2014-03-01

Outsourcing Information Security: Contracting Issues and Security Implications

UTD AUTHOR(S): Huseyin Cavusoglu and Srinivasan Raghunathan

Management Science

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Outsourcing Information Security: Contracting Issues and Security Implications

Asunur Cezar, Huseyin Cavusoglu, Srinivasan Raghunathan

To cite this article:
Asunur Cezar, Huseyin Cavusoglu, Srinivasan Raghunathan (2014) Outsourcing Information Security: Contracting Issues and Security Implications. Management Science 60(3):638-657. http://dx.doi.org/10.1287/mnsc.2013.1763

MANAGEMENT SCIENCE
Vol. 60, No. 3, March 2014, pp. 638–657
ISSN 0025-1909 (print) | ISSN 1526-5501 (online)

http://dx.doi.org/10.1287/mnsc.2013.1763

Outsourcing Information Security: Contracting Issues and Security Implications

Asunur Cezar
Department of Business Administration, TOBB University of Economics and Technology, Ankara 06560, Turkey, acezar@etu.edu.tr

Huseyin Cavusoglu, Srinivasan Raghunathan
Naveen Jindal School of Management, University of Texas at Dallas, Richardson, Texas 75080
{huseyin@utdallas.edu, sraghu@utdallas.edu}

A unique challenge in information security outsourcing is that neither the outsourcing firm nor the managed security service provider (MSSP) perfectly observes the *outcome*, the occurrence of a security breach, of prevention effort. Detection of security breaches often requires specialized effort. The current practice is to outsource both prevention and detection to the same MSSP. Some security experts have advocated outsourcing prevention and detection to different MSSPs. We show that the former outsourcing contract leads to a significant disincentive to provide detection effort. The latter contract alleviates this problem but introduces misalignment of incentives between the firm and the MSSPs and eliminates the advantages offered by complementarity between prevention and detection functions, which may lead to a worse outcome than the current contract. We propose a new contract that is superior to these two on various dimensions.

Keywords: outsourcing; information security; contracting; managed security service providers; IT security services
History: Received July 7, 2011; accepted March 24, 2013, by Lorin Hitt, information systems. Published online in *Articles in Advance* September 27, 2013.

1. Introduction

Information security management has become a critical as well as challenging business function because of reasons such as the rising cost of security breaches;[1] increasing scale, scope, and sophistication of security attacks; complexity of information technology (IT) environments; and compliance and regulatory obligations. Firms are responding to information security challenges by increasingly outsourcing IT security operations to managed security service providers (MSSPs).[2] Though MSSPs have expanded their offerings over the years to provide firms with a multitude of solutions—ranging from device management and vulnerability scanning to network monitoring for incident detection and response—to achieve comprehensive protection, these managed services can be grouped into two main categories based on the fundamental objectives they serve for security management: prevention and detection. Whereas prevention services such as firewall, intrusion prevention system, virtual private network management, and vulnerability scanning services seek to protect a firm from security breaches to avoid potential losses, detection services such as 24/7 security monitoring and intrusion detection system management services aim to detect security breaches while they are in progress to avoid some of the potential losses (Kark 2010).

Any outsourcing deal potentially suffers from a moral hazard problem, and information security outsourcing is not an exception. Moral hazard arises because a firm cannot perfectly observe or verify the MSSP's efforts. The firm typically designs an appropriate contract that provides the right incentives to mitigate the moral hazard issue. Additionally, the firm often builds an ex post investigation into the contract to assign responsibility in case of a bad outcome. Outsourcing in the information security context is confronted with another challenge that gives rise to additional incentive problems. In information security outsourcing, neither the firm nor the MSSP can perfectly observe the outcome of MSSP's prevention effort. An important outcome of prevention effort relates to whether the firm suffered a security breach, which is often the only contractible quantity when the prevention function is outsourced. However, neither

[1] The average total cost of a data breach, which includes the cost of recovery, lost productivity costs, and customer opportunity costs, in 2009 was $204 for each breached customer record (Ponemon Institute 2011).

[2] In 2009, 60% of Fortune 500 companies had used an MSSP and about 25% of enterprise firewalls were under remote monitoring or management (Kavanagh and Pescatore 2009).

the firm nor the MSSP is able to detect every security breach that the firm experiences.[3] The failure to detect a breach can imply any of the following: (i) the firm did not experience an attack, (ii) the MSSP prevented the attack, or (iii) the MSSP could not detect the attack. Therefore, to properly assess the performance of the MSSP that is providing prevention services, detection of breaches becomes important. This creates an interdependency between prevention and detection functions at the contract level.

Like prevention, detection of security breaches often requires significant effort and expertise. Detection of a security breach is important to the firm not only because this information allows the firm to gauge the MSSP's prevention effort (thereby enabling the firm to incorporate an appropriate incentive mechanism into the contract so that the MSSP exerts adequate prevention effort) but also because it enables the firm to recover from some damage resulting from the breach. Furthermore, detection of a breach does not automatically imply that it is the lack of prevention effort by the MSSP that caused the breach,[4] and it becomes necessary to conduct an ex post investigation, which is generally part of the response function of information security management.[5] All these challenges make contract design a difficult, but at the same time a very important, aspect of information security outsourcing.

Details about structure and framework of prevailing information security outsourcing contracts are publicly available on the websites of leading MSSPs such as IBM, Verizon Business, and Megapath[6] and on websites of some outsourcing firms.[7] An analysis of information found in these websites, industry market reports (Kavanagh and Pescatore 2009, Frost & Sullivan 2010, Kark 2010), and our conversations with security experts reveal the following.[8] First, firms usually outsource both prevention and detection functions to the same MSSP. Second, contracts are typically implemented using service-level agreements (SLAs) and indemnifications when SLAs are not met. The SLAs, as one part of the contract, spell out the attributes of the security service (i.e., service levels) agreed upon between the firm and the MSSP (Allen et al. 2003). Service levels deal with various service quality measures such as prevention of specific breaches, availability of security services, time for notifying event alarm, and event response time. For instance, IBM Managed Security Services guarantees protection against breaches listed in the Internet Security Systems X-Force® Certified Attack List (IBM 2007). The request for proposal for security services by Indian Railways calls for an event alert time of less than 15 minutes for high-priority events and less than 30 minutes for medium-priority events (IRCTC 2011). In conjunction with the SLA, the contract specifies the service fee that the firm will pay the provider for provisioning of security services. In general, the provider charges a monthly or yearly fixed fee for a specific level of service.[9]

The contract usually also specifies the courses of action to be taken if the MSSP fails to meet the service levels in the SLA. This is typically operationalized with a penalty or service credit. For instance, IBM pays a penalty of $50,000 if it fails to prevent an attack listed in the SLA. Verizon provides a credit on the fees. The contract between the city of Los Angeles and the Computer Sciences Corporation (CSC) specifies that CSC fully covers the damage of the city in case of a data breach.[10] In other words, the penalty captures the refund the provider gives to the firm for missing security breaches (Allen et al. 2003, Butler Group 2007, Roiter 2009). Given the prevalence of contracting with a single MSSP for comprehensive protection, we first analyze how the firm should design a contract

[3] It is estimated that 30%–60% of security breaches go undetected (Baker et al. 2011).

[4] Roiter (2009) notes, "If your email security or Web filtering service is slow, for example, is the problem on the provider end? A lot of factors can slow things down on the Internet. Unless you can show that a bunch of other customers were affected, clearly pointing back to the provider, you're probably out of luck," suggesting that the performance is measured within the context of what can be reasonably expected. Since information security is a dynamic field with ever-changing attacks, the question of what can be reasonably expected is subject to interpretation.

[5] Information security management is often viewed using a framework that has three layers of functions: prevention, detection, and response (LaPiedra 2002).

[6] http://www-935.ibm.com/services/us/iss/pdf/gtd00763-usen-01.pdf, http://www.verizonbusiness.com/terms/us/products/security/intrusion/, http://www.megapath.com/pdfs/service_level_assurances.pdf (accessed February 15, 2013).

[7] https://www.irctc.co.in/betaDoc/tender_Managed_Services.pdf, http://www.scribd.com/doc/32676277/City-of-Los-Angeles-and-CSC-Google-Contract (accessed February 15, 2013).

[8] In talking with security experts to understand the MSSP market, we extensively benefited from our conversation with Bruce Schneier (2011), a noted security guru and the chief security technology officer of BT, which offers managed security services. He mentioned that "close to 100%" of outsourcers outsource both preventive and detective security services to the same MSSP. He said that "only reasonable recompense" in the real contracts include "money back or a credit of some sort." In addition, he mentioned that rewarding the MSSP for detective services is "a clever idea, but [he] has never seen it in practice" and that "a good SLA" is the most important point in designing security outsourcing contracts.

[9] Prices range between $1,500 and $2,500/month for detection only, $3,000 and $4,000/month for mitigation only, and $5,000 and $6,000/month for both detection and mitigation services (Arbor Networks 2010).

[10] http://www.scribd.com/doc/32676277/City-of-Los-Angeles-and-CSC-Google-Contract (accessed February 15, 2013).

that has a fixed service fee and a penalty for missing security breaches.

Despite the popularity of outsourcing prevention and detection services to a single provider, some experts in the security community have advocated outsourcing prevention and detection functions to different MSSPs (Schneier 2002, Allen et al. 2003). Their argument is that if the same outsourcer performs both prevention and detection services, a conflict of interest between security functions may arise. By detecting a security lapse, the MSSP implicitly acknowledges that it failed to prevent the security lapse. Schneier (2002, p. 21) notes, "If the outsourcer finds a security problem with my network, will the company tell me or try to fix it quietly?" The firm can eliminate the conflict of interest by outsourcing these two functions to different MSSPs. This argument is consistent with the result in the traditional job-design literature that shows when the principal has the ability to divide responsibility for many tasks between agents, it may be better to make one agent responsible for one task and design a separate contract for each task (Holmstrom and Milgrom 1991).

Following this suggestion, we next analyze how the firm should design the optimum incentive structure to outsource prevention and detection functions to two MSSPs with a contract that has (i) a fixed service fee and penalty for missing security breaches for the MSSP responsible for prevention and (ii) a fixed service fee and reward for detecting security breaches for the MSSP responsible for detection. We demonstrate that although using two different MSSPs can alleviate the conflict of interest faced by the MSSP under the prevalent contract, it introduces a different incentive issue: the interdependent security functions require coordination even if these functions are performed by separate service providers. This creates a strong interdependency between the parameters of the two contracts. Hence, contracting with two different MSSPs may lead to an outcome that is worse for the firm than when both prevention and detection functions are outsourced to the same MSSP.

Finally, we propose a new contract and obtain a series of results that show that the proposed contract is superior to the other two on several dimensions. In the proposed contract, the firm outsources both prevention and detection functions to a single MSSP, and it offers a reward to the MSSP for revealing security breaches and imposes a penalty on the MSSP if it is found to be responsible for the breach, in addition to the fixed fee.

Our results provide important implications for the design of security outsourcing contracts. Apart from offering theoretical support for the concerns expressed by the information security experts with regard to outsourcing different security functions to a single MSSP, we uncover additional insights that are new and surprising. When the incentives to perform two activities conflict with each other, the conventional wisdom suggests assigning the activities to different agents. However, we show that this strategy may not lead to the best outcome in the information security outsourcing context. Hiring different agents to perform prevention and detection activities introduces a new source of inefficiency in the form of interdependency between two contracts, requiring coordination between contracts, and also eliminates the complementarity between the two activities. However, hiring a single agent to perform both tasks with two different performance incentives mitigates this inefficiency while simultaneously exploiting the complementarity that exists between prevention and detection efforts. It also leads to the solution that maximizes the joint payoff. These benefits of using a single MSSP for both security functions are in addition to other potential benefits the proposed contract offers relative to other contracts. For instance, having a single MSSP eliminates the need to coordinate with two different MSSPs. Therefore, the fundamental insight offered by our analysis is that firms should continue to outsource both prevention and detection functions to a single MSSP but alter the nature of the contract they currently have to maximize the benefit of security outsourcing.

1.1. Related Literature

Since the present paper studies outsourcing contracts, it is related to the vast literature on outsourcing, both in IT (see, e.g., Lacity et al. 2009 for a survey of IT outsourcing literature) and in other contexts such as manufacturing, as well as to contract theory in economics. Rather than attempting to identify the link between the present paper and the voluminous outsourcing/contracting literature, we confine our discussion of references here to the part of the literature that deals with analytical models in IT and information security outsourcing contracts. In one of the earliest papers on IT outsourcing, Whang (1992) analyzed a multiperiod software development contract between a firm and an outside developer and derived an optimal contact that replicates the equilibrium outcome of a benchmark in-house development. More recently, Dey et al. (2010) examined different types of software outsourcing contracts under information asymmetry and incentive divergence and showed that more complicated outsourcing contract forms do not guarantee higher performance. In the information security context, Rowe (2007) discussed a number of benefits offered by MSSPs, such as information sharing and economies of scale. Ding and Yurcik (2005, 2006) and Ding et al. (2005) examined the characteristics of optimal MSSP contracts under moral hazard

and found that an optimal contract should be performance based. The extant information security and traditional IT contracting literature assumes that a single type of service is outsourced. For instance, information security outsourcing literature has focused on outsourcing prevention services, and general IT outsourcing literature has focused on software development. An exception to this observation is the work of Cezar et al. (2009), which analyzed a context in which two firms outsource security to a single MSSP and showed that the nature of information security risk, extent of competition between firms, and predominant nature (infrastructure management or monitoring) of the security function outsourced affect firms' incentives to outsource. In this paper, we consider outsourcing two different but related security services and analyze the question of whether they should be outsourced to the same or two different MSSPs.

