

Outsourcing Information Security: Contracting Issues and Security Implications

Asunur Cezar
Middle East Technical University
Northern Cypress Campus
Kalkanlı, Güzelyurt, KKTC, Mersin 10, Turkey
asunur@metu.edu.tr

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

Abstract

We examine the implications of a firm outsourcing both (i) security device management which attempts to prevent security breaches and (ii) security monitoring which attempts to detect security breaches to managed security service providers (MSSPs). In the context of security outsourcing, the firm not only faces the traditional moral hazard problem as it cannot observe an MSSP's prevention or detection effort, but also observes the security breach outcome only imperfectly. Furthermore, outsourced prevention and detection services are separate but interrelated security functions, and thereby cannot be considered independently. Hence, the firm needs to carefully design a contract or contracts to induce the desired efforts from the service providers to effectively manage the cost of information security. We first show that the current practice of outsourcing both device management and monitoring functions to the same MSSP using a contract that imposes a penalty on MSSP when the MSSP is deemed responsible for a breach results in a higher than the first-best prevention effort and zero (and less than the first-best) detection effort. This is due to the conflict of interest faced by the MSSP and the substitutable nature of prevention and detection services. We then propose two new contracts, both of which achieve the first-best outcomes. The first contract imposes a penalty for a breach and offers a reward for detecting and revealing breaches to the firm and the second contract calls for the firm to use two different MSSPs - one for prevention and the other for detection. The required penalty and reward are smaller when the firm uses two MSSPs than when it uses a single MSSP. It is possible for all three types of contracts to fail to satisfy the fairness criterion – the penalty does not exceed the firm's loss from a security breach -, and also fail to achieve the first-best efforts when there are limits on penalty and/or reward. However, the two-MSSP contract meets the fairness criterion whenever the other two contracts do. An increase in the prevention cost relative to the detection cost increases the likelihood that the two-MSSP contract meets the fairness criterion, making the two-MSSP contract even more attractive relative to the single MSSP contract with penalty and reward. Despite these advantages of the two-MSSP contract over single MSSP contracts, the firm may be better off outsourcing both prevention and detection functions to the same MSSP with a penalty-and-reward-based contract if a strong cost complementarity exists between the two functions.

May 2010

1. Introduction

Information security management has become a critical and challenging business function because of reasons such as rising cost of security breaches¹, increasing scale, scope and sophistication of information security attacks, complexity of information technology (IT) environments, shortage of qualified security professionals, diverse security solutions from vendors, 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 The popular security functions outsourced include firewall and virtual private network (VPN) management, which seeks to protect a firm from security breaches and avoid a potential loss, and security monitoring, which attempts to detect breaches and recover some of the loss. As in many other outsourcing contexts, moral hazard is a potential problem in information security outsourcing also because the firm cannot observe or verify the efforts spent by the MSSP. Furthermore, in the information security context, the firm is confronted with the following challenges that give rise to additional incentive problems. One, neither the firm nor the MSSP observes the *outcome* of the MSSP's efforts (viz., whether the firm's security has been breached or not) perfectly (Baker et al. 2009). Two, the MSSP may choose not to report breaches only it detects to the firm. Finally, decisions regarding prevention efforts affect decisions regarding detection efforts and vice versa requiring the firm to coordinate the two outsourced functions. Therefore, a key question that arises in information security outsourcing is how the contract should be structured by the firm to incentivize the MSSPs and coordinate the prevention and detection efforts.

We analyze this question by first considering the current practice of outsourcing both device management and monitoring functions to the same MSSP using a penalty/refund-based contract in which the MSSP is penalized in the form of a refund to the firm when a breach occurs and the MSSP is deemed

¹ The average total cost of a data breach, which includes the cost of recovery, lost productivity costs, and customer opportunity costs, ranges from \$90 to \$305 for each breached customer record (Gaudin 2007).

² In 2006, 60% of Fortune 500 companies had used an MSSP and about 20% of enterprise firewalls were under remote monitoring or management (Gartner 2007).

to be responsible for the breach. We show that this contract results in a prevention effort that is higher than the first-best prevention effort and zero (and less than the first-best) detection effort. The results of the analysis of penalty/refund contract led us to propose and analyze two other contracts. The first one offers a reward to the MSSP for detecting and revealing breaches to the firm and imposes a penalty if the MSSP is deemed to be responsible for a breach, and the second calls for the firm to use two different MSSPs - one for prevention and the other for detection. We show that both of these contracts achieve the first-best prevention and detection efforts. However, the required penalty and reward for achieving the first-best outcomes are smaller when the firm uses two MSSPs than when it uses a single MSSP.

Not all contracts are feasible. In particular, institutions such as courts could provide limits on the penalty based on a fairness criterion. For example, in the context of outsourcing manufacturing operations, courts have refused to enforce terms contained in outsourcing contracts that are deemed unfair, such as excessive penalty for poor performance (Starkman 1997). Therefore, we also analyze the feasibility of different contracts based on a fairness criterion – that is, the penalty does not exceed the firm’s loss from a security breach. We show that all three types of contracts may fail to satisfy the fairness criterion. Furthermore, when there are limits on penalty and/or reward, all three contracts may fail to achieve the first-best efforts. However, the two-MSSP contract meets the fairness criterion (and/or achieves the first-best outcomes) whenever the other two contracts do, but the reverse does not occur.³ An increase in the prevention cost relative to the detection cost increases the likelihood that the two-MSSP contract meets the fairness criterion, making the two-MSSP contract more attractive relative to the single MSSP contracts under high prevention cost and/or low detection cost environments. Despite these advantages of the two-MSSP contract over single MSSP contracts, we show that the firm may be better-off outsourcing both prevention and detection services to a single MSSP with a penalty-and-reward-based contract if a strong cost complementarity exists between the two functions.

³ The single MSSP contract that only has penalty never achieves the first-best efforts.

The results provide important insights about and implications for security outsourcing. For example, in many contexts hiring two different agents to perform two related services may introduce an additional moral hazard problem and a new source of inefficiency (Baiman et al. 1987), and hiring a single agent to perform both services may mitigate this inefficiency. However, in security outsourcing context, the dual and conflicting roles of penalty and reward in incentivizing a single outsourcer to provide the optimum levels of prevention and detection efforts makes outsourcing these functions to two different MSSPs superior to outsourcing them to a single MSSP. However, the benefit of using two MSSPs comes at the expense of not exploiting the complementarities that may exist between prevention and detection efforts. This tradeoff is crucial when choosing to outsource information security. The current practice of outsourcing both device management and device monitoring to the same outsourcer using a simple penalty-based contract creates a conflict of interest between the two services for the MSSP and leads to an inferior outcome for the firm..

The results provide theoretical support and additional insights into concerns expressed by information security experts regarding security outsourcing. For instance, the information security community has recognized the concern regarding the incentive for a MSSP that is responsible for both device management and monitoring to hide security breaches from the firm, which has led to a prediction about the eventual disappearance of providers offering both of these services together (Schneier 2002). Our results provide partial theoretical support to the claim about hiding of security breaches; while the claim holds under the currently adopted penalty-based contract, it does not hold if firms adopt the penalty-and-reward-based contract we have proposed. Further, whether the single-source MSSP offering both device management and monitoring will survive in the future may depend on factors such as cost of prevention relative to the cost of detection and the extent of complementarity between prevention and detection. If the scale and scope of future security breaches is such that the cost of preventing them increases so much that the firms manage security risks by focusing more on detection, then single-source MSSPs are less likely to survive in the future. On the other hand, if the sophistication of future security attacks is such that detecting them ex post proves costly and firms focus more on prevention, then single-

source MSSPs are less likely to vanish in the future. Of course, strong complementarity between prevention and detection services also favors the single-source MSSPs.

1.1 Related Literature

Since the present paper concerns the study of outsourcing contracts, the paper is related to the vast literature on outsourcing both in IT and in other contexts such as manufacturing (see, e.g., Lacity, Khan, and Willcocks (2009) for a survey of IT outsourcing literature). Rather than attempting to identify the linkage between present paper and the voluminous outsourcing literature, we confine discussion of references here to the part of the literature dealing with analytical models in IT and information security contracting. In one of the earliest papers on IT outsourcing, Whang (1992) analyzed a multi-period software development contract between a firm and an outside developer and derived an optimal contract which replicates the equilibrium outcome of a benchmark in-house development. More recently, Dey et al. (2008) 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, Ding et al. (2005a, 2005b, 2006) examined the characteristics of optimal MSSP contracts under moral hazard and reputation effects and found that an optimal contract should be performance based even in the existence of a strong reputation effect, and that outsourcing decision is relatively insensitive to variation in service quality but highly sensitive to bankruptcy risk. Gupta and Zhdanov (2007) examined the growth of a MSSP network under a for-profit MSSP monopoly and under a consortium-based market structure. The information security as well as the traditional IT outsourcing literature assumes that there is a single type of service that is outsourced. For instance, information security outsourcing assumes that only prevention services are outsourced and the general IT outsourcing assumes that software development is outsourced. On the other hand, we consider outsourcing two different but related security services. 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.

