D'Acquisto G (2013) Information security investments: When being idle equals negligence. Altmann J, Vanmechelen K, Rana O, eds. *Economics of Grids, Clouds, Systems, and Services—GECON 2013, Lecture Notes in Computer Science*, vol. 7150 (Springer, Cham, Switzerland), 268–279.
- National Institute of Standards and Technology (2012) Guide for conducting risk assessments. NIST Special Publication: 800-30 Revision 1, 1–95, National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, MD.
- Overby S (2012) IT service providers and customers battle over data breaches. *CIO Magazine* (March 9), <http://www.cio.com/article/2395626>.
- Rees J (2012) Tackling the PCI DSS challenges. *Comput. Fraud Security* 2012(1):15–17.
- Riley M, Elgin B, Lawrence D, Matlack C (2014) Missed alarms and 40 million stolen credit card numbers: How Target blew it. *Bloomberg* (March 13), <http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data>.

- Roels G, Karmarkar US, Carr S (2010) Contracting for collaborative services. *Management Sci.* 56(5):849–863.
- Rubinfeld DL (1987) Efficiency of comparative negligence. *J. Legal Stud.* 16(2):375–394.
- Rustad ML, Koenig TH (2007) Extending Learned Hand’s negligence formula to information security breaches. *I/S J. Law Policy Inform. Soc.* 3(2):236–270.
- Schneier B (2002) The case for outsourcing security. *Computer* 35(4): 20–26.
- Schwartz M (2013). How South Korean bank malware spread. *Dark Reading* (March 25), <https://www.darkreading.com/d/d-id/1109239>.
- Shavell S (1979) On moral hazard and insurance. *Quart. J. Econom.* 93(4):541–562.
- Susarla A, Subramanyam R, Karhade P (2010) Contractual provisions to mitigate holdup: Evidence from information technology outsourcing. *Inform. Systems Res.* 21(1):37–55.
- Technavio (2016) Global managed security services market 2016–2020. Retrieved September 21, 2017, <https://www.technavio.com/report/global-it-security-managed-security-market>.
- Tipton HF, Krause M (2007) *Information Security Management Handbook* (CRC Press, Boca Raton, FL).
- van der Walt A (2003) Managed security services: who needs it? *Comput. Fraud Security* 2003(8):15–17.
- van Kessel P, Allan K (2014) Get ahead of cybercrime: EY’s global information security survey 2014. Ernst & Young Global Limited. Retrieved September 21, 2017, [https://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/\\$FILE/EY-global-information-security-survey-2014.pdf](https://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf).
- Varian H (2004) System reliability and free riding. Camp LJ, Lewis S, eds. *Economics of Information Security*, Advances in Information Security, vol. 12 (Springer, Boston), 1–15.
- Viebeck E (2015) Premera Blue Cross sued over data breach. *TheHill.com* (March 27), <http://thehill.com/policy/cybersecurity/237181-premera-blue-cross-sued-over-data-breach>.
- Zhao X, Xue L, Whinston AB (2013) Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *J. Management Inform. Systems* 30(1):123–152.