A few papers on information security have analyzed issues such as interdependent security risks among firms in managed security services and the formation and growth of MSSP networks (Gupta and Zhdanov 2012, Zhao and Whinston 2013). However, their focus was not on contracting issues but on how to attain the critical mass to form this network profitably. Hence, they considered the economies of scale in making security infrastructure investment and network externalities associated with being served by the same MSSP. Since we are considering contracting issues with an established MSSP, economies of scale associated with initial infrastructure investment do not play any role. Yet we consider the benefit resulting from network externalities through learning effects. In our model, the efforts needed to provide security services for a new client are exerted using the existing security infrastructure, and both prevention and detection efforts are firm specific. They do not refer to additional security investment to the common security infrastructure.[11]

A few models in the manufacturing context have considered outsourcing multiple sequential tasks in which the output of one becomes the input to another (see, e.g., Sridhar and Balachandran 1997), but our outsourcing model does not assume any sequential relationship between prevention and detection services. Models in the general contracting theory assume that although efforts are unobservable, the outcomes—though they are noisy signals of efforts—for which contracts are written are observable by the principal and the agent. In our model, no party perfectly observes the outcome.

Our paper is related to the topic of multitask job design, which has been extensively researched in the economics literature. In their seminal paper, Holmstrom and Milgrom (1991) examined how jobs with tasks that have varying degrees of performance measurability should be assigned to agents. They showed that tasks whose performance can be easily measured and tasks whose performance cannot be easily measured should be assigned to different agents with different contracts. Following that paper, several papers looked at various performance measures in multitask principal-agent problems (see e.g., Itoh 1991, 1994; Feltham and Xie 1994; Holmstrom and Milgrom 1994; Dewatripont et al. 2000; MacDonald and Marx 2001). The focus of these papers has been mainly on how performance signals from multiple agents can be used to incentivize agents. These papers typically assume that efforts and outcomes of these efforts are separable and use a total payoff function that is linear in efforts on various tasks. Some other papers consider the correlation between the outcomes of agents' efforts, but they assume binary effort levels and outcomes (see, e.g., Chen 2012). These models do not apply to the information security context for the following reasons. First, the outcomes of prevention and detection efforts in information security are interdependent in the following sense: the outcome of prevention effort can only be assessed using the outcome of detection effort. Detecting a breach implies that prevention effort led to a bad outcome, but not detecting a breach does not imply that the outcome of prevention effort was good (or bad). Second, the payoff function is nonlinear in efforts. Third, all efforts exerted by MSSPs are continuous.

The present paper is also related to the auditing literature in accounting (see, e.g., Antle 1982, Baiman et al. 1987, Caplan 1999). The key difference between our paper and papers in the auditing literature lies in the model setup considered. In the auditing context, the agent who privately observes the outcome has an incentive to misreport the outcome, and the principal hires an auditor to attest to the validity of the report issued by the agent. In our model, the outcome may not be known perfectly to any party including the agent, and the detection effort (which could be viewed as one that is similar to the auditing effort) is not used to detect misrepresentation about the outcome (i.e., breach) but to detect the outcome itself.

[11] Johnson (2005, p. 3) argues that "a MSSP should provide regular upgrades and maintenance, such as log rotation and rule cleanup, to your security devices." Also, "the MSSP should interface with your security device to provide any rule changes that you require, or that are dictated by security events." This is consistent with the argument of Schneier (2002) that companies outsourcing security require too much individual attention. About network monitoring, Schneier (2007, p. 4) says that "software can only provide generic information; real understanding requires experts.... To make network monitoring work, people are needed every step of the way. Software doesn't think, doesn't question, doesn't adapt. Without people, computer security software is just a static defense."

Therefore, in the auditing context, the information produced by the auditor is used only to incentivize the manager in truthful reporting (i.e., the auditor is not directly productive), but in the security context, both prevention and detection efforts are productive, and the firm's problem is coordinating as well as incentivizing the parties that provide these efforts.

2. The Model

We consider a firm that has decided to outsource information security prevention and detection services and is faced with the problem of determining the optimal outsourcing contract. We model the contracting problem as a one-shot game in which the firm offers a contract and the MSSP accepts or rejects the contract.[12] The MSSP may serve multiple client firms during the contract period. The MSSP's and the firm's payoffs depend on the number of clients the MSSP serves and the MSSP's efforts toward the firm's security. The contract between the MSSP and the firm is bilateral, which is common practice, as discussed in §1.

Consistent with the one-shot game, we model security attacks during the contract period at the incident level. We consider only a series of attacks that lead to an incident. That is, all attacks that occur during the contract period are treated as part of a single security incident. Going forward, we will refer to this incident simply as a *breach*. A security breach inflicts a total monetary loss of L on the firm if it goes undetected and $L\alpha$, $0 \le \alpha \le 1$ if it is detected.[13] The parameter L includes both tangible costs, such as the revenue loss from disruption of services, and intangible costs, such as those associated with the loss of reputation and customer distrust (Cavusoglu et al. 2004).[14] The probability of breach on this firm, $\theta(e_p, N_p)$, is a function of the prevention effort, e_p, exerted to protect this firm and the number of firms, N_p, the MSSP offers its protection services to (including the firm under consideration). The dependence of θ on N_p models not only the multiclient nature of the MSSP network but also the MSSP's capability to improve the effectiveness of prevention effort by sharing knowledge and infrastructure when it serves multiple clients. θ is a decreasing convex function of e_p and N_p; i.e., $\partial\theta/\partial e_p = \theta'_{e_p} < 0$, $\partial^2\theta/\partial e_p^2 = \theta''_{e_p} > 0$, $\partial\theta/\partial N_p = \theta'_{N_p} < 0$, and $\partial^2\theta/\partial N_p^2 = \theta''_{N_p} > 0$. We assume that absolute prevention is impossible for any finite level of prevention effort; i.e., $\arg_{e_p}(\theta(e_p, N_p) = 0) = \infty$.

A breach is sometimes detected by the firm's own employees during the course of normal work hours and by third parties such as customers and partner firms. We assume that the probability of the firm and other third parties detecting a breach is κ. Positive detection effort exerted by the MSSP for this firm improves breach detection further. The probability of detecting a breach, $\phi(e_d, N_d)$, is an increasing concave function of the detection effort, e_d, exerted to protect this firm and the number of clients, N_d, the MSSP offers its detection services to; i.e., $\partial\phi/\partial e_d = \phi'_{e_d} > 0$, $\partial^2\phi/\partial e_d^2 = \phi''_{e_d} < 0$, $\partial\phi/\partial N_d = \phi'_{N_d} > 0$, $\partial^2\phi/\partial N_d^2 = \phi''_{N_d} < 0$. Similar to the prevention effort, we assume that perfect detection is impossible for any finite level of detection effort; i.e., $\arg_{e_d}(\phi(e_d, N_d) = 1) = \infty$.

The cost of security services depends on the efforts. Further, the cost of security services may also depend on the number of firms currently served by the MSSP because the larger the MSSP's client base, the better the MSSP can reap the benefit of information sharing among clients and the more efficient its efforts are. When a firm outsources its security services, the MSSP analyzes the firm's security infrastructure and collects data on incoming and outgoing network traffic. This information is then combined with the same type of information and data from other firms that outsource to the same MSSP. As the number of firms that outsource to one MSSP increases, the MSSP is able to analyze a larger set of data and network configurations with which to provide prevention and detection services. Hence, for the same effort levels, the MSSP may be able to attain a certain level of security for a given firm (both for prevention and detection) at a lower cost. In addition, prevention and detection efforts exerted for the firm by the same MSSP are often complementary. The rationale for the complementarity is the following. Suppose the MSSP knows that its prevention effort is very effective in addressing a specific security vulnerability for the firm. Then it can focus its detection efforts on exploitation of other security vulnerabilities. Also, the MSSP learns from the observed outcome of security services to redefine its efforts to take advantage of this learning. For instance, knowledge gained from detection of a breach could facilitate better targeting of prevention and detection efforts. For these reasons, we model the total cost of efforts as the following: $C(e_p, e_d, N_p, N_d) = C_p(e_p, N_p) + C_d(e_d, N_d) - \rho f(e_p, e_d, N_p, N_d)$,[15] where $\rho > 0$ can be considered

[12] This implies that the firm has bargaining power over the MSSP. In §5, we show that the results do not change qualitatively in the more general case in which the firm and the MSSP may have different bargaining strengths.

[13] Schneier (2001, p. 494) points out, "If [the firm] can respond quickly and effectively, [the firm] can repel the attacker before he does any damage. Good detection and response can make up for imperfect prevention."

[14] We assume that a security breach inflicts a fixed damage. However, our analysis can easily be extended to the stochastic damage case, as shown in §5.

[15] There could also be fixed costs for prevention and detection efforts, but we normalize them to 0 without loss of generality.

a proxy that captures the level of complementarity between prevention and detection efforts. We assume that $C(e_p, e_d, N_p, N_d)$ is increasing and convex in efforts but decreasing in number of firms. Hence, $C'_{p_{e_p}} > \rho f'_{e_p}$, $C''_{p_{e_p}} > \rho f''_{e_p}$, $C'_{d_{e_d}} > \rho f'_{e_d}$, $C''_{d_{e_d}} > \rho f''_{e_d}$, $C'_{N_p} < \rho f'_{N_p}$, $C'_{N_d} < \rho f'_{N_d}$. Also, efforts are cost complements (i.e., $f''_{e_p, e_d} \geq 0$). We also assume that the absolute and marginal cost of no prevention is 0 and the marginal cost of full prevention (i.e., zero breach) is sufficiently high; i.e., $C_p(\arg_{e_p}(\theta = 1), N_p) = C'_p(\arg_{e_p}(\theta = 1), N_p) = 0$ and $C'_p(\arg_{e_p}(\theta = 0), N_p) = \infty$. Similarly, we assume $C_d(\arg_{e_d}(\phi = 0), N_d) = C'_d(\arg_{e_d}(\phi = 0), N_d) = 0$ and $C'_d(\arg_{e_d}(\phi = 1), N_d) = \infty$. These assumptions are necessary to ensure an optimal interior solution. Complementarity between prevention and detection functions does not exist if they are performed by different agents.

When a breach is detected, the firm and the MSSP that offers prevention services undertake appropriate actions to respond. These postdetection incident-handling activities serve multiple purposes such as incident recovery and forensic investigation. For instance, incident recovery involves stopping the incident and recovering control of systems using a containment strategy, such as reconfiguring the firewall to block traffic from the attack source or disabling services/accounts associated with the incident (Whitman and Mattord 2011). Once the incident has been contained, incident recovery deals with restoring the systems, such as analyzing the system logs, investigating the cause and responsible party for the incident, patching the vulnerabilities that allowed the incident to happen, restoring data from backups, and restoring compromised services. In contrast, forensic investigation deals with preserving the breach state and evidence of criminal activity, possibly for prosecution of hackers. All these postdetection activities have cost implications. The extent of postdetection activities will clearly depend on the severity of the damage caused by breach, and therefore, the cost of postdetection activities will likely be function of L. Since we deal with a single breach type with a fixed exogenously specified loss, we model the total cost of this postdetection response effort as a fixed constant $C_r < L(1 - \alpha)$.[16] We assume the policy regarding postdetection response is exogenous to the contract.

Further, the cost function used for the variable costs does not affect our results qualitatively, as long as the cross derivatives with respect to the two arguments are negative.

[16] It is conceivable that the nature of postdetection activities is also governed by the detection activities. In such cases, the cost of postdetection activities will be a function of detection effort. In the Extensions section (§5.4), we analyze a model with this feature and show that our results do not change qualitatively.

Table 1 Model Notation

Variable	Description
L	Total monetary loss from a breach
α	Proportion of total loss inflicted when a breach is detected
e_p	The MSSP's prevention effort
e_d	The MSSP's detection effort
ρ	Level of complementarity between prevention and detection efforts
C_p	Cost of prevention effort
C_d	Cost of detection effort
C	Total cost of efforts
N_p	Number of firms the MSSP offers its protection services to
N_d	Number of clients the MSSP offers its detection services to
M_P	The MSSP that provides the prevention services
M_D	The MSSP that provides the detection services
θ	Probability of a breach
ϕ	Probability of detecting a breach
κ	Probability of the firm or other third parties detecting a breach
C_r	Total cost of postdetection response effort
γ	The fraction of the postdetection response cost borne by the firm
F	Fixed fee paid by the firm to the MSSP
u	The MSSP's reservation wage
p	Penalty paid by the MSSP when a breach is detected and the MSSP is responsible for the breach
m	Probability that the MSSP is responsible for the breach
r	Reward offered to the MSSP when it detects a breach not detected by the firm or others

Our assumptions regarding prevention and detection efforts and security breaches imply the following. Not all prevention and detection efforts exerted by an MSSP are observable and therefore verifiable by the firm. A security breach is imperfectly observable—that is, it is detected only with a probability less than 1. The probability of detecting a breach is a function of detection effort. The loss from an observed breach is perfectly verified. However, because not all breaches are observed, some losses the firm incurs from security breaches are not verifiable.

We assume that the number of clients serviced by an MSSP does not change during the contract period. That is, we do not model the dynamic aspects or the growth of MSSP networks in this paper. Further, we assume that MSSPs do not have incentives to engage in fraudulent activities, such as intentionally hiding security breaches they detect from the firm or intentionally causing a security breach. The expected cost of such actions, which may include tarnished reputation and severe penalty if found guilty of fraud, outweighs any gain that can be realized. Finally, all parties are risk neutral, and model parameters are common knowledge. Table 1 summarizes the model notation.