The present paper is also related to auditing research in the accounting area (see e.g., Antle 1982, Baiman, Evans, and Noel 1987, Caplan 1999). In a typical auditing context, a principal contracts with an agent and an auditor. The key difference between the present 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, 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. 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 or destructive), but in the security context both prevention and detection efforts are productive and the firm's problem is one of coordinating in addition to incentivizing the parties that provide these efforts.

The paper proceeds as follows. Section 2 outlines the base model and presents the “first-best” results as the benchmark for analyzing the various contracts. Section 3 analyzes the penalty-based, penalty-and-reward-based, and the two-MSSP contracts. This section also compares the contracts based on a fairness criterion. Section 4 presents results about the impact of limits on penalty and reward as well as prevention and detection costs on the optimum contracts. Section 5 provides an analysis of two extensions of the base model and section 6 concludes the paper with a summary of main results.

2. The Model

We consider a firm that has decided to outsource services related to the prevention and detection of security breaches. An undetected security breach and a detected security breach, respectively, inflict a total monetary loss of L and αL , $0 \leq \alpha < 1$, on the firm.⁴ The parameter L includes tangible costs, such as the revenue loss from disruption of services, and intangible costs, such as those associated with the loss

⁴ Schneier (2001) points out, “if you [the firm] can respond quickly and effectively, you [the firm] can repel the attacker before he does any damage. Good detection and response can make up for imperfect prevention.” See also, the news article about a bank recovering about 75% of the loss after it was alerted about a security breach related to identity theft (Case 2010).

of reputation and customer distrust (Cavusoglu et al. 2004).⁵ The probability of a breach, $\theta(e_p)$, is a decreasing convex function of the prevention effort, e_p , exerted by the MSSP, i.e., $\theta'(e_p) < 0, \theta''(e_p) \geq 0$. The cost of prevention effort, $C_p(e_p)$, is an increasing convex function of e_p , i.e., $C_p'(e_p) > 0, C_p''(e_p) \geq 0$. Even in the absence of any detection effort, there is a fixed probability $\kappa < 1$ with which a breach can be detected by the firm. The parameter κ models the observation that security breaches sometimes are detected by employees during the course of normal work or are publicly observable (such as denial of service attacks) without the need for detection effort.⁶ We restrict κ and α to be strictly less than one to ensure that detection offers a strictly positive value to the firm. The probability of the MSSP detecting a breach that requires detection effort, $\phi(e_d)$, is an increasing concave function of detection effort, e_d , exerted by the MSSP, i.e., $\phi'(e_d) > 0, \phi''(e_d) \leq 0$. The cost of detection effort, $C_d(e_d)$, is an increasing convex function of e_d , i.e., $C_d'(e_d) > 0, C_d''(e_d) \geq 0$. In other words, we make the standard assumption that efforts exhibit a declining marginal utility and an increasing marginal cost. We also assume that the absolute and marginal cost of no prevention is zero and the marginal cost of full prevention (i.e., zero breach) is sufficiently high, that is $C_p(\arg(\theta(e_p)=1)) = C_p'(\arg(\theta(e_p)=1)) = 0$ and $C_p'(\arg(\theta(e_p)=0)) = \infty$. Similarly, we assume $C_d(\arg(\phi(e_d)=0)) = C_d'(\arg(\phi(e_d)=0)) = 0$ and $C_d'(\arg(\phi(e_d)=1)) = \infty$. These assumptions are necessary to ensure an interior solution for the optimal prevention and detection efforts. Our model implies that there is no complementarity between prevention and detection efforts⁷. All parties are risk neutral and model parameters are common knowledge.

2.1 Benchmark: First-Best Efforts

⁵ We assume that a security breach inflicts a fixed damage. However, our analysis can easily be extended to the stochastic damage case.

⁶ According to 2009 Data Breach Investigation Report, 13% of breaches are detected by employees during normal work activities (Baker et al. 2009).

⁷ We discuss the implications of complementarity between prevention and detection efforts in Section 5.1.

The expected joint payoff can be written as

$$\Pi = -\theta(e_p)L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - C_p(e_p) - C_d(e_d)$$

Then, the optimization problem for the first-best efforts is

$$\text{Max}_{e_p, e_d} \Pi \quad (1)$$

We assume that $\left| \frac{\partial^2 \Pi}{\partial e_p^2} \right| > \left| \frac{\partial^2 \Pi}{\partial e_p \partial e_d} \right|$ and $\left| \frac{\partial^2 \Pi}{\partial e_d^2} \right| > \left| \frac{\partial^2 \Pi}{\partial e_p \partial e_d} \right|$ to ensure the concavity of the objective function in

e_p and e_d , and hence a unique optimal solution for our problem (Tirole 1990). The first-best effort levels, e_d^* and e_p^* , are obtained by solving the following simultaneous equations.

$$\left. \frac{\partial \Pi}{\partial e_p} \right|_{e_d=e_d^*, e_p=e_p^*} = -\theta'(e_p^*)L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d^*))) - C'_p(e_p^*) = 0 \quad (2)$$

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

Equations (2) and (3) show that in the first-best solution, for each effort, the marginal benefit and the marginal cost are set equal. The assumptions regarding the marginal costs of prevention and detection ensure that the first-best prevention and detection efforts are positive and finite.

An examination of the first-best solution gives rise to the following result⁸.

PROPOSITION 1. (1) *When the cost of prevention effort increases, the first-best prevention effort decreases and the first-best detection effort increases.*

(2) *When the cost of detection effort increases, the first-best prevention effort increases and the first-best detection effort decreases.*

Proposition 1 implies that prevention and detection efforts are substitutes from the social welfare perspective to manage the cost of security. The substitution effect between the prevention and detection efforts arises because an increase in the prevention effort decreases the likelihood of a breach, which, in turn, reduces the expected benefit from detection services and, therefore, the detection effort. A similar

⁸ All proofs are given in appendix A.

reasoning applies when the detection effort increases. Further, it is straightforward to show that if κ or α decreases (i.e., detection becomes more valuable), the first-best detection effort increases and the first-best prevention effort decreases. We next proceed to analyze the contracting game.

3. Unobservable MSSP Efforts

The firm outsources the prevention and detection services to a MSSP. The MSSP's efforts are unobservable and non-contractible; hence the firm induces the MSSP to choose the optimum efforts using contracts that are based on observed breach 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 first consider the penalty-based contract which appears to be the most prevalent one in the MSSP industry.

3.1 Penalty-Based Contract

The penalty-based contract has two components: $[F, p]$, where F is the up-front fee paid by the firm to the MSSP, and p is the penalty or refund the MSSP pays the firm if the firm becomes aware of the breach and the MSSP is deemed responsible for the breach. An example for this contract is the IBM's service level agreement (SLA) that provides US\$50,000 to the client firm for any security breach listed in the contract (IBM Managed Protection Services SLA)⁹. However, not all contracts are feasible. Specifically, courts could provide limits on the level of penalty based on a fairness criterion. For example, a contract that imposes a penalty that is higher than the actual loss suffered by the firm may be deemed unfair. We do not assume any limits on p in the base model, but we discuss the implications of liability limits in Section 4.1.

The firm becomes aware of a breach if the firm detects the breach on its own (i.e., the breach is publicly observable) or if the MSSP detects and reveals the breach to the firm. The penalty is imposed on the MSSP only if it is found to be negligent in its services and therefore responsible for the breach. An independent investigation concludes whether or not the MSSP is at fault and m , $0 < m \leq 1$, is the

⁹ Other MSSPs that use a similar contract include Verizon, Counterpane Internet Security, and MegaPath.

probability that the MSSP will be liable for the breach. We restrict m to be strictly positive because the MSSP will not spend prevention effort otherwise. We assume that m is not necessarily equal to one because the contracts often include various disclaimers that are subject to multiple interpretations (Allen et al. 2003, Rittinghouse et al. 2003). That is, the specificity of the contract terms may play a key role in the outcome of the investigation. Furthermore, attackers frequently delete system logs to avoid being later detected, thereby eliminating a valuable source of breach information for the after-attack investigation (Panko 2009). We normalize the cost of this investigation to zero because it does not affect our results.

The sequence of events is provided below.

- (1) The firm and the MSSP agree on $[F, p]$.
- (2) The MSSP chooses e_p and e_d .
- (3) If a breach occurs and
 - (3.1) if neither the firm nor the MSSP detects it, nothing else happens,
 - (3.2) if the firm detects it, then an investigation occurs and the MSSP pays the firm p if the MSSP is held responsible,
 - (3.3) if the firm does not detect it and the MSSP does, the MSSP decides whether to reveal it to the firm¹⁰. If the breach is revealed, then an investigation occurs and the MSSP pays the firm p if the MSSP is held responsible.