2.1. Benchmark: Efforts That Maximize the Joint Payoff

As a benchmark, we first determine the efforts that maximize the joint payoff for the system that includes

the firm and the MSSP(s). Clearly, the maximum joint payoff occurs only when both prevention and detection functions are exerted by the same party because of the complementarity between the two functions that exists only when a single party performs both.[17] The optimization problem for choosing the benchmark efforts is

$$\max_{e_p, e_d} \Pi = -\theta(e_p, N_p)(L-(L(1-\alpha)-C_r)(\kappa+(1-\kappa)\phi(e_d, N_d))) - C_p(e_p, N_p) - C_d(e_d, N_d) + \rho f(e_p, e_d, N_p, N_d). \quad (1)$$

We assume that $|\partial^2\Pi/\partial e_p^2| > |\partial^2\Pi/\partial e_p\partial e_d|$ and $|\partial^2\Pi/\partial e_d^2| > |\partial^2\Pi/\partial e_p\partial e_d|$ to ensure the concavity of the objective function in e_p and e_d. Hence the unique efforts that maximize the joint payoff, e_p^* and e_d^*, are obtained by solving the following simultaneous equations (Fudenberg and Tirole 1998):

$$\left.\frac{\partial\Pi}{\partial e_p}\right|_{e_p=e_p^*, e_d=e_d^*} = -\theta'_{e_p}(e_p^*, N_p)[L-(L(1-\alpha)-C_r)(\kappa+(1-\kappa)\phi(e_d^*, N_d))] - C'_{p_{e_p}}(e_p^*, N_p) + \rho f'_{e_p}(e_p^*, e_d^*, N_p, N_d) = 0, \quad (2)$$

$$\left.\frac{\partial\Pi}{\partial e_d}\right|_{e_p=e_p^*, e_d=e_d^*} = \theta(e_p^*, N_p)\phi'_{e_d}(e_d^*, N_d)(L(1-\alpha)-C_r)(1-\kappa) - C'_{d\,e_d}(e_d^*, N_d) + \rho f'_{e_d}(e_p^*, e_d^*, N_p, N_d) = 0. \quad (3)$$

Hereafter, we refer to e_p^* and e_d^* as the benchmark prevention effort and benchmark detection effort, respectively. An examination of the benchmark efforts gives rise to the following result.[18]

Proposition 1. *The benchmark prevention effort and the benchmark detection effort are substitutes if and only if*

$$\rho < \frac{-\theta'_{e_p}(e_p^*, N_p)(L(1-\alpha)-C_r)(1-\kappa)\phi'_{e_d}(e_d^*, N_d)}{f''_{e_p, e_d}(e_p^*, e_d^*, N_p, N_d)}.$$

Proposition 1 is the result of two opposing effects one effort has on the marginal payoff of the other effort. Consider the prevention effort. An increase in the prevention effort decreases the likelihood of a breach, which in turn reduces the marginal benefit from detection. On the other hand, an increase in the prevention effort also decreases the marginal cost of detection effort because of the complementarity between the efforts. When the complementarity is lower (higher) than a threshold, the former (latter) effect dominates the latter (former), leading to the substitution (complementarity) of the benchmark efforts.

[17] We are implicitly ruling out communication and joint coordination of efforts by different parties.

[18] All proofs are given in the appendix.

3. Outsourcing Contracts

The firm outsources prevention and detection functions to one or more MSSPs. However, not all efforts exerted by MSSPs are observable. In practice, a firm may be able to observe and verify some of these efforts through periodic security audits, activity logs, and other means[19] but may not be able to observe or verify the MSSP's efforts related to monitoring and analysis of security alerts that require human diligence. The unobservable efforts are noncontractible; hence, the firm can only design a contract that is based on observed events. Such moral hazard is common in many contractual settings (Arrow 1971, Ross 1973, Holmstrom 1979, Harris and Raviv 1979, Grossman and Hart 1983). We denote the observable prevention effort and observable detection effort as e_p^0 and e_d^0, respectively. We assume $e_p^0 < e_p^*$ and $e_d^0 < e_d^*$ because moral hazard does not arise otherwise.

We first consider the 1-MSSP-penalty (1-MSSP-P) contract followed by the 2-MSSP contract. The reasons for analyzing these two contracts are the following. The 1-MSSP-P contract is common in the MSSP industry. In this contract, the firm outsources both prevention and detection services to the same MSSP and imposes a penalty if there is a breach for which the MSSP is responsible. In the 2-MSSP contract, prevention and detection services are outsourced to two different MSSPs. In addition to the analyses of the two popular contracts, we subsequently propose and analyze a third contract, a 1-MSSP-penalty-and-reward (1-MSSP-P-R) contract, and show that this contract is superior to the other two on various dimensions.

3.1. 1-MSSP-Penalty Contract

In a 1-MSSP-P contract, the firm outsources both prevention and detection services to the same MSSP and enters into a contract that has two components: $[F, p]$, where F is the up-front fixed fee paid by the firm to the MSSP and p is the penalty or refund the MSSP pays to the firm when a breach is detected and the MSSP is deemed to be at fault for the breach.[20] The postdetection response effort concludes whether the MSSP is responsible, and m is the probability that

[19] For instance, the contract between the city of Los Angeles and CSC has a provision to conduct security audits.

[20] Implicit in this contract is the assumption that the MSSP will always reveal a detected breach to the firm. This assumption is reasonable when the cost (e.g., reputation and litigation) to the MSSP of hiding the breach from the firm is very high. We discuss the impact of relaxing this assumption at the end of this subsection.

the MSSP will be liable for the breach.[21] The imperfectness of investigation comes from several sources. First, it is well known that attackers frequently delete system logs to avoid being later detected, thereby eliminating a valuable source of breach information useful in the postdetection investigation (Panko 2009). Second, contracts often include various disclaimers that are subject to multiple interpretations (Allen et al. 2003, Rittinghouse and Hancock 2003), making the investigation outcome imperfect. Under this contract, we assume that the firm bears $\gamma \in [0, 1]$ fraction of the postdetection response cost and the MSSP bears the rest of this cost.[22] The sequence of events is as follows.

Stage 1. The firm offers the contract $[F, p]$.

Stage 2. If the MSSP accepts the contract, it chooses e_p and e_d; otherwise, the game ends.

Stage 3. If a breach occurs and

Stage 3.1. if the breach is not detected, the firm incurs damage cost L;

Stage 3.2. if the breach is detected, the firm incurs damage cost αL; the MSSP and the firm incurs response costs of $(1-\gamma)C_r$ and γC_r, respectively; and the MSSP pays the firm p if the MSSP is held responsible.

The expected payoff for the firm and the MSSP are given by the following:

$$\pi_F = -F - \theta(e_p, N_p)(L - (L(1-\alpha) + pm - \gamma C_r)(\kappa + (1-\kappa)\phi(e_d, N_d))), \quad (4)$$

$$\pi_M = F - \theta(e_p, N_p)(\kappa + (1-\kappa)\phi(e_d, N_d))(pm + (1-\gamma)C_r) - C_p(e_p, N_p) - C_d(e_d, N_d) + \rho f(e_p, e_d, N_p, N_d). \quad (5)$$

We use backward induction to solve the firm's contracting problem.[23]

In Stage 2 of the game, the MSSP determines the optimum prevention and optimum detection efforts by maximizing π_M. The first derivative of π_M with respect to e_d is negative, implying that the MSSP's optimum detection effort will be equal to e_d^0. That is, the MSSP exerts only the base-level observable detection effort. This is intuitive because the MSSP expects to gain nothing by detecting a breach. On the contrary, by detecting a breach, the MSSP triggers an investigation that finds the MSSP responsible for the breach with probability m and results in an expected loss of pm to the MSSP. Therefore, the MSSP has no incentive to exert any detection effort beyond e_d^0 because detection effort is costly.

Also in Stage 2, the MSSP determines the optimum prevention effort by maximizing π_M after setting $e_d = e_d^0$. Anticipating how the MSSP will determine its best response in prevention effort, the firm solves the problem provided in Program 1-MSSP-P in Stage 1 of the game:

Program 1-MSSP-P

$$\max_{F,p} \{-F - \theta(e_p(p), N_p) \cdot (L - (L(1-\alpha) + pm - \gamma C_r)(\kappa + (1-\kappa)\phi(e_d^0, N_d)))\}$$

$$\text{s.t. } -\theta'_{e_p}(e_p(p), N_p)(\kappa + (1-\kappa)\phi(e_d^0, N_d)) \cdot (pm + (1-\gamma)C_r) - C'_{p\,e_p}(e_p(p), N_p) + \rho f'_{e_p}(e_p(p), e_d^0, N_p, N_d) = 0, \quad (IC_{e_p})$$

$$F - \theta(e_p(p), N_p)(\kappa + (1-\kappa)\phi(e_d^0, N_d)) \cdot (pm + (1-\gamma)C_r) - C_p(e_p(p), N_p) - C_d(e_d^0, N_d) + \rho f(e_p(p), e_d^0, N_p, N_d) \geq u. \quad (IR)$$

The firm maximizes its expected payoff by choosing the terms of the contract. IC_{e_p} denotes the MSSP's incentive compatibility constraint with respect to prevention effort. IR is the MSSP's individual rationality constraint, which guarantees a minimum expected payoff for the MSSP to accept the contract. The following proposition characterizes the solution to Program 1-MSSP-P, where $p^{\text{1-MSSP-P}}$ and $F^{\text{1-MSSP-P}}$ denote the optimal contract terms, and $e_p^{\text{1-MSSP-P}} \triangleq e_p^*(p^{\text{1-MSSP-P}})$ indicates the equilibrium prevention effort.

Proposition 2. *The solution to Program* 1*-MSSP-P has the following properties*:

(i) $p^{\text{1-MSSP-P}} = \dfrac{L - (L(1-\alpha) - \gamma C_r)(\kappa + (1-\kappa)\phi(e_d^0, N_d))}{m(\kappa + (1-\kappa)\phi(e_d^0, N_d))}$ *and*

$F^{\text{1-MSSP-P}} = \theta(e_p^{\text{1-MSSP-P}}, N_p) \cdot (L - (L(1-\alpha) - C_r)(\kappa + (1-\kappa)\phi(e_d^0, N_d))) + C_p(e_p^{\text{1-MSSP-P}}, N_p) + C_d(e_d^0, N_d) - \rho f(e_p^{\text{1-MSSP-P}}, e_d^0, N_p, N_d) + u.$

(ii) *The optimum penalty is greater than the total cost* (= *damage* αL + *response cost* γC_r) *the firm incurs from a detected breach*.

[21] The value of m is likely to depend on postdetection effort. Since postdetection response effort is exogenous in our model, we suppress the argument for m for notational brevity.

[22] Allen et al. (2003) argue that the client and provider may partially be responsible for the cost of remediation after the security incident. The client and the provider agree on the responsibilities and the process for handling incidents in the SLA of the contract.

[23] The equilibrium concept we use is the subgame perfect Nash (Fudenberg and Tirole 1998, p. 69).

(iii) *The equilibrium prevention effort is greater than the benchmark prevention effort*.

Proposition 2(i) characterizes the optimum 1-MSSP-P contract. We observe that the optimum penalty is increasing in L and α, as expected. The optimum penalty is decreasing in κ. Furthermore, it can be shown that the optimum penalty is decreasing in e_d^0, implying that if the extent of observable detection effort increases, the firm decreases the penalty. This is because the MSSP exerts only the detection effort the firm can observe. Any increase in the observable detection effort increases the marginal benefit of prevention and decreases the marginal cost of prevention for the MSSP. Thus, when the observable detection effort increases, the MSSP is inclined to increase prevention effort more than the firm prefers. Therefore, the firm decreases the penalty to offset the MSSP's enhanced incentive to exert more prevention effort.

An implication of Proposition 2(i) is that the penalty imposed under the 1-MSSP-P contract is likely to be high when the firm's ability to observe detection effort is limited or the postdetection investigation outcome is likely to favor the MSSP. However, Proposition 2(ii) shows that, regardless of the firm's ability to observe detection effort and the likelihood that investigation blames the MSSP for the breach, the penalty is larger than the total loss the firm incurs from a detected breach. This is because the firm does not always receive compensation from the MSSP for detected breaches, and, furthermore, the MSSP detects only a fraction of all breaches. Therefore, the firm compensates for the unrecovered loss by setting a penalty that is larger than the loss the firm incurs from a detected breach.

We note that the equilibrium detection effort in the 1-MSSP-P contract is smaller than the benchmark detection effort (i.e., $e_d^0 < e_d^*$). Proposition 2(iii) shows that the equilibrium prevention effort in the 1-MSSP-P contract is greater than the benchmark prevention effort, implying that the firm sets the contract terms in such a way that they induce more prevention effort to compensate for the reduction in detection effort. One would expect this outcome when the benchmark efforts are substitutes (i.e., when ρ is sufficiently low so that a high benchmark detection effort is accompanied by a low benchmark prevention effort). However, our finding reveals that this is true regardless of whether the benchmark efforts are substitutes or complements. The main intuition behind this unintuitive result is the following. In the 1-MSSP-P contract, the firm is faced with a constraint that it cannot induce a detection effort larger than the base-level effort, but there is no such constraint regarding detection effort in the benchmark scenario. In the benchmark scenario, the firm balances the two efforts, which results in a benchmark prevention effort smaller than the equilibrium prevention effort in the 1-MSSP-P contract, even when the benchmark efforts are complements.

The role of the cost of response effort on the optimal penalty is also insightful. We note that

$$mp^{\text{1-MSSP-P}} = \frac{L-(L(1-\alpha)-\gamma C_r)(\kappa+(1-\kappa)\phi(e_d^0,N_d))}{(\kappa+(1-\kappa)\phi(e_d^0,N_d))}$$
$$= L\left(\frac{1}{\kappa+(1-\kappa)\phi(e_d^0,N_d)}-1\right)+(\alpha L+\gamma C_r),$$

which reveals that, in the expected sense, the firm transfers the cost of response effort it incurs to the MSSP when a breach is detected. That is, although the firm incurs a response cost after each detection, the refund received from the MSSP when it is found liable fully pays for the firm's response cost. Therefore, an increase in response effort cost results in an increase in penalty and hence an increase in the prevention effort.