The expected payoff for the firm and the MSSP are

$$\pi_F = \begin{cases} -F - \theta(e_p) \left(L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - \kappa pm - \phi(e_d)(1 - \kappa) pm \right) & \text{if the MSSP reveals the breach} \\ -F - \theta(e_p) \left(L(1 - (1 - \alpha)\kappa) - \kappa pm \right) & \text{if the MSSP does not reveal the breach} \end{cases} \quad (4)$$

¹⁰ We assume that the MSSP chooses to reveal all breaches or none of the breaches. In principle, the MSSP could perform an investigation of its own and choose to reveal only those breaches for which the MSSP is not likely to be found responsible by a subsequent investigation. Such an action by the MSSP has the effect of decreasing m in our model.

$$\pi_M = \begin{cases} F - \theta(e_p)(mp\kappa + (1-\kappa)\phi(e_d)pm) - C_p(e_p) - C_d(e_d) & \text{if the MSSP reveals the breach} \\ F - \theta(e_p)mp\kappa - C_p(e_p) & \text{if the MSSP does not reveal the breach} \end{cases} \quad (5)$$

We use backward induction to solve the firm's contracting problem¹¹. The following result obtains in stage 3.3 and stage 2 of the game.

LEMMA 1. (1) *The MSSP does not reveal security breaches it detects to the firm.*
(2) *The MSSP does not spend any detection effort.*

If only the MSSP detects the breach, it expects to gain nothing by revealing the breach to the firm that is unaware of the breach. On the contrary, by revealing, the MSSP triggers an investigation which finds the MSSP responsible for the breach with probability m and results in an expected loss of mp to the MSSP. Therefore, the MSSP prefers to hide the breaches from the firm. If the MSSP will not reveal the security breaches, then it has no incentive to spend any detection effort because detection effort is costly. Lemma 1 reveals an inherent conflict of interest faced by a MSSP to which both prevention and detection services are outsourced and a penalty-based contract is adopted. Detecting a breach may imply a failure to avoid the breach, but preventing a breach diminishes the value of detection effort. The penalty-based contract penalizes the failure to prevent a breach, and therefore, the MSSP does not see any value in exerting detection effort. Conflicts of interest faced by MSSPs offering comprehensive security services such as security device management and monitoring, consulting and security product development have been recognized by security experts. For example, Schneier (2002) notes "Some outsourcers offer security management and monitoring. This worries me. If the outsourcer finds a security problem with my network, will the company tell me or try to fix it quietly?" Lemma 1 confirms this major concern and offers a theoretical support to this argument.

¹¹ The equilibrium concept we use is Sub-game Perfect Nash Equilibrium (Fudenberg and Tirole 1998, page 69).

In stage 2 of the game, while the MSSP does not exert any detection effort, it determines the optimum prevention effort by maximizing π_M recognizing that a breach will be detected by the firm with probability κ . In stage 1, knowing that the MSSP will only put prevention effort, the firm's problem is provided in Program 1-MSSP-P.

Program 1-MSSP-P

$$\begin{aligned} \text{Max}_{F, p} \quad & -F - \theta(e_p) \left(L(1 - (1 - \alpha)\kappa) - \kappa pm \right) \\ \text{s.t.} \quad & -\theta'(e_p) mp\kappa - C'_p(e_p) = 0 && (IC_{e_p}) \\ & F - \theta(e_p) mp\kappa - C_p(e_p) \geq u && (IR) \end{aligned}$$

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 $p^{1-MSSP-P}$, $F^{1-MSSP-P}$, and $e_p^{1-MSSP-P}$ indicate the optimum contract terms and the equilibrium prevention effort.

PROPOSITION 2. *When the contract includes a fixed fee and a penalty for breaches, the solution to Program 1-MSSP-P has the following properties.*

- (1) *The first-best solution is not achieved.*
- (2) *The optimum prevention (detection) effort is greater (smaller) than the first-best optimum prevention (detection) effort.*
- (3) $p^{1-MSSP-P} = \frac{L(1 - (1 - \alpha)\kappa)}{m\kappa}$ and $F^{1-MSSP-P} = u + \theta(e_p^{1-MSSP-P})L(1 - (1 - \alpha)\kappa) + C_p(e_p^{1-MSSP-P})$.
- (4) *The optimum penalty could be greater than the damage L the firm incurs from a breach. Technically, $p^{1-MSSP-P} > L$ if and only if $\kappa(1 + m - \alpha) < 1$.*

Proposition 2 shows that the first-best solution cannot be obtained in a penalty-based contract. The intuition for Proposition 2 follows from Lemma 1 and Proposition 1. That is, a penalty-based contract does not provide any incentive for the MSSP to spend detection effort. Because prevention and detection efforts are used as substitutes (Proposition 1), and the MSSP puts a zero (that is, less than the first-best) effort in detection, the firm prefers to induce a prevention effort beyond the first-best prevention effort. In the equilibrium, the firm will set F such that the IR constraint is binding; that is, the expected payoff to

the MSSP equals its reservation wage u . Thus, the firm's payoff becomes $-u - C_p(e_p) - \theta(e_p)L(1 - (1 - \alpha)\kappa)$, which the firm maximizes while setting p . Comparing the first-order condition for e_p that maximizes the firm's payoff with the first-order condition for the MSSP's payoff (i.e., IC_{e_p} constraint), we find that the firm sets p such that the expected marginal benefit of the prevention effort for the MSSP, $-\theta'(e_p)mp\kappa$, is equal to that of its own, $-\theta'(e_p)L(1 - (1 - \alpha)\kappa)$, which gives the optimum p shown in Proposition 2(3). While the firm recovers a fraction of the loss from a breach when it detects the breach on its own, it does not always receive the refund from the MSSP for a detected breach, and, furthermore, the firm detects only a fraction of all breaches given that the MSSP does not provide the firm with any help in detection. Therefore, the firm compensates for the unrecovered loss by setting a penalty that may be larger than the damage the firm incurs from a breach. An increase in either the probability of finding the MSSP responsible for the breach or the probability of the firm detecting a breach on its own reduces the likelihood of penalizing the MSSP more than the loss from a breach.

While Lemma 1 reveals the conflict of interest faced by the MSSP in a penalty-based contract, which results in the hiding of breaches and lack of detection effort under such a contract, Proposition 2 highlights another potential problem regarding the feasibility of a penalty-based contract. The conflict of interest forces the firm to design a contract with a large penalty, possibly deemed unfair by a court of law. If the firm is unable to enforce the contract as shown in Proposition 2 because the contract is regarded as unfair, then the firm will have to settle for a contract with a less-than-optimum penalty. In this case, the firm will suffer from a lower prevention effort than the one shown in Proposition 2, in addition to the zero detection effort.

In this subsection, we showed that the common practice of outsourcing device management and security monitoring to the same MSSP using a penalty-based contract suffers from the misalignment of incentives and possibly feasibility related problems. The insights gained from this analysis led us to

propose two other contracts which mitigate the problems associated with the penalty-based contract. We discuss these contracts in the next two subsections.

3.2. Penalty-and-Reward-Based Contract

The penalty-and-reward-based contract has a reward component in addition to penalty and fixed fee: $[F, p, r]$. The firm offers the MSSP a reward of r if the MSSP reveals a breach the firm could not detect on its own. Parameters F and p have the same meanings as in the penalty-based contract. Therefore, in the penalty-and-reward-based contract, an upfront fixed fee F is paid by the firm to the MSSP, a reward r is offered to the MSSP if the firm becomes aware of the breach because the MSSP reveals the breach to the firm, and a penalty p is imposed on the MSSP subsequently if the MSSP is deemed responsible for the breach. The timeline remains identical to that under penalty-based contract except in step (3.3), the firm pays the MSSP r if the MSSP reveals the breach to the firm. Note that the MSSP is still penalized p if the subsequent investigation holds the MSSP liable for the breach.

The expected payoffs for the firm and the MSSP are

$$\pi_F = \begin{cases} -F - \theta(e_p) \left(L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - \kappa pm - \phi(e_d)(1 - \kappa)(pm - r) \right) & \text{if the MSSP reveals the breach} \\ -F - \theta(e_p) \left(L(1 - (1 - \alpha)\kappa) - \kappa pm \right) & \text{if the MSSP does not reveal the breach} \end{cases} \quad (6)$$

$$\pi_M = \begin{cases} F - \theta(e_p)(mp\kappa + (1 - \kappa)\phi(e_d)(pm - r)) - C_p(e_p) - C_d(e_d) & \text{if the MSSP reveals the breach} \\ F - \theta(e_p)mp\kappa - C_p(e_p) & \text{if the MSSP does not reveal the breach} \end{cases} \quad (7)$$

In stage (3.3) of the game, the MSSP will reveal the breach to the firm if and only if the expected benefit from revelation $(r - mp)$ is non-negative. Therefore, whether the MSSP will reveal or hide the breach is determined endogenously by the r and p values set in the contract. We refer to the equilibrium that induces the MSSP to reveal the breach as the *revelation equilibrium* and the one that induces the MSSP to hide the breach as the *no-revelation equilibrium*. Unlike the penalty-based contract in which the MSSP will never reveal a breach to the firm, in a penalty-and-reward-based contract the firm can induce the

MSSP to reveal breaches if it sets r sufficiently high relative to p . However, it is unclear whether it is always in the best interest of the firm to do so. Therefore, we solve for the optimum contracts corresponding to the revelation and no-revelation regimes and identify the regime that will offer a higher expected payoff to the firm.

3.2.1. Revelation Regime

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

Program 1-MSSP-P-R-R

$$\begin{aligned}
& \text{Max}_{F,p,r} -F - \theta(e_p) \left(L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - \kappa pm - \phi(e_d)(1 - \kappa)(pm - r) \right) \\
& \text{s.t.} \quad -\theta'(e_p)(mp\kappa + (1 - \kappa)\phi(e_d)(pm - r)) - C'_p(e_p) = 0 \quad (IC_{e_p}) \\
& \quad -\theta(e_p)(1 - \kappa)\phi'(e_d)(pm - r) - C'_d(e_d) = 0 \quad (IC_{e_d}) \\
& \quad F - \theta(e_p^{1-MSSP})(mp\kappa + (1 - \kappa)\phi(e_d^{1-MSSP})(pm - r)) - C_p(e_p^{1-MSSP}) - C_d(e_d^{1-MSSP}) \geq u \quad (IR) \\
& \quad r \geq mp \quad \text{(Revelation)}
\end{aligned}$$

Similar to Program 1-MSSP-P, IC_{e_p} , IC_{e_d} , and IR in Program 1-MSSP-P-R-R denote the MSSP's incentive compatibility constraints with respect to prevention and detection efforts and the individual rationality constraint, respectively. The last constraint specifies the condition that has to be satisfied in a revelation equilibrium. The following proposition presents the solution to Program 1-MSSP-P-R-R with $p^{1-MSSP-P-R-R}$, $r^{1-MSSP-P-R-R}$, $F^{1-MSSP-P-R-R}$, $e_p^{1-MSSP-P-R-R}$, and $e_d^{1-MSSP-P-R-R}$ characterizing the optimum contract terms and the equilibrium efforts.

PROPOSITION 3. *When the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches, and the firm induces a revelation equilibrium, the solution to Program 1-MSSP-P-R-R has the following properties.*

(1) *The first-best solution is achieved, i.e., $e_p^{1-MSSP-P-R-R} = e_p^*$ and $e_d^{1-MSSP-P-R-R} = e_d^*$*

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

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

$$F^{1-MSSP-P-R-R} = \theta(e_p^*)L \left(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d^*)) \right) + C_p(e_p^*) + C_d(e_d^*) + u$$

(3) *The optimum penalty could be greater than the damage the firm incurs from an undetected breach. Technically, $p^{1-MSSP-P-R-R} > L$ if and only if $\kappa(1 + m - \alpha) < 1$.*

(4) *The optimum reward is greater than the damage L the firm incurs from an undetected breach, but is equal to the expected benefit the firm obtains from the detection of the breach. Technically, $r^{1-MSSP-P-R-R} = (1-\alpha)L + mp^{1-MSSP-P-R-R} > L$.*

Proposition 3 shows that the firm induces the first-best prevention and detection efforts if it adopts the penalty-and-reward contract and induces a revelation equilibrium. To see the intuition for this result, note that the firm will pay the MSSP an expected payoff equal to its reservation utility, which is a constant, as in the penalty-based contract. In a revelation equilibrium, since the MSSP puts in detection effort and reveals all breaches it detects, the firm's payoff is equal to the joint payoff in the first-best benchmark case minus the constant reservation utility. Therefore, the firm effectively maximizes the joint payoff as it does in the first-best problem and hence induces the first-best efforts. Unlike the penalty-based contract in which the firm has to work only with penalty, in the penalty-and-reward-based contract the firm is able to induce the two first-best efforts because it can manipulate two variables (viz., penalty and reward). In order to induce the first-best efforts, the firm sets p and r such that the marginal value of (or benefit from) prevention effort for the MSSP is equal to the marginal value of prevention in the first-best problem, and analogously for the detection effort.

Consider the detection effort. The marginal value of detection effort in the first-best problem is $\theta(e_p)\phi'(e_d)L(1-\kappa)(1-\alpha)$, and the marginal value of detection for the MSSP is $\theta(e_p)(1-\kappa)\phi'(e_d)(r-pm)$. Therefore, in order to induce the first-best detection effort, the firm is forced to offer the entire benefit it receives from knowing about the breach (which consists of the reduction in loss when the breach is detected by the firm $(1-\alpha)L$ and the expected penalty it will receive from the MSSP for the breach $mp^{1-MSSP-P-R-R}$) as reward to the MSSP for revealing a breach, which leads to the optimum reward shown in Proposition 3(4). The indirect effect of setting this optimum reward is that the firm's equilibrium payoff expression becomes independent of reward and detection effort and equal to that in the penalty-based contract. Therefore, the optimum penalty amount under the penalty-and-reward-based contract (shown in Proposition 3(2)) is equal to that under the penalty-based

contract (Proposition 2(2)). In spite of the same amount of penalty, the MSSP puts in the first-best prevention effort under the penalty-and-reward-based contract because the firm forces the MSSP to internalize the substitution effect between prevention and detection efforts, induced by the reward. As a result, the MSSP puts just enough prevention effort, not as much prevention effort as in the penalty-based contract.

3.2.2. No-Revelation Regime

In the no-revelation equilibrium, since the MSSP does not reveal any breach to the firm, the MSSP's expected payoff from detecting a breach is zero. Therefore, part 2 of Lemma 1 holds in this equilibrium. That is, the MSSP will not spend any detection effort. In this case, the reward amount does not play a role, and the firm's problem is same as Program 1-MSSP-P. Therefore, we have the following result.

PROPOSITION 4. When the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches, and the firm induces a no-revelation equilibrium, the properties of the optimum contract and the resulting equilibrium efforts are characterized in Proposition 2.

Now, we show the following result for the penalty-and-reward-based contract.

PROPOSITION 5. When the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches, the firm induces the first-best efforts from the MSSP and a revelation equilibrium.

The firm prefers the revelation-equilibrium to the no-revelation equilibrium under the penalty-and-reward-based contract because the joint payoff is maximized only when a positive detection effort is spent and the firm keeps the remaining surplus after providing the reservation utility u to the MSSP from the joint payoff, the firm is better off when the MSSP puts a positive effort into detection than when it does not. The reward component in the penalty-and-reward-based contract enables the firm to eliminate the conflict of interest problem that arises in the penalty-based contract, incentivize the MSSP to spend detection effort, and simultaneously force the MSSP to internalize the substitution between prevention and detection efforts. A significant observation is that the penalty-and-reward-based contract offers this benefit by imposing the same penalty as in the penalty-based contract. Thus, on the feasibility dimension, the penalty-and-reward contract and the penalty-based contract are identical. That is, the optimum

penalty-and-reward-based contract suffers from the infeasibility problem whenever the penalty-based contract does, and vice versa.

An interesting observation common to both Proposition 2 and Proposition 3 is that the optimum penalty and the optimum reward in the two contracts are independent of the MSSP parameters. This result arises because the optimum penalty and reward depend only on the marginal joint benefits of prevention and detection efforts, which are independent of costs of prevention effort and detection effort. Consequently, the firm does not have to alter the penalty and reward when the cost of one or both of these efforts changes. This result has practical implications to contract design. The finding implies that it is not necessary for the firm to know MSSP's private cost parameters in order to set the penalty and reward components in the contract. On the other hand, the fixed fee, which determines the division of the joint payoff between the firm and the MSSP and depends on the cost parameters, can be negotiated and is likely to depend on the relative bargaining strengths of the players. If the firm is the Stackelberg leader and if it knows the cost parameters of the MSSP, as we model in the current paper, the firm will have bargaining power over the MSSP, and will extract the remaining surplus after providing the reservation utility the MSSP requires to participate in the contract.

3.3. Two-MSSP Contract

Sections 3.1 and 3.2 considered contracts when the firm outsources both prevention and detection functions to a single MSSP. In this section, we analyze the case in which the firm outsources the prevention function to one MSSP and the detection function to a different MSSP. We label the MSSP that offers the prevention services M_p and the one that offers the detection services M_D . The firm offers a penalty-based contract $[F_p, p]$ to M_p and a reward-based contract $[F_D, r]$ to M_D . 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 previous two contracts we considered. Further, we assume that the sum of the reservation payoffs of the two MSSPs in the two-MSSP case is equal to the reservation payoff of the MSSP in the single MSSP case. Lastly, we assume that there is no collusion between the two MSSPs.

The sequence of events under the two-MSSP contract is as follows.

- (1) The firm and M_P agree on $[F_P, p]$; the firm and M_D agree on $[F_D, r]$.
- (2) M_P chooses e_p ; M_D chooses e_d .
- (3) If a breach occurs and
 - (3.1) if neither the firm nor M_D detects it, nothing else happens,
 - (3.2) if the firm detects it, then an investigation occurs and M_P pays the firm p if M_P is held responsible,
 - (3.3) if the firm does not detect it and M_D does, then M_D reveals the breach to the firm and receives r from the firm. An investigation occurs and M_P pays the firm p if M_P is held responsible.