Two aspects of the 1-MSSP-P contract are worth noting. One, the contract does not provide any incentive for the MSSP to exert more than a base-level detection effort. Two, the contract imposes an excessive penalty (relative to the loss suffered by the firm) for a breach the MSSP is responsible for. The first aspect confirms the assertion of the proponents of separating the security prevention and detection functions regarding the conflict of interest present in prevailing security outsourcing contracts. The second aspect reveals that a contract in which the MSSP simply covers the entire loss of the firm when the MSSP is found liable for the breach, which is seemingly fair to both parties, is suboptimal for the firm.

Our model of the 1-MSSP-P contract assumes that the MSSP always reveals the breaches it detects to the firm. This is a reasonable assumption if the consequence of hiding a breach and being caught later is severe. In contrast, when detecting a breach is difficult, it is certainly conceivable that detecting the hiding of a breach is also likely to be difficult. Schneier (2002) also raised hiding breaches by MSSPs as a potential adverse outcome of 1-MSSP-P contracts. If we relax our model and allow the MSSP to decide whether to reveal or hide a breach from the firm, then we can show that under the 1-MSSP-P contract the MSSP will choose to hide all breaches from the firm if the consequence of this action is not sufficiently severe. This will have the equivalent effect of replacing $\phi(e_d^0, N_d)$ with 0 in Proposition 2, which exacerbates the adverse consequences of the 1-MSSP-P contract.

3.2. The 2-MSSP Contract

Under the 2-MSSP contract, the firm outsources the prevention function to one MSSP and the detection

function to a different MSSP. We label the MSSP that provides the prevention services M_P and the one that provides the detection services M_D. Clearly, the firm will use a penalty to incentivize M_P and reward to incentivize M_D. Thus, we assume that the firm offers a penalty-based contract $[F_P, p]$ to M_P and a reward-based contract $[F_D, r]$ to M_D. Parameters F (subscripted to denote the MSSP) and p have the same meanings as in the 1-MSSP-P contract. Parameter r denotes the reward the firm pays M_D for a breach it detects but the firm does not. Since our goal is to understand the implications of contract structures on prevention and detection of security breaches, we assume that the benefit and cost functions related to prevention and detection efforts remain the same as in the 1-MSSP-P contract. We note that since M_P exerts only prevention effort, its cost of effort is $C_p(e_p, N_p)$, and analogously, the cost of effort for M_D is $C_d(e_d, N_d)$. Also, we assume that M_P and M_D serve, respectively, N_p and N_d clients during the contract period, as in the 1-MSSP-P contract. We need this assumption to perform an "apples-to-apples" comparison of the various contracts—in the absence of such an assumption, the results of comparisons will be driven by the differences in client size in various contract structures rather than by the difference regarding whether prevention and detection functions are outsourced to the same MSSP or two different MSSPs. Further, we assume that the sum of the reservation payoffs of the two MSSPs in the 2-MSSP case is equal to the reservation payoff of the MSSP in the 1-MSSP-P contract. Finally, we assume that there is no collusion between the two MSSPs. The sequence of events under the 2-MSSP contract is as follows.

Stage 1. The firm offers the contract $[F_P, p]$ to M_P and the contract $[F_D, r]$ to M_D.

Stage 2. If both accept their respective contracts, then M_P chooses e_p and M_D chooses e_d; otherwise, the game ends.

Stage 3. If a breach occurs and

Stage 3.1. if neither the firm nor M_D detects it, the firm incurs damage cost L;

Stage 3.2. if the firm detects it, then the firm incurs damage cost αL, M_P and the firm incur response costs of $(1-\gamma)C_r$ and γC_r, respectively, and M_P pays the firm p if M_P is held responsible;

Stage 3.3. if the firm does not detect it and M_D does, then the firm incurs damage cost αL, and M_D receives r from the firm. M_P and the firm incur response costs of $(1-\gamma)C_r$ and γC_r, respectively, and M_P pays the firm p if M_P is held responsible.

The expected payoffs for the firm and the MSSPs are given by the following:

$$\pi_F = -F_D - F_P - \theta(e_p, N_p)\big(L - (L(1-\alpha) + pm - \gamma C_r) \cdot (\kappa + (1-\kappa)\phi(e_d, N_d)) + \phi(e_d, N_d)(1-\kappa)r\big), \quad (6)$$

$$\pi_{M_P} = F_P - \theta(e_p, N_p)(\kappa + (1-\kappa)\phi(e_d, N_d)) \cdot (pm + (1-\gamma)C_r) - C_p(e_p, N_p), \quad (7)$$

$$\pi_{M_D} = F_D + \theta(e_p, N_p)\phi(e_d, N_d)(1-\kappa)r - C_d(e_d, N_d). \quad (8)$$

The firm's problem is presented in Program 2-MSSP:

Program 2-MSSP

$$\max_{F_D, F_P, p, r} \big\{-F_D - F_P - \theta(e_p(p,r), N_p) \cdot (L - (L(1-\alpha) + pm - \gamma C_r)(\kappa + (1-\kappa) \cdot \phi(e_d(p,r), N_d)) + \phi(e_d(p,r), N_d)(1-\kappa)r)\big\}$$

s.t.

$$-\theta'_{e_p}(e_p(p,r), N_p)(\kappa + (1-\kappa)\phi(e_d(p,r), N_d)) \cdot (pm + (1-\gamma)C_r) - C'_{p_{e_p}}(e_p(p,r), N_p) = 0, \quad (IC_{e_p})$$

$$\theta(e_p(p,r), N_p)\phi'_{e_d}(e_d(p,r), N_d)(1-\kappa)r - C'_{d_{e_d}}(e_d(p,r), N_d) = 0, \quad (IC_{e_d})$$

$$F_P - \theta(e_p(p,r), N_p)(\kappa + (1-\kappa)\phi(e_d(p,r), N_d)) \cdot (pm + (1-\gamma)C_r) - C_p(e_p(p,r), N_p) \geq u_P, \quad (IR_P)$$

$$F_D + \theta(e_p(p,r), N_p)\phi(e_d(p,r), N_d)(1-\kappa)r - C_d(e_d(p,r), N_d) \geq u_D. \quad (IR_D)$$

The reservation payoffs of M_P and M_D are u_P and u_D, respectively, and $u = u_P + u_D$. The following proposition characterizes the solution to Program 2-MSSP, where $p^{\text{2-MSSP}}$; $F_P^{\text{2-MSSP}}$, $r^{\text{2-MSSP}}$, and $F_D^{\text{2-MSSP}}$ denote the optimum contract terms; and $e_p^{\text{2-MSSP}} \triangleq e_p^*(p^{\text{2-MSSP}}, r^{\text{2-MSSP}})$ and $e_d^{\text{2-MSSP}} \triangleq e_d^*(p^{\text{2-MSSP}}, r^{\text{2-MSSP}})$ refer to the equilibrium prevention and detection efforts, respectively.

Proposition 3. *The solution to Program* 2*-MSSP has the following properties*:

(i)

$$p^{\text{2-MSSP}} = \frac{L - (L(1-\alpha) - \gamma C_r)(\kappa + (1-\kappa)\phi(e_d^{\text{2-MSSP}}, N_d))}{m(\kappa + (1-\kappa)\phi(e_d^{\text{2-MSSP}}, N_d))},$$

$$r^{\text{2-MSSP}} = L(1-\alpha) - C_r,$$

$$F_P^{\text{2-MSSP}} = \theta(e_p^{\text{2-MSSP}}, N_p)(L - (L(1-\alpha) - C_r) \cdot (\kappa + (1-\kappa)\phi(e_d^{\text{2-MSSP}}, N_d))) + C_p(e_p^{\text{2-MSSP}}, N_p) + u_P,$$

$$F_D^{\text{2-MSSP}} = -\theta(e_p^{\text{2-MSSP}}, N_p)\phi(e_d^{\text{2-MSSP}}, N_d)(L(1-\alpha) - C_r) \cdot (1-\kappa) + C_d(e_d^{\text{2-MSSP}}, N_d) + u_D.$$

(ii) *The optimum penalty is greater than the total cost* (= *damage* αL + *response cost* γC_r) *the firm incurs from a detected breach.*

(iii) *Either the equilibrium prevention effort or the equilibrium detection effort is smaller than the corresponding benchmark effort*.

Proposition 3(i) offers several interesting insights about the optimum 2-MSSP contract structure. The reward provided to M_D is equal to the savings $L(1-\alpha)$ realized via damage recovery when a breach is detected less the cost of postdetection response effort C_r. The penalty expression function remains identical to that in the 1-MSSP-P contract, except that e_d^0 in the expression for the 1-MSSP-P contract is replaced by $e_d^{2\text{-MSSP}}$ for the expression in the 2-MSSP contract. We find it interesting that the reward expression suggests that M_D bears the brunt of the cost of response effort even though M_D is not responsible for the occurrence of breach in any way. Note that, as in the 1-MSSP-P contract, the firm fully transfers the cost of response effort it incurs to M_P through penalty when M_P is found to be liable for the breach. Therefore, even though the firm, in the expected sense, does not incur any net response cost, it reduces the reward to M_D by an amount equal to the total response cost. The intuition for this seemingly counterintuitive result comes from a closer look at how response cost affects the three parties. Consider the firm. As the leader of the game, the firm provides each MSSP with an expected payoff equal to its reservation wage; i.e., both (IR_P) and (IR_D) are binding in the equilibrium. Therefore, the firm's payoff is equal to the total joint payoff minus a constant term representing the sum of the reservation wages of the two MSSPs. That is, the firm sets penalty and reward parameters to induce those prevention and detection efforts that maximize the total joint payoff minus the sum of the reservation wages, as given by the following:

$$\begin{aligned}\Pi = &-\theta(e_p(p,r),N_p)\\ &\cdot(L-(L(1-\alpha)-C_r)(\kappa+(1-\kappa)\phi(e_d(p,r),N_d)))\\ &-C_p(e_p(p,r),N_p)-C_d(e_d(p,r),N_d)-u.\end{aligned}$$

Since the firm also needs to satisfy the IC conditions of MSSPs while maximizing the expression above, the optimal r and p must equalize the marginal payoffs of efforts for the firm and the MSSPs. We find that the cost of response effort reduces the marginal payoff of detection for the firm (i.e., $\partial(\partial\Pi/\partial e_d)/\partial C_r = -\theta(e_p(p,r),N_p)\phi'(e_d(p,r),N_d)(1-\kappa) < 0$). In contrast, response cost does not affect the marginal payoff of detection for M_D (i.e., $\partial(\partial\pi_{M_D}/\partial e_d)/\partial C_r = 0$). This is because M_D receives a reward from the firm for each breach it detects, regardless of whether the firm eventually transfers its cost of response effort to M_P. That is, under the 2-MSSP contract, the response cost creates an excess incentive to exert detection effort for M_D relative to the level the firm desires. Therefore, to align the M_D's incentives with its own, the firm is forced to decrease r when C_r increases. Furthermore, the marginal payoff of detection for the firm is affected by C_r but unaffected by γ, which explains why the firm decreases the reward by an amount equal to the total cost of response effort.

The response cost has a direct and an indirect effect on the optimal penalty in the 2-MSSP contract. Since the firm transfers the response cost to M_P when a breach is detected as part of penalty, an increase in response cost increases the penalty. This is because the response cost increases the marginal payoff of prevention for the firm at a higher rate than that for M_P (i.e., $\partial(\partial\pi_{M_p}/\partial e_p)/\partial C_r = (1-\gamma)\partial(\partial\Pi/\partial e_p)/\partial C_r > 0$). Hence, the firm increases the penalty to provide incentive for M_P. This is the direct effect of response cost, and this cost on penalty is also observed in the 1-MSSP-P contract, as seen from the discussion that followed Proposition 2. Furthermore, since response cost reduces the marginal payoff of detection for the firm, an increase in C_r decreases the induced detection effort, which in turn causes the firm to increase the penalty indirectly. This is the indirect effect of the response cost. Therefore, in the equilibrium, the firm balances the impact of the cost of response effort by reducing the reward to M_D and increasing the penalty to M_P.

Proposition 3(i) demonstrates that outsourcing the prevention and detection functions to separate MSSPs alleviates the conflict of interest faced by an MSSP when both functions are outsourced to it, in the sense that the firm induces a detection effort beyond the base observable level. However, separation of prevention and detection functions also creates a situation in which response cost alters the firm's and MSSPs' incentives to exert efforts in fundamentally different ways, and these incentives are misaligned. Aligning these incentives creates a strong interdependency between the contract parameters, requiring appropriate coordination of the two contracts. An adverse implication of this interdependency is that if the contract with one of the MSSPs—say, M_P—changes for any reason (e.g., change in the probability of prevention function), then the firm has to alter the contract for the other party (namely, M_D) as well.

We observe that the penalty is larger than the loss suffered by the firm for a detected breach, even in the 2-MSSP contract. The intuition behind this is the same as for the 1-MSSP-P contract. Additionally, we find that the reward offered to M_D for detecting a breach is strictly less than the benefit the firm receives from detection. The firm receives two benefits from detecting a breach: (i) it reduces the loss caused by the breach by an amount equal to $L(1-\alpha)-\gamma C_r$, and (ii) it receives compensation from M_P in the amount of $mp^{2\text{-MSSP}}$. However, the reward amount set by the firm is even less than the savings related to loss avoidance.