Please note that in step (3.3), unlike the single MSSP case, M_D does not have any incentive to hide a breach it detects; on the contrary, it has an incentive in the form of a reward to reveal the breach to the firm.

The expected payoffs for the firm and the MSSPs are

$$\pi_F = -F_P - F_D - \theta(e_p) \left(L \left(1 - (1 - \alpha) (\kappa + (1 - \kappa) \phi(e_d)) \right) - \kappa pm - \phi(e_d) (1 - \kappa) (pm - r) \right) \quad (8)$$

$$\pi_{M_P} = F_P - \theta(e_p) mp (\kappa + (1 - \kappa) \phi(e_d)) - C_p(e_p) \quad (9)$$

$$\pi_{M_D} = F_D + \theta(e_p) (1 - \kappa) \phi(e_d) r - C_d(e_d). \quad (10)$$

The firm's problem is provided in Program 2-MSSP.

Program 2-MSSP

$$\begin{aligned} \text{Max}_{F, p, r} \quad & -F_P - F_D - \theta(e_p) \left(L \left(1 - (1 - \alpha) (\kappa + (1 - \kappa) \phi(e_d)) \right) - \kappa pm - \phi(e_d) (1 - \kappa) (pm - r) \right) \\ \text{s.t.} \quad & -\theta'(e_p) mp (\kappa + (1 - \kappa) \phi(e_d)) - C'_p(e_p) = 0 & (IC_{e_p}) \\ & \theta(e_p) (1 - \kappa) \phi'(e_d) r - C'_d(e_d) = 0 & (IC_{e_d}) \\ & F_P - \theta(e_p) mp (\kappa + (1 - \kappa) \phi(e_d)) - C_p(e_p) \geq u_p & (IR_p) \\ & F_D + \theta(e_p) (1 - \kappa) \phi(e_d) r - C_d(e_d) \geq u_D & (IR_D) \end{aligned}$$

Because there are two MSSPs, there are two *IR* and *IC* constraints in Program 2-MSSP. The reservation payoffs of M_P and M_D are, respectively, u_P and u_D , and $u = u_P + u_D$. The following proposition characterizes the solution to Program 2-MSSP and p^{2-MSSP} , F_P^{2-MSSP} , r^{2-MSSP} , F_D^{2-MSSP} , e_p^{2-MSSP} , e_d^{2-MSSP} denote the optimum contract terms and the equilibrium efforts.

PROPOSITION 6. *When the firm uses a MSSP for prevention and another MSSP for detection, the solution to Program 2-MSSP has the following properties.*

- (1) *The first-best solution is achieved, i.e., $e_p^{2-MSSP} = e_p^*$ and $e_d^{2-MSSP} = e_d^*$.*
- (2) *The optimal contract is given by the following*

$$p^{2-MSSP} = L \frac{1-(1-\alpha)(\kappa + (1-\kappa)\phi(e_d^*))}{m(\kappa + (1-\kappa)\phi(e_d^*))}, \quad r^{2-MSSP} = L(1-\alpha),$$

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

$$F_D^{2-MSSP} = -\theta(e_p^*)(1-\kappa)\phi(e_d^*)L(1-\alpha) + C_d(e_d^*) + u_D$$

- (3) *The optimum penalty could be greater than the damage L that the firm incurs from an undetected breach; Technically, $p^{2-MSSP} > L$ if and only if $(\kappa + (1-\kappa)\phi(e_d^*))(1+m-\alpha) < 1$.*
- (4) *The optimum reward is less than the damage L the firm incurs from an undetected breach as well as the expected benefit the firm obtains from the detection of the breach. Technically, $r^{2-MSSP} < (1-\alpha)L + mp^{2-MSSP} < L$.*

As in the penalty-and-reward contract for a single MSSP, the firm is able to induce the first-best efforts in the two-MSSP contract. The intuition for this result is the same in both contracts – because the firm has two variables it can control to induce two first-best efforts, the firm can force the two MSSPs to internalize the substitution effect between prevention and detection efforts by appropriately choosing the penalty and reward parameters. However, as shown in the following result, the optimum penalty and the optimum reward are substantially different under the two contracts.

COROLLARY 1: *All contract terms, i.e., the reward, the penalty, and the sum of fixed payments to the two MSSPs, under the two-MSSP contract are smaller than the corresponding terms under the penalty-and-reward-based contract. Technically, $p^{2-MSSP} < p^{1-MSSP-P-R-R}$, $r^{2-MSSP} < r^{1-MSSP-P-R-R}$, and $F_D^{2-MSSP} + F_P^{2-MSSP} < F^{1-MSSP-P-R-R}$.*

Even though the firm sets the marginal benefit of prevention effort for the MSSP providing prevention services to the marginal benefit of prevention effort in the first-best problem, and analogously for the detection effort under both the two-MSSP and the penalty-and-reward-based contracts, the contract terms are smaller in the former than in the latter. The differences in the optimum contract terms for the two contracts are attributed to the differences in the roles played by penalty and reward in the two contracts. In the single MSSP penalty-and-reward-based contract, both penalty and reward play a dual role with regards to the prevention and detection functions. For instance, consider the penalty p . It is straightforward to see that the penalty amount affects the prevention effort exerted by the MSSP; *ceteris paribus*, an increase in the penalty will increase the prevention effort. Furthermore, the penalty amount affects the detection effort because the positive likelihood of the investigation finding the MSSP responsible for the breach reduces the net benefit (which is equal to $r - mp$) the MSSP realizes from detecting and revealing a breach to the firm; *ceteris paribus*, an increase in the penalty will reduce the detection effort. That is, the penalty amount serves not only the role of inducing prevention effort but also the role of discouraging detection effort. Similarly, the reward amount r serves not only the role of inducing detection effort but also, by reducing the effective penalty 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 play dual roles of affecting the marginal benefits of both prevention and detection efforts of the MSSP. In a two-MSSP contract, the penalty and reward play their intended roles. The penalty amount does not reduce the reward received by the MSSP providing detection services for detecting and revealing breaches, and the reward amount does not reduce the effective penalty paid by the MSSP providing prevention services when it is held responsible for breaches. Therefore, while the firm has to account for the conflicting roles played by penalty and reward in the penalty-and-reward-based contract, the firm is able to independently set the penalty and reward parameters based solely on their intended purpose – penalty to induce prevention effort and reward to induce detection effort – in the two-MSSP contract. Thus, the firm is forced to set both a higher penalty and a higher reward in the penalty-and-reward-based contract than in the two-MSSP contract. In essence, by separating the prevention and detection functions and outsourcing

them to two different MSSPs, the firm increases the marginal benefits of prevention and detection efforts for a given set of penalty and reward values.

We should observe that while the two-MSSP contract has smaller penalty, reward and fixed payment than the penalty-and-reward-based contract with a single MSSP, both achieve the first-best outcomes and the firm's expected payoff is identical under both contracts. On the other hand, we note that unlike in the penalty-and-reward-based contract, the optimum penalty in the two-MSSP contract depends on the MSSPs' cost parameters. Therefore, the firm needs to know the cost structure of the MSSPs to set the terms in the optimal contracts.

3.4 Fairness and Feasibility of Contracts

Our analysis of the penalty-based, penalty-and-reward-based, and two-MSSP contracts showed that the optimum penalty could be greater than the maximum loss L the firm incurs from a breach. However, institutions such as the courts might limit the level of penalty based on a notion of fairness. In outsourcing contracts, if the firm requires a compensation that is more than the loss it incurs from a breach, the contract could be deemed unfair by the courts. Analogously, though not based on the notion on fairness, the firm may be reluctant to offer more than the loss it incurs from a breach as a reward for detecting breaches. We operationalize the fairness criterion by comparing the penalty and maximum loss from a security breach. Specifically, the fairness criterion is satisfied by a contract if $p^* - L \leq 0$ where $p^* = p^{1-MSSP-P}$ in the penalty-based contract, $p^* = p^{1-MSSP-P-R-R}$ in the penalty-and-reward-based contract, and $p^* = p^{2-MSSP}$ in the two-MSSP contract. The effects of the fairness criterion on the three contracts are highlighted in Proposition 2(4), Proposition 3(3), and Proposition 6(3). Essentially, a penalty-based contract and a penalty-and-reward-based contract satisfy the fairness criterion if and only if $\kappa(1+m-\alpha) \geq 1$ and the two-MSSP contract satisfies the fairness criterion if and only if $(\kappa + (1-\kappa)\phi(e_d^*))(1+m-\alpha) \geq 1$.

It is clear that none of the three contracts satisfies the fairness criterion if $m \leq \alpha \Rightarrow 1 - m \geq 1 - \alpha$. That is, when the expected benefit from detection is small, either because the probability of finding the MSSP responsible for a breach (i.e., m) is small or the fraction of loss recovered when a breach is detected by the firm (i.e., $1 - \alpha$) is small, the contract is less likely to satisfy the fairness criterion. If $m > \alpha$, then the fairness criterion is satisfied by all contracts when the likelihood of the firm detecting a breach on its own (i.e., κ) is above a threshold value; this threshold value is smaller for the two-MSSP contract than for the other two contracts. Further, we find that whenever the penalty-based and penalty-and-reward-based contracts satisfy the fairness criterion, the two-MSSP contract also satisfies the fairness criterion, but the reverse may not be true. These results imply that the two-MSSP contract is feasible based on the fairness criterion in a larger region of the parameter space compared to the two contracts that involve one MSSP. While the cost and efficiency of prevention and detection efforts affect (through their impact on the first-best detection effort) the feasibility of the two-MSSP contract, they do not affect the feasibility of the two contracts that involve one MSSP.

The major findings from the analysis of the penalty-based, penalty-and-reward-based, and two-MSSP contracts are summarized below.

(1) The first-best prevention and detection efforts are achieved if the contracts include a penalty for missing breaches and a reward for detecting breaches, irrespective of whether the firm outsources security to a single MSSP or two MSSPs. However, the first-best outcome is not achieved if the firm uses a single MSSP and a contract that specifies only a penalty for breaches.

(2) The optimum penalty and the optimum reward are smaller when the firm uses two MSSPs than when it uses a single MSSP.

(3) All contracts may fail to satisfy the fairness criterion when κ is small, m is small, and α is high. However, the two-MSSP contract satisfies the fairness criterion whenever a single MSSP contract satisfies the fairness criterion and also sometimes when a single MSSP contract does not.

(4) If the firm offers a reward in a contract, then the optimum reward is greater than the maximum loss from a breach when it uses a single MSSP but less than the maximum loss when it uses two MSSPs.

Thus, in general, the two-MSSP contract appears to be superior for inducing the MSSPs to choose the first-best prevention and detection efforts. However, one significant drawback of two-MSSP contract, relative to the other two, is that it requires the firm to know the MSSP's prevention and detection cost and efficiency parameters, which are generally private information.

4. Effects of Limit on Penalty, Limit on Reward, and Costs of Prevention and Detection

We operationalized the fairness criterion using the difference between penalty and loss and used it to analyze the feasibility of contracts in Section 3.4. In general, feasibility constraints impose limits on penalty and/or reward. We now provide insights into how limits on the penalty and reward affect the contract characteristics as well as prevention and detection efforts in general. Further, we analyze how prevention cost and detection cost affect our results. We obtain some of the insights in this section using a numerical example. For the numerical example, we set

$$\theta(e_p) = \nu e^{-\xi_p e_p}, \phi(e_d) = 1 - e^{-\xi_d e_d}, C_p(e_p) = c_p e_p, \text{ and } C_d(e_d) = c_d e_d.$$

For the above the specifications, we obtain the first-best solution as the following.

$$e_p^* = \frac{\text{Log} \left(\frac{Lv\alpha\xi_d\xi_p}{c_p\xi_d - c_d\xi_p} \right)}{\xi_p}, e_d^* = \frac{\text{Log} \left(\frac{(1-\alpha)(1-\kappa)(c_p\xi_d - c_d\xi_p)}{\alpha c_d\xi_p} \right)}{\xi_d}$$

Further, we set the following values for model parameters.

$$c_p = 5, c_d = 1, \nu = 0.7, \xi_p = 0.9, \xi_d = 0.8, \kappa = 0.3, \alpha = 0.4, m = 0.4, L = 3000, u_p = u_d = u = 0.$$

4.1 Limit on Penalty

We assume that there is an exogenously specified limit on penalty that can be enforced by the firm. We label this P . Note that P could be a function of L and other exogenous parameters. We assume

$$P < L \frac{1-(1-\alpha)\kappa}{m\kappa} \text{ because a higher value of } P \text{ will have no impact on the results we derived in Section 3.}$$

Other aspects of the model remain the same.

The firm's problems under the penalty-based, penalty-and-reward-based, and two-MSSP contracts are similar to Program 1-MSSP-P, Program 1-MSSP-P-R-R, and Program 2-MSSP, respectively, with the exception of the additional constraint $p \leq P$.

PROPOSITION 7. *If $P < L \frac{1-(1-\alpha)\kappa}{m\kappa}$,*

(1) *When the firm uses a single MSSP and the contract includes a fixed fee and a penalty for breaches, the first-best solution is not achieved and the MSSP does not spend any detection effort.*

(2) *When the firm uses a single MSSP and the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches, the first-best solution is not achieved but a revelation equilibrium is induced.*

(3) *When the firm uses a MSSP for prevention services and a different MSSP for detection services, the*

first-best solution is achieved if and only if $L \frac{1-(1-\alpha)(\kappa + (1-\kappa)\phi(e_d^))}{m(\kappa + (1-\kappa)\phi(e_d^*))} \leq P < L \frac{1-(1-\alpha)\kappa}{m\kappa}$.*

The penalty constraint is binding at the optimum under the penalty-based and penalty-and-reward-based

contracts. The constraint is binding only when $P < L \frac{1-(1-\alpha)(\kappa + (1-\kappa)\phi(e_d^*))}{m(\kappa + (1-\kappa)\phi(e_d^*))}$ if the firm uses two

MSSPs. Regardless of the contract type, the firm cannot induce the first-best efforts and realizes a smaller payoff than the first-best payoff when the penalty limit is binding. In the penalty-based contract, the inability of the firm to induce the MSSP to spend detection effort and reveal breaches as well as the limit on the prevention effort that can be induced (because of the limit on penalty) contribute to the smaller payoff to the firm. However, in the other two contracts, the firm's smaller payoff is not because of its inability to force the MSSP to spend detection effort and reveal the breaches. In fact, we found that a binding limit on penalty causes the firm to offer a smaller reward for revealing breaches than that the firm would offer if there were no limit on penalty. The intuition for this is as follows. A decrease in penalty decreases the MSSP's incentive to spend prevention effort, which increases the probability of breach and the marginal benefit from detection, which, in turn, decreases the firm's incentive to reward the MSSP to exert detection effort.

For the numerical analysis, we vary P from 1000 to 20500¹². The optimum values for the numerical example are provided in Table 1. When the penalty limit increases, the prevention effort increases under all three contracts, as expected. On the other hand, as the penalty limit increases, while the detection effort increases when the firm uses the penalty-and-reward-based contract, it decreases when the firm uses the two-MSSP contract.¹³ Because prevention effort and detection effort are substitutes, the firm prefers to reduce the detection effort when the penalty limit increases. When the firm uses the two-MSSP contract, since the prevention and detection efforts are spent by different MSSPs and the firm does not face any constraint in choosing the reward, the firm reduces the detection effort by reducing the reward when the penalty limit increases. On the other hand, in the 1-MSSP-P-R-R scenario, an increase in the penalty limit forces the firm to increase the reward amount also because it has to satisfy the revelation constraint ($r > mp$) to induce a revelation equilibrium. Recall from Proposition 7(2) that a limit on penalty does not alter the firm's preference for the revelation equilibrium. Furthermore, as discussed previously about the dual and conflicting role played by r , an increase in reward also reduces the marginal benefit from penalty. Therefore, an increase in the penalty limit does not allow the firm to extract as much prevention effort in the 1-MSSP-P-R-R contract as in the two-MSSP contract, thereby forcing the firm to depend on more detection effort to maximize its payoff even when the penalty limit increases.

Although a tighter penalty limit results in a lower payoff for the firm under all three contracts, the reduction gap in the payoff from the first-best payoff is higher for the 1-MSSP-P and 1-MSSP-P-R-R contracts than for the two-MSSP contract. This implies that a tighter penalty limit makes two-MSSP contract more desirable compared to single MSSP contracts.

Table 1. Impact of Limits on Penalty

<i>Penalty Limit</i>	<i>Contract Type</i>	e_p	e_d	π_F	p^*	r^*
	1-MSSP-P	6.37383	0	-37.4247	20500	-

¹² When the penalty limit exceeds 20500, it is not binding in any of the three contracts.

¹³ Penalty limits do not impact detection effort in a penalty-based contract because the detection effort is always zero under this contract.

20500	1-MSSP-P-R-R	5.859	1.607	-36.460	20500	10000
	two-MSSP	5.859	1.607	-36.460	4800	1800
3000	1-MSSP-P	4.23848	0	-59.1554	3000	-
	1-MSSP-P-R-R	4.013	0.866	-55.526	3000	1388.86
	two-MSSP	5.446	2.307	-36.819	3000	2172.79
1000	1-MSSP-P	3.0178	0	-128.978	1000	-
	1-MSSP-P-R-R	2.806	0.823	-118.585	1000	461.598
	two-MSSP	4.319	3.846	-43.498	1000	2700

4.2 Limit on Reward

We assume that there is an exogenously specified limit on reward that the firm can offer to a MSSP for revealing breaches. We label this R . As in the case of limit on penalty, R could be a function of L and other exogenous parameters. We assume $R < \frac{L}{\kappa}$ because a higher value of R will have no impact on results we derived in Section 3. Other aspects of the model remain the same.