At least one of the two efforts induced by the 2-MSSP contract is smaller than the corresponding benchmark effort. As far as the firm is concerned, the response cost reduces the marginal payoff of detection effort but increases the marginal payoff of prevention effort. Although the response cost has the same qualitative impact on M_P, it does not affect M_D. Therefore, the firm is forced to coordinate the efforts of two MSSPs by setting incentives that are interdependent, a problem the firm does not face in the benchmark scenario. Further, the firm is unable to exploit the complementarity between the two efforts in the 2-MSSP scenario, which it is able to do in the benchmark scenario. For these two reasons, the firm induces a smaller effort for at least one of the security functions. We also note that the 2-MSSP contract, by design, eliminates the complementarity effect between prevention and detection functions. Consequently, this contract does not result in the maximum joint payoff that is realized in the benchmark setup in which the efforts are complementary.

In summary, the 2-MSSP contract eliminates the disincentive that exists in the 1-MSSP-P contract to exert detection effort beyond the base-level effort. However, it is unclear whether the 2-MSSP contract improves on the 1-MSSP-P contract. Intuitively, one would think that the 2-MSSP contract can never perform worse than the 1-MSSP-P contract because the firm has two degrees of freedom (i.e., penalty and reward) in choosing the optimum 2-MSSP contract, whereas it has one degree of freedom (i.e., penalty) in choosing the optimum 1-MSSP-P contract. However, as we show in the next result, the 2-MSSP contract is not necessarily better than the 1-MSSP-P contract on all performance dimensions.

Proposition 4. (i) $e_d^{\text{1-MSSP-P}} \leq e_d^{\text{2-MSSP}}$, (ii) $e_p^{\text{1-MSSP-P}} \geq e_p^{\text{2-MSSP}}$, (iii) $p^{\text{1-MSSP-P}} \geq p^{\text{2-MSSP}}$, *and* (iv) $\pi_F^{\text{2-MSSP}}$ *can be greater or smaller than* $\pi_F^{\text{1-MSSP-P}}$.

Proposition 4 reveals that the firm indeed imposes a smaller penalty (and induces a smaller prevention effort) under the 2-MSSP contract than under the 1-MSSP-P contract. This is because the firm is able to induce a higher level of detection effort in the 2-MSSP contract than in the 1-MSSP-P contract; therefore, inducing as much prevention effort in the 2-MSSP contract as in the 1-MSSP-P contract is not necessary. In essence, the firm sacrifices prevention in favor of more detection when it has the ability to control detection effort. Hence, the concern about the excessive penalty is somewhat mitigated in the 2-MSSP contract. However, as shown in Proposition 3, the penalty under the 2-MSSP contract is higher than the actual loss incurred by the firm because of the breach, so the concern is not fully eliminated. Further, an increase in the detection effort from the base-level detection effort exerted in the 1-MSSP-P contract also helps the firm detect security breaches more frequently. Notwithstanding these benefits, the 2-MSSP contract does not always increase the firm's overall payoff. The reason the 2-MSSP contract may perform worse than the 1-MSSP-P contract is because the 2-MSSP contract cannot take advantage of the complementarity between prevention and detection efforts, whereas the 1-MSSP-P contract can. Therefore, even though the detection effort is higher in the 2-MSSP contract than in the 1-MSSP-P contract, the detection effort does not reduce the marginal cost of prevention effort in the 2-MSSP contract. Consequently, the prevention effort is lower under the 2-MSSP contract than the 1-MSSP-P contract, which results in a higher likelihood of experiencing breaches and may lead to a larger overall loss for the firm.

Our analysis shows that although the 2-MSSP contract advocated by some security experts mitigates the conflict of interest problem present in the 1-MSSP-P contract, which leads to a small detection effort, it is not always optimal for the firm to use the 2-MSSP contract. This finding leads us to the question of whether another contract can be designed that preserves the good features and mitigates the bad features of the 1-MSSP-P and 2-MSSP contracts. We answer this question affirmatively and propose and analyze such a contract in the next section.

4. The 1-MSSP-Penalty-and-Reward Contract

In the proposed 1-MSSP-penalty-and-reward (1-MSSP-P-R) contract, the firm outsources both prevention and detection services to the same MSSP as in the 1-MSSP-P contract. However, the contracts differ in that the 1-MSSP-P-R contract has a reward component in addition to a penalty and fixed fee: $[F, p, r]$. That is, the firm offers the MSSP a reward of r when the MSSP detects a breach not detected by the firm or other third parties. Parameters F and p have the same meanings as in the penalty-based contract. The timeline under this contract, which is similar to the one used in 1-MSSP-P contract, is given below.

Stage 1. The firm offers the contract $[F, p, r]$ to the MSSP.

Stage 2. If the MSSP accepts the contract, it chooses e_p and e_d; otherwise, the game ends.

Stage 3. If a breach occurs and

Stage 3.1. if neither the firm nor the MSSP detects the breach, the firm incurs damage cost L;

Stage 3.2. if the firm detects it, then the firm incurs damage cost αL, the MSSP and the firm incur response costs of $(1-\gamma)C_r$ and γC_r, respectively, and the MSSP pays the firm p if the MSSP is held responsible;

Stage 3.3. if the firm does not detect it and the MSSP does, then the firm incurs damage cost αL and the MSSP receives r from the firm. The MSSP and the firm incur response costs of $(1-\gamma)C_r$ and γC_r, respectively, and the MSSP pays the firm p if the MSSP is held responsible.

The expected payoffs for the firm and the MSSP are given by the following:

$$\begin{aligned}\pi_F &= -F-\theta(e_p,N_p)\big(L-(L(1-\alpha)+pm-\gamma C_r)\\ &\qquad\cdot(\kappa+(1-\kappa)\phi(e_d,N_d))+(1-\kappa)\phi(e_d,N_d)r\big),\\ \pi_M &= F-\theta(e_p,N_p)\big((\kappa+(1-\kappa)\phi(e_d,N_d))(pm+(1-\gamma)C_r)\\ &\qquad-(1-\kappa)\phi(e_d,N_d)r\big)-C_p(e_p,N_p)-C_d(e_d,N_d)\\ &\qquad+\rho f(e_p,e_d N_p N_p).\end{aligned}$$

The firm's problem is provided in Program 1-MSSP-P-R.

Program 1-MSSP-P-R

$$\begin{aligned}\max_{F,p,r}\big\{&-F-\theta(e_p(p,r),N_p)(L-(L(1-\alpha)+pm-\gamma C_r)\\ &\cdot(\kappa+(1-\kappa)\phi(e_d(p,r),N_d))\\ &+(1-\kappa)\phi(e_d(p,r),N_d)r)\big\}\\ \text{s.t. }&-\theta'_{e_p}(e_p(p,r),N_p)((\kappa+(1-\kappa)\phi(e_d(p,r),N_d))\\ &\cdot(pm+(1-\gamma)C_r)-(1-\kappa)\phi(e_d(p,r),N_d)r)\\ &-C'_{p_{e_p}}(e_p(p,r),N_p)\\ &+\rho f'_{e_p}(e_p(p,r),e_d(p,r),N_p,N_d)=0, \qquad (IC_{e_p})\\ &-\theta(e_p(p,r),N_p)(1-\kappa)\phi'_{e_d}(e_d(p,r),N_d)\\ &\cdot(pm+(1-\gamma)C_r-r)-C'_{d_{e_d}}(e_d(p,r),N_d)\\ &+\rho f'_{e_d}(e_p(p,r),e_d(p,r),N_p,N_d)=0, \qquad (IC_{e_d})\\ &F-\theta(e_p(p,r),N_p)((\kappa+(1-\kappa)\phi(e_d(p,r),N_d))\\ &\cdot(pm+(1-\gamma)C_r)-(1-\kappa)\phi(e_d(p,r),N_d)r)\\ &-C_p(e_p(p,r),N_p)-C_d(e_d(p,r),N_d)\\ &+\rho f(e_p(p,r),e_d(p,r),N_p,N_d)\ge u. \qquad (IR)\end{aligned}$$

The following proposition presents the solution to Program 1-MSSP-P-R, where $p^{\text{1-MSSP-P-R}}$, $r^{\text{1-MSSP-P-R}}$, and $F^{\text{1-MSSP-P-R}}$ characterize the optimal contract terms and $e_p^{\text{1-MSSP-P-R}} \triangleq e_p^*(p^{\text{1-MSSP-P-R}}, r^{\text{1-MSSP-P-R}})$, $e_d^{\text{1-MSSP-P-R}} \triangleq e_d^*(p^{\text{1-MSSP-P-R}}, r^{\text{1-MSSP-P-R}})$ capture the equilibrium prevention and detection efforts, respectively.

Proposition 5. *The solution to Program* 1*-MSSP-P-R has the following properties.*

(i) *The optimal contract is given by the following*:

$$p^{\text{1-MSSP-P-R}} = \frac{L-\kappa(L(1-\alpha)-\gamma C_r)}{\kappa m}, \quad r^{\text{1-MSSP-P-R}} = \frac{L}{\kappa},$$

and $F^{\text{1-MSSP-P-R}}$

$$\begin{aligned}&= \theta(e_p^{\text{1-MSSP-P-R}}, N_p)\big(L-(L(1-\alpha)-C_r)\\ &\quad\cdot((\kappa+(1-\kappa)\phi(e_d^{\text{1-MSSP-P-R}}, N_d))\big)\\ &\quad+C_p(e_p^{\text{1-MSSP-P-R}}, N_p)+C_d(e_d^{\text{1-MSSP-P-R}}, N_d)\\ &\quad-\rho f(e_p^{\text{1-MSSP-P-R}}, e_d^{\text{1-MSSP-P-R}}, N_p, N_d)+u.\end{aligned}$$

(ii) *The optimum penalty is greater than the total cost* (= *damage* αL + *response cost* γC_r) *the firm incurs from a detected breach.*

(iii) *The equilibrium prevention and detection efforts are identical to the benchmark efforts.*

The notable features of the optimum 1-MSSP-P-R contract, in comparison to other two contracts, are the following.

a. As in the other two contracts, the penalty in the 1-MSSP-P-R contract transfers the expected cost of response effort incurred by the firm to the MSSP.

b. Unlike the 2-MSSP contract, however, the optimum reward is independent of the cost of response effort in the 1-MSSP-P-R contract. The reason for this difference is that although the response cost impacts the firm's payoff but does not impact the detection MSSP's payoff in the 2-MSSP contract, the response cost has (qualitatively) the same marginal impacts on the firm and the MSSP in the 1-MSSP-P-R contract. Hence, although the cost of response effort forces the firm to reduce the incentive of M_D to exert detection effort in the 2-MSSP contract, it does not when both prevention and detection efforts are exerted by the same MSSP. On the contrary, in the 1-MSSP-P-R contract, the reward amount exceeds the maximum potential loss the firm incurs from an undetected breach.

c. Like the other two contracts, the 1-MSSP-P-R contract does not eliminate the potential problem associated with excessive penalty because the penalty is larger than the loss suffered from a detected breach.

d. Finally, in sharp contrast to the other two contracts, the 1-MSSP-P-R contract induces the benchmark efforts for both prevention and detection functions.

Apart from achieving the benchmark efforts, the 1-MSSP-P-R contract possesses several desirable properties that the other two contracts do not. First, the optimal penalty and reward parameters are independent of N_p and N_d, which indicates that the externality effect of the MSSP network size does not play a role, at least with regard to setting the penalty and reward parameters. Second, the penalty and reward parameters are independent of the cost of prevention and detection efforts, eliminating the need for the firm to know the MSSP's cost functions to set penalty and reward parameters in the contract. The fixed fee still

depends on the cost functions, probability functions, and externality. However, we note that the fixed fee does not play any role in MSSP's choices of prevention and detection efforts, and therefore the firm uses the fixed fee not to induce the efforts it desires but to guarantee the reservation wage for the MSSP.

In summary, the 1-MSSP-P-R contract exhibits some of the positive features of both the 1-MSSP-P contract and the 2-MSSP contract, in addition to possessing other desirable characteristics. For instance, the 1-MSSP-P-R contract takes advantage of cost complementarity, as does the 1-MSSP-P contract; eliminates the problem related to the conflict of interest between prevention and detection, as does the 2-MSSP contract; and does not suffer from the problem of strong interdependency between the contract parameters, unlike the 2-MSSP contract. Naturally, the important question is how the contract parameters and equilibrium efforts and payoff in the 1-MSSP-P-R contract compare to the other two. The next result answers this question.

Proposition 6. (i) $p^{\text{1-MSSP-P-R}} \geq p^{\text{1-MSSP-P}} \geq p^{\text{2-MSSP}}$.
(ii) $r^{\text{2-MSSP}} \leq r^{\text{1-MSSP-P-R}}$.
(iii) $e_d^{\text{1-MSSP-P}} \leq e_d^{\text{2-MSSP}}, e_d^{\text{1-MSSP-P-R}}$.
(iv) $e_p^{\text{1-MSSP-P}} \geq e_p^{\text{1-MSSP-P-R}}, e_p^{\text{2-MSSP}}$.
(v) $e_p^{\text{1-MSSP-P-R}} < e_p^{\text{2-MSSP}} \Rightarrow e_d^{\text{1-MSSP-P-R}} > e_d^{\text{2-MSSP}}$ *and* $e_d^{\text{1-MSSP-P-R}} < e_d^{\text{2-MSSP}} \Rightarrow e_p^{\text{1-MSSP-P-R}} > e_p^{\text{2-MSSP}}$.
(vi) $\pi_F^{\text{1-MSSP-P-R}} \geq \pi_F^{\text{1-MSSP-P}}, \pi_F^{\text{2-MSSP}}$.