Since the penalty-based contract does not offer a reward for revealing breaches, we consider only the other two contracts in this sub section. The firm's problems under the penalty-and-reward-based and two-MSSP contracts are similar to Program 1-MSSP-P-R-R, and Program 2-MSSP, respectively, with the exception of the additional constraint $r \leq R$.

PROPOSITION 8. If $R < \frac{L}{\kappa}$,

- (1) When the firm uses a single MSSP and the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches, the first-best solution is not achieved and a revelation equilibrium is induced if and only if $R \geq mp^{1-MSSP-P-R-LIMIT}$, where $p^{1-MSSP-P-R-LIMIT}$ is the optimum penalty when $r = R$.
- (2) When the firm uses a MSSP for prevention services and a different MSSP for detection services, the first-best solution is not achieved if and only if $R < L(1 - \alpha)$.

The reward constraint is binding at the optimum when the firm uses a single MSSP and induces a revelation equilibrium. The constraint is binding only if $R < L(1 - \alpha)$ when the firm uses two MSSPs. As in the case of binding penalty limit, the firm cannot induce first-best efforts when the reward constraint is binding. The most interesting implication of Proposition 8 is that when faced with a binding limit on reward, the firm may prefer a no-revelation equilibrium in the penalty-and-reward-based contract. In

order to provide insights into the conditions under which the firm will prefer the no-revelation equilibrium, we use the numerical results provided in Table 2. We observe from this table that the firm induces a revelation equilibrium when $R \geq 7500$ and a no-revelation equilibrium when $R < 7500$. When the reward limit decreases, the firm has to reduce the penalty also in order to force the MSSP to reveal breaches. This has the consequence of the MSSP reducing the prevention effort, which increases the likelihood of breaches, and reducing the detection effort, which decreases the probability of detecting breaches. If R is not too low, the firm may still benefit from MSSP's detection effort and the benefit may offset the higher likelihood of breaches, and therefore the firm will reduce the penalty and induce revelation equilibrium in response to a decrease in reward limit (see 1-MSSP-P-R-R contract when $R=7500$). On the other hand, when R becomes sufficiently low, the benefit from the detection effort does not offset the increase in loss because of a low penalty. The firm then switches to a no-revelation equilibrium, and because it does not face the revelation constraint the firm increases the penalty in order to reduce the likelihood of a breach, but the firm detects a smaller number of breaches because there is no detection effort exerted by the MSSP (see 1-MSSP-P-R-R contract when $R=5000$). In this case, recall from Proposition 1 that the firm sets the penalty high enough to achieve prevention effort higher than the first best and no detection effort. Of course, if the firm uses two MSSPs, revelation is not an issue, but the first-best solution is still not achieved when the reward constraint is binding.

An interesting observation is that in the two-MSSP contract the firm induces the first-best prevention effort even when the reward limit becomes binding. In other words, even when the reward limit prohibits the firm from inducing the first-best detection effort, the firm still induces the first-best prevention effort as long as the detection effort is non-zero. The above result is explained by the following. In a two-MSSP contract, a decrease in the reward (because of the reward limit) decreases the incentive of the MSSP offering the detection services to exert detection effort, *ceteris paribus*. Any increase in the prevention effort reduces the incentive to exert detection effort further because the probability of breach decreases with an increase in the prevention effort. Therefore, the firm that prefers to induce more detection effort does not exacerbate the incentive problem by inducing a higher prevention

effort from the MSSP that offers the prevention services. Further, the firm does not prefer to reduce the prevention effort also because of the substitutable nature of these two efforts from the firm's perspective. Therefore, inducing any effort other than the first-best prevention effort from the MSSP offering the prevention services hurts the firm when the firm is forced to induce a less-than first-best detection effort from the MSSP offering the detection services.

Table 2. Impact of Limits on Reward

<i>Reward Limit</i>	<i>Contract Type</i>	e_p	e_d	π_F	p^*	r^*
10000	1-MSSP-P-R-R	5.859	1.607	-36.460	20500	10000
	two-MSSP	5.859	1.607	-36.460	4800	1800
7500	1-MSSP-P-R-R	5.721	1.245	-36.617	15774.3	7500
	two-MSSP	5.859	1.607	-36.460	4800	1800
5000	1-MSSP-P-R-R	6.374	0	-37.425	20500	0
	two-MSSP	5.859	1.607	-36.460	4800	1800
3000	1-MSSP-P-R-R	6.374	0	-37.425	20500	0
	two-MSSP	5.859	1.607	-36.460	4800	1800
1000	1-MSSP-P-R-R	6.374	0	-37.425	20500	0
	two-MSSP	5.859	0.872	-36.725	5940	1000

Our analysis of the impact of limits on penalty and reward shows that in a penalty-and-reward contract, a limit on penalty does not change the type of equilibrium (in this case, the revelation) but a limit on reward may. The firm finds allowing the MSSP to hide the breaches preferable to forcing the MSSP to reveal the breaches under low reward limits. Therefore, between a limit on penalty and a limit on reward, it seems that the reward constraint is more restrictive in the sense that a reward limit may lead to hiding of security breaches but a penalty limit does not. However, we should recognize that in practice the firm may have more flexibility in setting the reward limit compared to the penalty limit because the limit on reward is often self-imposed, but the penalty limit is often externally imposed by institutions such as courts. On the other hand, in a two-MSSP contract, a binding penalty limit prevents the firm from inducing either the first-best prevention effort or the first-best detection effort, but a binding reward limit does not prevent the firm from inducing the first-best prevention effort unless the reward limit is very

low. This suggests, at least from the perspective of inducing first-best efforts, that a penalty limit is more restrictive for a two-MSSP contract.

4.3 Effects of Prevention Cost and Detection Cost

The following result shows the impacts of prevention cost and detection cost under different contracts.

PROPOSITION 9. *If there is no limit either on penalty or reward,*
(1) an increase in either the prevention cost or the detection cost does not affect either the optimum penalty or the optimum reward when the firm uses a single MSSP,
(2) an increase in prevention (detection) cost decreases (increases) the optimum penalty and does not affect the optimum reward when the firm uses two MSSPs.

The optimum penalty and reward are independent of cost parameters when the firm uses a single MSSP (Proposition 2 and Proposition 3). The discussion at the end of Section 3.2 provides the reason why prevention and detection costs do not affect the contracts when a single MSSP is used. On the other hand, these parameters do affect the penalty and reward in the two-MSSP contract. The result that an increase in the prevention cost reduces the optimum penalty in a two-MSSP contract is apparently counter-intuitive because one would expect that an increase in the prevention cost reduces the MSSP's incentive to exert prevention effort, *ceteris paribus*, thereby forcing the firm to increase the penalty to compensate for the reduction in incentive. The reason for Proposition 9(2) is as follows. An increase in prevention cost has two effects: (i) it reduces the incentive of the MSSP offering the prevention services to exert effort, *ceteris paribus*, and (ii) it reduces (increases) the first-best prevention (detection) effort (Proposition 1). Therefore, the firm prefers to reduce, rather than increase, the prevention effort when prevention cost increases. Proposition 9(2) reveals that the increase in prevention cost does not reduce the MSSP's incentives to exert prevention effort sufficiently enough to achieve the necessary reduction in first-best prevention effort. This is because while the marginal benefit from the first-best prevention effort accounts for the savings from detection effort, the MSSP's prevention effort does not. Furthermore, the firm cannot change the reward offered in response to an increase in the prevention cost because the firm is already transferring the entire savings it obtains (in the form of loss recovered when a breach is detected) as reward (and this reward is independent of prevention and detection cost). Therefore, the firm reduces the

penalty in order to provide additional incentives to the MSSP to reduce the prevention effort in response to an increase in the prevention cost. On the other hand, an increase in the detection cost decreases the detection effort, *ceteris paribus*. Since an increase in the detection cost increases the first-best prevention effort and since reward cannot be changed, the firm increases the penalty to improve the incentive of the MSSP providing the prevention services and thereby to exert higher prevention effort.

An important implication of Proposition 9 is that when security breaches are more difficult to prevent or less difficult to detect, a two-MSSP contract is more likely to satisfy the fairness criterion. It follows that if we begin with a setting for which the fairness criterion is not met by any of the three contracts, and as the cost of prevention increases, relative to the cost of detection, the fairness criterion could likely be met by the two-MSSP contract but not by the other two contracts. This could provide one rationale, in addition to the conflict of interest associated with the single MSSP contracts, for the prediction about the likely outsourcing of prevention and detection to separate outsourcers by firms. However, the magnitude of this shift is likely to depend on factors such as cost of prevention relative to the cost of detection. If the scale and scope of future security breaches is such that cost of preventing them increases so much that the firms manage security risks by focusing more on detection, then the magnitude of the shift towards using two MSSPs is more likely to be significant. On the other hand, if the sophistication of future security attacks is such that detecting them proves costly and firms focus more on prevention, then the shift is less likely to be significant.