We find that the 1-MSSP-P-R contract sets the highest penalty and reward among the three contracts (Proposition 6, parts (i) and (ii)). The reason for this is the *dual* and *conflicting* role played by penalty and reward in this contract. For instance, consider penalty p. In the 1-MSSP-P-R contract, it is straightforward to see that p serves the intended purpose of affecting the fine paid by the MSSP if there is a breach that the MSSP is responsible for. More important, p also affects the net reward (which is equal to $r - mp$) offered to the MSSP if the MSSP is held responsible for the breach. That is, a higher penalty serves not only the role of inducing prevention effort but also the role of discouraging detection effort. Analogously, higher reward serves not only the role of inducing detection effort but also—by reducing the effective fine paid by the MSSP when it is found to be responsible for the breach—the role of discouraging prevention effort. In essence, both p and r affect the marginal benefits of both prevention and detection efforts of the MSSP in opposite directions. Consequently, it becomes necessary for the firm to set a high r and a high p to achieve the desired net reward and net penalty required to induce optimal prevention and detection efforts. Proposition 6(vi) clearly demonstrates the overall superiority of the 1-MSSP-P-R contract over the other two contracts. The 1-MSSP-P-R contract achieves the maximum payoff by setting the highest reward and the highest penalty among the three contracts. This strategy balances the trade-off between prevention and detection functions for a given response cost, so that prevention or detection effort in the 1-MSSP-P-R contract is not the highest among the three contracts (Proposition 6, parts (iii), (iv), and (v)).

The superiority of the 1-MSSP-P-R contract is demonstrated further by the following result.

Proposition 7. (i) *If* $\rho > 0$, *only* 1-*MSSP-P-R contract induces the benchmark efforts*.
(ii) *If* $\rho = 0$, *both* 1-*MSSP-R and* 2-*MSSP contracts induce the benchmark efforts*.

Proposition 7 provides partial (only under the condition $\rho = 0$) theoretical support to the argument that outsourcing the prevention and detection functions to two different MSSPs benefits the firm. In fact, when $\rho = 0$, Proposition 7 provides strong support to the above argument by showing that there is no contract that can be better for the firm from the payoff perspective. However, this result holds only under the restrictive and perhaps unrealistic case in which there is no complementarity between prevention and detection efforts. More important, our results show that even under this restricted case, the 1-MSSP-P-R contract achieves the same maximum payoff as the 2-MSSP contract, but it is much simpler to implement because of the several desirable properties it has. Finally, Proposition 7, along with the previous results, shows that the current practice of outsourcing both prevention and detection functions to the same MSSP using a penalty contract can lead to an inferior outcome for the firm, compared to the new contracts analyzed in this paper.

5. Model Extensions

In this section, we consider four model extensions to demonstrate that the results of this paper generalize to many other situations. We discuss only these extensions and their effects on the results. The detailed analysis and proofs are available from the authors upon request.

5.1. Uncertainty in Loss from a Breach

We assume that the loss from a breach is a deterministic constant L. Thus, our original model considers one type of breach incident. In this extension, we assume that the loss from a breach follows a probability distribution with a density function d and mean $\bar{L}$. All other aspects remain the same as in the original model. Since the exact loss from a breach is unknown to any player (under any contract and in the benchmark scenario), every player maximizes his expected payoff, taking into account the different possible loss

amounts while making the optimal choices. We find that the expected payoff for any player under any contract is derived by simply substituting L with $\bar{L}$ in the payoff expression shown earlier in §§2 and 3. Therefore, the results under this model variation can be obtained by simply substituting L with $\bar{L}$ in the results of the original model. Since the qualitative nature of our results is unaffected by deterministic loss, modeling uncertainty in loss does not change the qualitative nature of the results either.

5.2. Complementarity Between Benefits of Prevention and Detection Efforts

In the original model, we assume that prevention and detection efforts are complementary only on the cost side. In this model variation, we assume that the two efforts can complement each other on both the benefit and cost sides. To model this variation, we make the following changes to the original model.

a. The prevention probability function is changed to $\theta(e_p, n_p) - t \cdot h(e_p, e_d)$, $t \geq 0$, $h'_{e_d} > 0$, $h''_{e_p, e_d} > 0$. The second term in this expression captures the complementarity between prevention and detection efforts for the prevention probability.

b. The detection probability function is changed to $\phi(e_d, n_d) + b \cdot g(e_p, e_d)$, $b \geq 0$, $g'_{e_p} > 0$, $g''_{e_p, e_d} > 0$. The second term in this expression captures the complementarity between prevention and detection efforts for the detection probability.

Further, we assume the following:

$$\text{A1:} \quad \left(\frac{(1-\kappa)(\phi'(e_d^0, n_d) + g'_{e_d}(e_p, e_d)b)}{h'_{e_d}(e_p, e_d)} > \frac{t(\kappa + (1-\kappa)[\phi(e_d^0, n_d) + g(e_p, e_d)b])}{[\theta(e_p, n_p) - h(e_p, e_d)t]} \right).$$

The left-hand side of the condition stated in Assumption A1 represents the detection effort's marginal impact in increasing the detection probability relative to its marginal impact in decreasing breach probability. The condition states that this ratio is not too low, implying that the primary purpose of detection effort is to improve detection rather than to improve prevention.

$$\text{A2:} \quad \left(\left| \frac{(\theta'_{e_p}(e_p, N_p) - h'_{e_p}(e_p, e_d)t)}{g'_{e_p}(e_p, e_d)} \right| > \frac{b(1-\kappa)[\theta(e_p, N_p) - h(e_p, e_d)t]}{(\kappa + (1-\kappa)[\phi(e_d^0, N_d) + g(e_p, e_d)b])} \right).$$

A2 is analogous to A1 for the prevention effort. The left-hand side of the condition stated in Assumption A2 represents the prevention effort's (absolute) marginal impact in decreasing the breach probability relative to its marginal impact in increasing detection probability. The condition states that this ratio is not too low, implying that the primary purpose of the prevention effort is to decrease breach probability rather than to improve detection.

Although the expressions for the equilibrium prevention and detection efforts, optimal penalty, reward, and fixed fee are significantly more complex in this model variation, a comparison of the different contracts yields the same qualitative results as those shown in §§3 and 4.

5.3. Bargaining Between the Firm and the MSSP

In the original model, we assume that the firm has bargaining power over service providers and therefore offers a take-it-or-leave-it contract to the MSSP. In this variation, the firm and the MSSP bargain over the division of surplus created by the outsourcing relationship (Nash 1950). The bargaining strengths of parties impact only the right-hand side of the *IR* constraint (i.e., parties negotiate on the agent's payoff beyond the reservation wage and settle on a percentage of it). Regardless of the payoff to any party, when each party's share of the joint payoff is negotiated, the optimal penalty and reward under the any of three contracts will be chosen to give the MSSP(s) an incentive to exert efforts that maximize the joint payoff. In this framework, the party that offers the contract does not change the induced efforts or optimal contact terms except the fixed fee, which depends on how the joint payoff is distributed between the parties, depending on their bargaining power. As can be seen from the results shown in §§3 and 4, the fixed fee does not affect the comparison of contracts. Therefore, even if the firm and the MSSP(s) bargain over the contract(s), the qualitative comparisons of the three contracts remain the same as shown in this paper.

5.4. Dependence Between Postdetection Response Effort and Detection Effort

In the base model, we assume the cost of postdetection effort is a function of severity of damage from the breach L. In this extension, we model the case in which the response cost from postdetection activities depends not only on L but also on the extent of detection effort exerted by the MSSP. Specifically, we assume that more intensive detection effort reduces the cost of postdetection response. That is, we model response cost as $C_r(e_d; L, \alpha)$ and $C'_{r_{e_d}}(e_d; L, \alpha) < 0$. Furthermore, we assume that the detection effort's marginal impact in increasing the detection probability is higher than its marginal impact in decreasing the postdetection response cost. That is, $(1-\kappa)\phi'_{e_d}(e_d^0, N_d)(pm + (1-\gamma)C_r(e_d; L, \alpha)) > |(\kappa + (1-\kappa)\phi(e_d, N_d))(1-\gamma)C'_r(e_d; L, \alpha)|$.

Under this new model, it is straightforward to show that all results presented in this paper hold qualitatively.

6. Conclusions

One of the challenges in information security outsourcing is that neither the firm nor the MSSP perfectly observes the occurrence of security breaches. The prevalent practice is that firms mostly outsource both prevention and detection functions to the same MSSP using a contract that penalizes the MSSP when it is deemed responsible for a breach. Some security experts have advocated contracting with different providers for different security functions to deal with the conflict of interest issue associated with the single provider. Our analysis reveals that neither of these contracts may yield the benchmark outcome. Further, neither of these two contracts dominates the other in terms of the firm's payoff. The contract with a single MSSP results in the MSSP exerting less detection effort and more prevention effort, compared to the benchmark. Furthermore, the lack of adequate detection effort forces the firm to set a high penalty to prevent breaches under this contract. In contrast, though the contract that uses two MSSPs lessens the conflict of interest between two security functions and alleviates the problem of low detection, it also eliminates the advantages offered by complementarity of prevention and detection functions. Furthermore, it introduces a new form of inefficiency resulting from interdependency between the contracts, thereby requiring coordination in setting the contract terms. We showed that a contract in which the firm outsources both prevention and detection functions to a single MSSP and offers a reward to the MSSP for revealing security breaches and imposes a penalty if it is found responsible for the breach is superior to the other two contracts. The proposed contract achieves the benchmark efforts, whereas the other two contracts do not. This benefit is in addition to the benefit of not having to coordinate with two providers.

Our findings have interesting implications for practice. One of the main implications is that firms should rethink the nature of current contractual practices, not by outsourcing these two functions to two different MSSPs and radically changing the outsourcing arrangement, as suggested by some security experts, but by changing the contract structure within the existing arrangement that outsources both prevention and detection functions to the same MSSP. Second, contracts in which the MSSP providing prevention services compensates the firm for the entire loss incurred by the firm from a detected breach may not offer adequate incentives to the MSSP to exert prevention effort. In particular, the penalty compensation should exceed the loss the firm may incur from a detected breach to provide sufficient incentives for the MSSP to exert prevention effort. Third, analogous to penalty, the firm should provide a reward that is higher than the loss the firm suffers from an undetected breach to extract adequate detection effort.

We derived the analytical results by analyzing a fairly general model of a typical information security outsourcing context without assuming any specific cost or probability functions for the two types of security services. We also analyzed four variations of the base model to show the robustness of our qualitative findings to modeling assumptions. Despite this, our model has several limitations and can be extended in different directions. A valuable extension would be to analyze the impact of players' risk aversion on the optimum contract terms. Another interesting extension would be to consider a dynamic model, as opposed to the static one-shot model considered in this paper. A dynamic model would provide richer and more comprehensive insights into how MSSP contracts might evolve as the size of the MSSP network changes over time. Finally, issues related to incentives for MSSPs to commit fraud that were outside the scope of this paper can be examined in future research. For instance, the MSSP that gets a reward for detecting breaches may have an incentive to manufacture attacks and get rewarded for detecting them. The issue of how the contract should be designed to eliminate such incentives is another fruitful research direction.

Appendix

Proof of Proposition 1. By the implicit function theorem,

$$\begin{aligned}\frac{\partial e_p^*}{\partial e_d^*} &= -\frac{(\partial^2\Pi/\partial e_p\partial e_d)|_{e_p=e_p^*,e_d=e_d^*}}{(\partial^2\Pi/\partial e_p\partial e_p)|_{e_p=e_p^*,e_d=e_d^*}}\\ &= \big[(\theta'_{e_p}(e_p^*,N_p)(L(1-\alpha)-C_r)(1-\kappa)\phi'_{e_d}(e_d^*,N_d)\\ &\quad +\rho f''_{e_p,e_d}(e_p^*,e_d^*,N_p,N_d))\big]\\ &\quad \cdot\big[(\theta''_{e_p}(e_p^*,N_p)(L-(L(1-\alpha)-C_r)(\kappa+(1-\kappa)\phi(e_d^*,N_d)))\\ &\quad +C''_{p_{e_p}}(e_p^*,N_p)-\rho f''_{e_p}(e_p^*,e_d^*,N_p,N_d))\big]^{-1}.\end{aligned}$$

Therefore, e_p^* and e_d^* are substitutes, i.e., $\partial e_p^*/\partial e_d^* < 0$ if and only if the numerator of the above expression is negative, which yields the condition given in the proposition. □

Proof of Proposition 2. (i) The Lagrangian of Program 1-MSSP-P with λ and μ as the Lagrange multipliers on IC_{e_p} and IR is

$$\begin{aligned}L^{\text{1-MSSP-P}} &= -F-\theta(e_p,N_p)\\ &\quad\cdot(L-(L(1-\alpha)+pm-\gamma C_r)(\kappa+(1-\kappa)\phi(e_d^0,N_d)))\\ &\quad+\lambda(-\theta'_{e_p}(e_p,N_p)(\kappa+(1-\kappa)\phi(e_d^0,N_d))(pm+(1-\gamma)C_r)\\ &\quad-C'_{p_{e_p}}(e_p,N_p)+\rho f'_{e_p}(e_p,e_d^0,N_p,N_d))\\ &\quad+\mu(F-\theta(e_p,N_p)(\kappa+(1-\kappa)\phi(e_d^0,N_d))(pm+(1-\gamma)C_r)\\ &\quad-C_p(e_p,N_p)-C_d(e_d^0,N_d)+\rho f(e_p,e_d^0,N_p,N_d)-u).\end{aligned}$$

The first-order conditions for optimality are

$$\frac{\partial L^{\text{1-MSSP-P}}}{\partial F} = -1 + \mu = 0, \tag{9}$$

$$\frac{\partial L^{\text{1-MSSP-P}}}{\partial \mathrm{p}} = m(\theta(e_p, N_p) - \lambda\theta'_{e_p}(e_p, N_p) - \mu\theta(e_p, N_p)) = 0, \tag{10}$$

$$\begin{aligned}\frac{\partial L^{\text{1-MSSP-P}}}{\partial \lambda} &= -\theta'_{e_p}(e_p, N_p)(\kappa + (1-\kappa)\phi(e_d^0, N_d)) \\ &\quad \cdot (pm + (1-\gamma)C_r) - C'_{p_{e_p}}(e_p, N_p) \\ &\quad + \rho f'_{e_p}(e_p, e_d^0, N_p, N_d) = 0,\end{aligned} \tag{11}$$

$$\begin{aligned}\frac{\partial L^{\text{1-MSSP-P}}}{\partial \mu} &= F - \theta(e_p, N_p)(\kappa + (1-\kappa)\phi(e_d^0, N_d)) \\ &\quad \cdot (pm + (1-\gamma)C_r) - C_p(e_p, N_p) - C_d(e_d^0, N_d) \\ &\quad + \rho f(e_p, e_d^0, N_p, N_d) - u = 0.\end{aligned} \tag{12}$$

Substituting $\mu = 1$ from (9) in (10), we get $\lambda = 0$. Substituting $\mu = 1$, and $\lambda = 0$ in $L^{\text{1-MSSP-P}}$, $L^{\text{1-MSSP-P}}$ simplifies to

$$\begin{aligned}&L^{\text{1-MSSP-P}} \\ &= -\theta(e_p, N_p)(L - (L(1-\alpha) - C_r)(\kappa + (1-\kappa)\phi(e_d^0, N_d))) \\ &\quad - C_p(e_p, N_p) - C_d(e_d^0, N_d) + \rho f(e_p, e_d^0, N_p, N_d) - u.\end{aligned} \tag{13}$$

Taking the first derivative of (13) with respect to (w.r.t.) e_p, we obtain the following condition:

$$\begin{aligned}&-\theta'_{e_p}(e_p, N_p)(L - (L(1-\alpha) - C_r)(\kappa + (1-\kappa)\phi(e_d^0, N_d))) \\ &\quad - C'_{p_{e_p}}(e_p, N_p) + \rho f(e_p, e_d^0, N_p, N_d) = 0.\end{aligned} \tag{14}$$

Comparing (14) with IC_{e_p}, we obtain

$$\begin{aligned}&L - (L(1-\alpha) - C_r)(\kappa + (1-\kappa)\phi(e_d^0, N_d)) \\ &\quad = (\kappa + (1-\kappa)\phi(e_d^0, N_d))(pm + (1-\gamma)C_r),\end{aligned}$$

and solving for p, we get

$$p^{\text{1-MSSP-P}} = \frac{L - (L(1-\alpha) - \gamma C_r)(\kappa + (1-\kappa)\phi(e_d^0, N_d))}{m(\kappa + (1-\kappa)\phi(e_d^0, N_d))}. \tag{15}$$

Substituting (15) in (12), we get

$$\begin{aligned}F^{\text{1-MSSP-P}} &= u + \theta(e_p, N_p)(L - (L(1-\alpha) - C_r) \\ &\quad \cdot (\kappa + (1-\kappa)\phi(e_d^0, N_d))) + C_p(e_p, N_p) \\ &\quad + C_d(e_d^0, N_d) - \rho f(e_p, e_d^0, N_p, N_d),\end{aligned} \tag{16}$$

$$\begin{aligned}\text{(ii) } p^{\text{1-MSSP-P}} &= \frac{L - (L(1-\alpha) - \gamma C_r)(\kappa + (1-\kappa)\phi(e_d^0, N_d))}{m(\kappa + (1-\kappa)\phi(e_d^0, N_d))} \\ &= \frac{L}{m}\left(\frac{1}{\kappa + (1-\kappa)\phi(e_d^0, N_d)} - 1\right) \\ &\quad + \frac{\alpha L + \gamma C_r}{m} > \alpha L + \gamma C_r.\end{aligned}$$

(iii) $e_d^0 < e_d^*$ implies that the left-hand side (LHS) of (14) is greater than the LHS of (2) for any e_p. Hence, $e_p^{\text{1-MSSP-P}} > e_p^*$. □

Proof of Proposition 3. (i) Just as in the proof for Proposition 2, we construct the Lagrangian of Program 2-MSSP, $L^{\text{2-MSSP}}$ with $\lambda_P^{\text{2-MSSP}}$, $\lambda_D^{\text{2-MSSP}}$, $\mu_P^{\text{2-MSSP}}$, and $\mu_D^{\text{2-MSSP}}$, respectively, as the Lagrange multipliers on IC_{e_p}, IC_{e_d}, IR_P, and IR_D and take the first-order conditions as follows:

$$\frac{\partial L^{\text{2-MSSP}}}{\partial F_P} = -1 + \mu_P^{\text{2-MSSP}} = 0, \tag{17}$$

$$\frac{\partial L^{\text{2-MSSP}}}{\partial F_D} = -1 + \mu_D^{\text{2-MSSP}} = 0, \tag{18}$$

$$\begin{aligned}\frac{\partial L^{\text{2-MSSP}}}{\partial \mu_P} &= F_P - \theta(e_p, N_p)(\kappa + (1-\kappa)\phi(e_d, N_d)) \\ &\quad \cdot (pm + (1-\gamma)C_r) - C_p(e_p, N_p) - u_P = 0,\end{aligned} \tag{19}$$

$$\begin{aligned}\frac{\partial L^{\text{2-MSSP}}}{\partial \mu_D} &= F_D + \theta(e_p, N_p)\phi(e_d, N_d)(1-\kappa)r \\ &\quad - C_d(e_d, N_d) - u_D = 0,\end{aligned} \tag{20}$$

where a superscript 2-MSSP indicates the optimum value of that quantity under the 2-MSSP contract.

After substituting $\mu_P^{\text{2-MSSP}} = 1$ and $\mu_D^{\text{2-MSSP}} = 1$ from (17) and (18), $L^{\text{2-MSSP}}$ simplifies to

$$\begin{aligned}L^{\text{2-MSSP}} &= -\theta(e_p, N_p)(L - (L(1-\alpha) - C_r)(\kappa + (1-\kappa)\phi(e_d, N_d))) \\ &\quad - C_p(e_p, N_p) - C_d(e_d, N_d) - u_P - u_D \\ &\quad + \lambda_P^{\text{2-MSSP}}(-\theta'_{e_p}(e_p, N_p)(\kappa + (1-\kappa)\phi(e_d, N_d)) \\ &\quad \cdot (pm + (1-\gamma)C_r) - C'_{p_{e_p}}(e_p, N_p)) \\ &\quad + \lambda_D^{\text{2-MSSP}}(\theta(e_p, N_p)\phi'_{e_d}(e_d, N_d)(1-\kappa)r - C'_{d_{e_d}}(e_d, N_d)).\end{aligned}$$

Continuing with the remaining first-order conditions for optimality,

$$\frac{\partial L^{\text{2-MSSP}}}{\partial p} = -\lambda_P^{\text{2-MSSP}}\theta'_{e_p}(e_p, N_p)(\kappa + (1-\kappa)\phi(e_d, N_d))m = 0, \tag{21}$$

$$\frac{\partial L^{\text{2-MSSP}}}{\partial r} = \lambda_D^{\text{2-MSSP}}\theta(e_p, N_p)\phi'_{e_d}(e_d, N_d)(1-\kappa) = 0, \tag{22}$$

$$\begin{aligned}\frac{\partial L^{\text{2-MSSP}}}{\partial \lambda_P} &= -\theta'_{e_p}(e_p, N_p)(\kappa + (1-\kappa)\phi(e_d, N_d))(pm + (1-\gamma)C_r) \\ &\quad - C'_{p_{e_p}}(e_p, N_p) = 0,\end{aligned} \tag{23}$$

$$\frac{\partial L^{\text{2-MSSP}}}{\partial \lambda_D} = \theta(e_p, N_p)\phi'_{e_d}(e_d, N_d)(1-\kappa)r - C'_{d_{e_d}}(e_d, N_d) = 0. \tag{24}$$

From (21) and (22), we get $\lambda_P^{\text{2-MSSP}} = 0$ and $\lambda_D^{\text{2-MSSP}} = 0$. After substituting these, $L^{\text{2-MSSP}}$ simplifies to

$$\begin{aligned}L^{\text{2-MSSP}} &= -\theta(e_p, N_p)(L - (L(1-\alpha) - C_r)(\kappa + (1-\kappa)\phi(e_d, N_d))) \\ &\quad - C_p(e_p, N_p) - C_d(e_d, N_d) - u_P - u_D.\end{aligned} \tag{25}$$

Taking the first derivative of this Lagrangian w.r.t. e_p and e_d, we obtain the following conditions:

$$\begin{aligned}&-\theta'_{e_p}(e_p, N_p)(L - (L(1-\alpha) - C_r)(\kappa + (1-\kappa)\phi(e_d, N_d))) \\ &\quad - C'_{p_{e_p}}(e_p, N_p) = 0,\end{aligned} \tag{26}$$

$$\begin{aligned}&\theta(e_p, N_p)(L(1-\alpha) - C_r)(1-\kappa)\phi'_{e_d}(e_d, N_d) \\ &\quad - C'_{d_{e_d}}(e_d, N_d) = 0.\end{aligned} \tag{27}$$

Comparing (26) with (IC_{e_p}), we obtain

$$p^{\text{2-MSSP}} = \frac{L-(L(1-\alpha)-\gamma C_r)(\kappa+(1-\kappa)\phi(e_d,N_d))}{m(\kappa+(1-\kappa)\phi(e_d,N_d))}. \quad (28)$$

Comparing (27) with (IC_{e_d}), we obtain

$$r^{\text{2-MSSP}} = L(1-\alpha)-C_r. \quad (29)$$

Substituting (28) in (19) and (29) in (20), we get

$$F_P^{\text{2-MSSP}} = \theta(e_p,N_p)(L-(L(1-\alpha)-C_r)(\kappa+(1-\kappa)\phi(e_d,N_d))) + C_p(e_p,N_p)+u_P, \quad (30)$$

$$F_D^{\text{2-MSSP}} = -\theta(e_p,N_p)\phi(e_d,N_d)(L(1-\alpha)-C_r)(1-\kappa) + C_d(e_d,N_d)+u_D. \quad (31)$$

(ii) Comparing (28) with $\alpha L+\gamma C_r$ yields the result.

(iii) Suppose $e_d^{\text{2-MSSP}} > e_d^*$. Comparing (28) and (3), we conclude $\theta(e_p^{\text{2-MSSP}},N_p) > \theta(e_p^*,N_p) \Rightarrow e_p^{\text{2-MSSP}} < e_p^*$. Using the same reasoning, we can show that $e_p^{\text{2-MSSP}} > e_p^* \Rightarrow e_d^{\text{2-MSSP}} < e_d^*$ by comparing (26) and (2). □

Proof of Proposition 4. (i) Since $e_d^{\text{1-MSSP-P}} = e_d^0$ and e_d can never be smaller than e_d^0 under any contract, $e_d^{\text{1-MSSP-P}} \le e_d^{\text{2-MSSP}}$.

(ii) Comparing (14) and (27), using $e_d^0 \le e_d^*$, the LHS of (14) is greater than the LHS of (27). So $e_p^{\text{1-MSSP-P}} \ge e_p^{\text{2-MSSP}}$.

(iii) Since $e_d^{\text{2-MSSP}} \ge e_d^{\text{1-MSSP-P}} = e_d^0$ and $\frac{\partial p^{\text{2-MSSP}}}{\partial e_d} < 0$, $p^{\text{1-MSSP-P}} \ge p^{\text{2-MSSP}}$.

(iv) We prove this using a numerical example. Assume $N_p=10$, $N_d=10$, $L=1$, $\alpha=0.4$, $\kappa=0.2$, $m=0.5$, $C_r=0.1$, $\gamma=0.4$, $e_d^0=0.01$, and the following probability and cost functions:

$$\theta(e_p,N_p)=\frac{e^{-4e_p}}{N_p}, \quad \phi(e_d,N_d)=1-\frac{e^{-5e_p}}{N_d},$$

$$C(e_p,e_d,N_p,N_d)=\frac{0.5e_p^2}{N_p}+\frac{0.5e_d^2}{N_d}-\rho e_p e_d.$$

Contract type		π_F^*	p^*	r^*	e_p^*	e_d^*
1-MSSP-P	$\rho=0$	−0.01884	1.045	—	0.413	0.01
	$\rho=0.2$	−0.01801	1.045	—	0.420	0.01
2-MSSP	$\rho=0$ or 0.2	−0.01882	1.026	0.5	0.412	0.03

□

Proof of Proposition 5. (i) We construct the Lagrangian of Program 1-MSSP-P-R, $L^{\text{1-MSSP-P-R}}$, with λ_p, λ_d, and μ, respectively, as the Lagrange multipliers on IC_{e_p}, IC_{e_d}, and IR, and we take the first-order conditions as follows:

$$\frac{\partial L^{\text{1-MSSP-P-R}}}{\partial F} = -1+\mu = 0. \quad (32)$$

After substituting $\mu=1$ from (32) in $L^{\text{1-MSSP-P-R}}$ and continuing with the remaining first-order conditions,

$$\frac{\partial L^{\text{1-MSSP-P-R}}}{\partial p} = -m\big(\theta'_{e_p}(e_p,N_p)\lambda_p(\kappa+(1-\kappa)\phi(e_d,N_d)) + \theta(e_p,N_p)\lambda_d(1-\kappa)\phi'_{e_d}(e_d,N_d)\big)=0, \quad (33)$$

$$\frac{\partial L^{\text{1-MSSP-P-R}}}{\partial r} = \lambda_p\theta'_{e_p}(e_p,N_p)\phi(e_d,N_d) + \lambda_d\theta(e_p,N_p)\phi'_{e_d}(e_d,N_d)=0, \quad (34)$$

$$\frac{\partial L^{\text{1-MSSP-P-R}}}{\partial \lambda_p} = -\theta'_{e_p}(e_p,N_p)((\kappa+(1-\kappa)\phi(e_d,N_d)) \cdot(pm+(1-\gamma)C_r)-(1-\kappa)\phi(e_d,N_d)r) - C'_{p_{e_p}}(e_p,N_p)+\rho f'_{e_p}(e_p,e_d,N_p,N_d)=0, \quad (35)$$

$$\frac{\partial L^{\text{1-MSSP-P-R}}}{\partial \lambda_d} = -\theta(e_p,N_p)(1-\kappa)\phi'_{e_d}(e_d,N_d)(pm+(1-\gamma)C_r-r) - C'_{d_{e_d}}(e_d,N_d)+\rho f'_{e_d}(e_p,e_d,N_p,N_d)=0, \quad (36)$$

$$\frac{\partial L^{\text{1-MSSP-P-R}}}{\partial \mu} = F-\theta(e_p,N_p)\big((\kappa+(1-\kappa)\phi(e_d,N_d)) \cdot(pm+(1-\gamma)C_r)-(1-\kappa)\phi(e_d,N_d)r\big)-C_p(e_p,N_p) - C_d(e_d,N_d)+\rho f(e_p,e_d,N_p,N_d)-u=0. \quad (37)$$

Solving (33) and (34) simultaneously, we get $\lambda_p=0$ and $\lambda_d=0$. After substituting these values in the Lagrangian, it further simplifies to

$$L^{\text{1-MSSP-P-R}} = -\theta(e_p,N_p)(L-(L(1-\alpha)-C_r)(\kappa+(1-\kappa)\phi(e_d,N_d))) - C_p(e_p,N_p)-C_d(e_d,N_d)+\rho f(e_p,e_d,N_p,N_d)-u. \quad (38)$$

Taking the first derivative of this Lagrangian w.r.t. e_p and e_d, we obtain the following conditions:

$$-\theta'_{e_p}(e_p,N_p)(L-(L(1-\alpha)-C_r)(\kappa+(1-\kappa)\phi(e_d,N_d))) - C'_{p_{e_p}}(e_p,N_p)+\rho f'_{e_p}(e_p,e_d,N_p,N_d)=0, \quad (39)$$

$$(L(1-\alpha)-C_r)\theta(e_p,N_p)(1-\kappa)\phi'_{e_d}(e_d,N_d)-C'_{d_{e_d}}(e_d,N_d) + \rho f'_{e_d}(e_p,e_d,N_p,N_d)=0. \quad (40)$$

Comparing (40) with (36), we get

$$L(1-\alpha)-\gamma C_r = r-pm. \quad (41)$$

Comparing (39) with (35), we obtain

$$L=\big((\kappa+(1-\kappa)\phi(e_d,N_d))(pm+L(1-\alpha)-\gamma C_r) - (1-\kappa)\phi(e_d,N_d)r\big), \quad (42)$$

and substituting (41) in (42), we get

$$p^{\text{1-MSSP-P-R}} = \frac{L-\kappa(L(1-\alpha)-\gamma C_r)}{\kappa m}. \quad (43)$$

Substituting (43) in (41), we get

$$r^{\text{1-MSSP-P-R}} = \frac{L}{\kappa}. \quad (44)$$

Substituting (41) and (43) in (37), we obtain $F^{\text{1-MSSP-P-R}}$, as shown in the proposition.

(ii) Comparing (43) with $\alpha L+\gamma C_r$ yields the result.

(iii) Since the reservation payoff u of the MSSP in payoff expression (38) is a constant, the effort levels that maximize (1) are identical to those that maximize (38). □

Proof of Proposition 6. (i) Algebraic manipulation of $(p^{\text{1-MSSP-P-R}} - p^{\text{1-MSSP-P}})$ yields the result.

(ii) $r^{\text{2-MSSP}} = L(1-\alpha) - C_r \le r^{\text{1-MSSP-P-R}} = L/\kappa$.

(iii) Since $e_d^{\text{1-MSSP-P}} = e_d^0$ and $e_d > e_d^0$ under any contract, $e_d^{\text{1-MSSP-P}} \le e_d^{\text{1-MSSP-P-R}}, e_d^{\text{2-MSSP}}$.

(iv) Comparing (14) with (26) and (39), using $e_d^0 < e_d^{\text{1-MSSP-P-R}}, e_d^{\text{2-MSSP}}$, we can show that the LHS of (14) is greater than the LHS of (26) and the LHS of (39). Therefore, $e_p^{\text{1-MSSP-P}} \ge e_p^{\text{1-MSSP-P-R}}, e_p^{\text{2-MSSP}}$.

(v) Suppose $e_p^{\text{1-MSSP-P-R}} < e_p^{\text{2-MSSP}}$. Then, $\theta(e_p^{\text{1-MSSP-P-R}}, N_p) > \theta(e_p^{\text{2-MSSP}}, N_p)$. Comparing (27) and (40), we have that the LHS of (40) is greater than LHS of (27) for any given e_d when $e_p^{\text{1-MSSP-P-R}} < e_p^{\text{2-MSSP}}$. Therefore, e_d that satisfies (40) should be greater than e_d that satisfies (27). Analogously, we show $e_d^{\text{1-MSSP-P-R}} < e_d^{\text{2-MSSP}} \Rightarrow e_p^{\text{1-MSSP-P-R}} > e_p^{\text{2-MSSP}}$ using (26) and (39).

(vi) A 1-MSSP-P-R contract reduces to a 1-MSSP-P contract by setting $r = 0$. Hence, $\pi_F^{\text{1-MSSP-P-R}} \ge \pi_F^{\text{1-MSSP-P}}$. The firm's payoffs (in terms of e_p and e_d) in the 2-MSSP contract and 1-MSSP-P-R contract are, respectively,

$$\begin{aligned}
&-\theta(e_p, N_p)(L - (L(1-\alpha) - C_r)(\kappa + (1-\kappa)\phi(e_d, N_d))) \\
&\quad - C_p(e_p, N_p) - C_d(e_d, N_d) - u, \quad \text{and} \\
&-\theta(e_p, N_p)(L - (L(1-\alpha) - C_r)(\kappa + (1-\kappa)\phi(e_d, N_d))) \\
&\quad - C_p(e_p, N_p) - C_d(e_d, N_d) + \rho f(e_p, e_d, N_p, N_d) - u.
\end{aligned}$$

Comparing the two payoff functions, we find that for any e_p and e_d, the payoff under the 1-MSSP-P-R contract is not smaller than the payoff under the 2-MSSP contract. □

Proof of Proposition 7. The proof follows by comparing (1) with (13), (25), and (38) when $\rho > 0$ and when $\rho = 0$. □

References

Allen J, Gabbard D, May C (2003) Outsourcing managed security services. Security Improvement Module CMU/SEI-SIM-012, Carnegie Mellon Software Engineering Institute, Pittsburgh. http://www.cert.org/archive/pdf/omss.pdf.

Antle R (1982) The auditor as an economic agent. *J. Accounting Res.* 20(2, Part II):503–527.

Arbor Networks (2010) How to use Arbor products and services to deliver in-cloud managed security services. Report, Arbor Networks, Chelmsford, MA. http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=45.

Arrow K (1971) *Essays in the Theory of Risk-Bearing* (Markham, Chicago).

Baiman S, Evans JH, Noel J (1987) Optimal contracts with a utility-maximizing auditor. *J. Accounting Res.* 25(2):217–244.

Baker WH, Hutton A, Hylender CD, Novak C, Porter C, Sartin B, Tippett P, Valentine JA (2011) 2009 Data breach investigations report. Verizon Business, New York. http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

Butler Group (2007) Managed services: How managed services can help IT departments deliver greater value and flexibility. Report, Butler Group, Rockville, MD.

Caplan D (1999) Internal controls and the detection of management fraud. *J. Accounting Res.* 37(1):101–117.

Cavusoglu H, Mishra B, Raghunathan S (2004) The effect of internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *Internat. J. Electronic Commerce* 9(1):70–104.

Cezar A, Cavusoglu H, Raghunathan S (2009) Competition, speculative risks, and IT security outsourcing. *Eighth Workshop on Econom. of Inform. Security (WEIS 2009), London*.

Chen B (2012) All-or-nothing payments. *J. Math. Econom.* 48(3):133–142.

Dewatripont M, Jewitt I, Tirole J (2000) Multitask agency problems: Focus and task clustering. *Eur. Econom. Rev.* 44(4–6):869–877.

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. *Internat. Conf. Telecommunication Systems, Modeling, and Analysis, Dallas*, November 17–20.

Ding W, Yurcik W (2006) Economics of Internet security outsourcing: Simulation results based on the Schneier model. *Workshop on the Economics of Securing the Information Infrastructure (WESII), Washington, DC*, October 23.

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*, Lecture Notes in Computer Science, Vol. 3828 (Springer, Berlin), 947–958.

Feltham G, Xie J (1994) Performance measure congruity and diversity in multi-task principal/agent relations. *Accounting Rev.* 69(3):429–453.

Frost & Sullivan (2010) Global managed security service providers rollup. Report, Frost & Sullivan, San Antonio, TX.

Fudenberg D, Tirole J (1998) *Game Theory* (MIT Press, Cambridge, MA).

Gaudin S (2007) Security breaches cost $90 to $305 per lost record. *InformationWeek* (April 11), http://www.informationweek.com/security-breaches-cost-90-to-305-per-los/199000222.

Grossman SJ, Hart OD (1983) An analysis of the principal-agent problem. *Econometrica* 51(1):7–45.

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

Harris M, Raviv A (1979) Optimal incentive contracts with imperfect information. *J. Econom. Theory* 20(2):231–259.

Holmstrom B (1979) Moral hazard and observability. *Bell J. Econom.* 10(1):74–91.

Holmstrom B, Milgrom P (1991) Multitask principal–agent analysis: Incentive contracts, asset ownership, and job design. *J. Law, Econom., Organ.* 7:24–52.

Holmstrom B, Milgrom P (1994) The firm as an incentive system. *Amer. Econom. Rev.* 84(4):972–991.

IBM (2007) IBM Managed Security Services. Report, IBM Global Services, Somers, NY. http://www-935.ibm.com/services/us/iss/pdf/gtd00763-usen-01.pdf.

IRCTC (2011) Request for proposal (RFP) for managed security services (MSS)—2011. RFP document, Indian Railway Catering and Tourism Corporation, New Delhi. https://www.irctc.co.in/betaDoc/tender_Managed_Services.pdf.

Itoh H (1991) Incentives to help in multi-agent situations. *Econometrica* 59(3):611–636.

Itoh H (1994) Job design, delegation, and cooperation: A principal-agent analysis. *Eur. Econom. Rev.* 38(3–4):691–700.

Johnson M (2005) Why outsource to a managed security service provider (MSSP)? White paper, Webfargo Data Security, Durham, NC.

Kark K (2010) Market overview: Managed security services. Report, Forrester Research, Cambridge, MA.

Kavanagh KM, Pescatore J (2009) Magic Quadrant for MSSPs, North America. Gartner RAS Core Research Note G00166138, Gartner, Stamford, CT. http://www.tatacommunications.com/downloads/enterprise/Tata_Communications_3053.pdf.

Lacity MC, Khan SA, Willcocks LP (2009) A review of the IT outsourcing literature: Insights for practice. *J. Strategic Inform. Systems* 18(3):130–146.

LaPiedra J (2002) The information security process: Prevention, detection and response. Report, SANS Institute, Bethesda, MD. http://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197.

MacDonald G, Marx LM (2001) Adverse specialization. *J. Political Econom.* 109(4):864–899.

Nash JF Jr (1950) The bargaining problem. *Econometrica* 18(2): 155–162.

Panko R (2009) *Corporate Computer and Network Security*, 2nd ed. (Prentice-Hall, Upper Saddle River, NJ).

Ponemon Institute (2011) Ponemon study shows the cost of a data breach continues to increase. Press release (January 25), Ponemon Institute, Menlo Park, CA. http://www.ponemon.org/news-2/23.

Rittinghouse JW, Hancock WM (2003) *Cybersecurity Operations Handbook* (Elsevier Digital Press, Amsterdam).

Roiter N (2009) How to build the right managed security service level agreement. SearchMidmarketSecurity.com, (August 6), http://searchmidmarketsecurity.techtarget.com/news/1363812/How-to-build-the-right-managed-security-service-level-agreement.

Ross SA (1973) The economic theory of agency: The principal's problem. *Amer. Econom. Rev.* 63(2):681–690.

Rowe (2007) Will outsourcing IT security lead to a higher social level of security? *Sixth Workshop on the Economics of Information Security, Pittsburgh*, June 7–8.

Schneier B (2001) Managed security monitoring: Network security for the 21st century. *Comput. Security* 20(6):491–503.

Schneier B (2002) The case for outsourcing security. *Computer* 35(4):20–26.

Schneier B (2007) Managed security monitoring: Network security for the 21st century. Report, British Telecommunications, London. http://www2.computable.nl/downloads/Counterpane_WP5.pdf.

Schneier B (2011) Personal communication via email with the authors, January 25.

Schwartz MJ (2010) More firms outsourcing security to MSSPs. *InformationWeek* (June 17), http://www.informationweek.com/security/management/more-firms-outsourcing-security-to-mssps/225700537.

Sridhar SS, Balachandran BV (1997) Incomplete information, task assignment, and managerial control systems. *Management Sci.* 43(6):764–778.

Whang S (1992) Contracting for software development. *Management Sci.* 38(3):307–324.

Whitman ME, Mattord HJ (2011) *Principles of Information Security*, 4th ed. (Cengage Learning, Boston).

Zhao X, Whinston A (2013) Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *J. Management Inform. Systems* 30(1):123–152.