5. Model Extensions

We derived the results discussed in the previous sections by analyzing a fairly general model of a typical information security outsourcing context without assuming any specific cost or probability function for the two types of security services. In this section, we show that our results are robust to model variations and hold under a more general set of conditions than those presented in the previous sections.

5.1 Complementarity between Prevention and Detection Services

In our base model, we assumed that prevention and detection functions are independent of each other. However, it may be reasonable to expect some kind of complementarity between prevention and detection

services when these two functions are performed by the same outsourcer. For example, knowledge gained or learned by the outsourcer when it detects a breach could reduce the required effort to prevent similar breaches. Analogously, prevention effort could facilitate detection of security breaches. That is, prevention effort can improve the productivity of detection effort and vice versa, if both services are provided by the same outsourcer. Such a complementarity between the two functions could be modeled either on the benefit side or on the cost side. We chose the latter approach and use the following cost function to model the complementarity between prevention and detection efforts.

$$C(e_p, e_d) = C_p(e_p) + C_d(e_d) - \rho C_p(e_p)C_d(e_d)$$

where $\rho \geq 0$ can be considered as a proxy that captures the level of complementarity between prevention and detection efforts. We assume that $C(e_p, e_d)$ is an increasing convex function of each of its arguments.

It is easy to verify that $\frac{\partial^2 C(e_p, e_d)}{\partial e_d \partial e_p} = -\rho \frac{\partial C_p(e_p)}{\partial e_p} \frac{\partial C_d(e_d)}{\partial e_d} \leq 0$. We assume that the rest of the model

discussed in Section 2 remains the same. Note that complementarity between prevention and detection functions does not exist if the firm uses two different MSSPs for these functions. So, we set $\rho = 0$ in the cost function when we analyze the two-MSSP contract.

Appendix B presents our analysis of the contracts when there is complementarity between prevention and detection functions. The analysis shows that the propositions under cost complementarity are identical to the corresponding propositions for the base model except for the optimum fixed fee in single MSSP contracts. The key impact of complementarity between prevention and detection functions relates to the conditions under which the firm will prefer two MSSPs over a single MSSP. The firm's expected payoffs under the three contracts are the following.

$$\text{Penalty-based contract: } -\theta(e_p^{1-MSSP-P})L(1-(1-\alpha)\kappa) - C_p(e_p^{1-MSSP-P}) - u$$

$$\text{Penalty-and-reward-based contract: } -\theta(e_p^*)L\left(1-(1-\alpha)\left(\kappa+(1-\kappa)\phi(e_d^*)\right)\right) - C_p(e_p^*) - C_d(e_d^*) + \rho C_p(e_p^*)C_d(e_d^*) - u$$

$$\text{2-MSSP contract: } -\theta(e_p^*)L\left(1-(1-\alpha)\left(\kappa+(1-\kappa)\phi(e_d^*)\right)\right) - C_p(e_p^*) - C_d(e_d^*) - u$$

We find that complementarity does not affect the firm's payoff when it uses a penalty-based contract because the MSSP does not spend any detection effort even when there is complementarity between prevention and detection efforts. Complementarity does not affect the firm's payoff in the two-MSSP contract also because the prevention and detection functions are separated and outsourced to different MSSPs. On the other hand, complementarity improves the firm's payoff when the firm uses a single MSSP and a penalty-and-reward-based contract.

Clearly, when a cost complementarity between prevention and detection efforts exists, the firm realizes the maximum payoff when it uses a single MSSP and the penalty-and-reward-based contract. However, as we discussed earlier, the two-MSSP contract is superior to the other two from the feasibility and fairness criterion perspective. Therefore, when complementarity exists between prevention and detection functions, the firm has to carefully analyze the tradeoff between feasibility and payoff before choosing to outsource to a single MSSP or two MSSPs. The following numerical example illustrates the tradeoff between feasibility and payoff while choosing between single MSSP and two MSSPs.

Table 3. Feasibility-Payoff Tradeoff when there is Complementarity between Prevention and Detection

($c_p = 5, c_d = 1, v = 0.7, \xi_p = 0.9, \xi_d = 0.8, \kappa = 0.7, \alpha = 0.1, m = 0.5, L = 3000, u_p = u_d = u = 0, \rho = 0.2$)

Contract Type	Optimum Penalty p	Feasibility? (Is $p < L=3000$?)	Firm's Payoff
1-MSSP-P-R	3171	No	-17.90
2-MSSP	800	Yes	-29.94

In the above example, the two-MSSP contract is feasible but the 1-MSSP-P-R contract is not. On the other hand, the two-MSSP contract has a lower payoff than the 1-MSSP-P-R contract.

5.2 m depends on e_p

In our base model, we assumed the probability of the investigation finding the MSSP responsible for a breach was independent of the MSSP's effort. We relax this assumption in this section and analyze the

case in which a higher prevention effort by the MSSP will decrease the likelihood of finding the MSSP to be at fault for the breach. We assume the probability of finding the MSSP liable for a breach $m(e_p)$ is a decreasing convex function of e_p . We also assume that $|m'(e_p)| < |\theta'(e_p)|$ which states that the prevention effort has a higher marginal impact on the probability of breach than on the probability of MSSP being deemed responsible for the breach. The rest of the model remains identical to that in the base model as discussed in Sections 3 and 4.

Our analysis shows that the first-best solution is unaffected by m , and therefore, Proposition 1 holds. Appendix C provides the analysis of the three contracts considered in this paper. The analysis shows that the characteristics of the optimum contracts when m is a function of e_p (given in Propositions C2 through C7) are qualitatively similar to those when m is independent of e_p (given in Propositions 2 through 7). Of course, the quantitative expressions are more complex when m is a function of e_p , than when m is independent of e_p .

6. Conclusions

We examined the implications for a firm outsourcing security device management and security monitoring to managed security service providers (MSSPs). We showed that the current practice of outsourcing both device management and monitoring functions to the same MSSP using a penalty-based contract results in a higher than the first-best prevention effort and zero (and less than the first-best) detection effort. We then proposed a penalty-and-reward-based contract and a two-MSSP contract, both of which achieve the first-best outcomes. The two-MSSP contract is superior to penalty-and-reward-based contract on the feasibility dimension, and in achieving first-best outcomes when there are limits on penalty and reward. However, outsourcing both prevention and detection functions to the same MSSP with a penalty-and-reward-based contract may offer a higher payoff than outsourcing to two MSSPs if a strong cost complementarity exists between the two functions.

The results provide important implications for security outsourcing. First, the penalty-based outsourcing contract discourages spending detection effort and encourages hiding of detected security

breaches, leading to inefficient outcomes. Second, separating prevention and detection and outsourcing these two different outsourcers eliminates the inefficiency without introducing any additional moral hazard. Third, outsourcing to two MSSPs is particularly desirable when a high level of detection effort is valuable to the firm and there are tight limits on penalty and/or reward. Fourth, a strong complementarity between prevention and detection efforts may tilt the balance in favor of using a single MSSP for both prevention and detection, and therefore, the arguments against using a single MSSP for prevention and detection do not always hold.

The research described in this paper can be extended in different directions. We assumed that the firm and the MSSPs are risk neutral. A valuable extension would be to analyze the impact of risk aversion on the optimum contracts. This extension will provide insights into how the different contracts affect risk sharing between the firm and the MSSPs. Another interesting extension would be to allow the MSSP that offers prevention services to investigate breaches on its own before deciding to reveal them to the firm. This model could provide richer and more comprehensive insights into MSSP's behavior related to hiding of breaches from the firm.

References

- Allen, J., Gabbard, D. and Christopher, M. 2003. "Outsourcing Managed Security Services, " <http://www.cert.org/security-improvement/modules/omss/index.html>. Accessed 6 July 2009
- Antle, R., 1982. "The Auditor as an Economic Agent," *Journal of Accounting Research*, Autumn, Vol. 20
- Arrow, K. 1971. *Essays in the Theory of Risk- Bearing*. Chicago: Markham.
- Baiman, S., Evans, J.H., Noel, J. 1987. "Optimal Contracts with a Utility-Maximizing Auditor, " *Journal of Accounting Research*, Vol. 25, No. 2, pp. 217-244.
- Baker, W. H., Hutton, A., Hylender, C. D., Novak, C., Porter, C., Sartin, B., Tippett, P., and Valentine, J.A. 2009. "Data Breach Investigations Report," A study conducted by the Verizon Business RISK Team.
- Caplan, D. 1999. "Internal Controls and the Detection of Management Fraud," *Journal of Accounting Research*, Vol. 37, No. 1, pp. 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," *International Journal of Electronic Commerce*, (9:1), pp. 70-104.

Dey, D., Fan, M., Zhang, C. 2008. "Design and Analysis of Contracts for Software Outsourcing," *Information Systems Research*, Forthcoming.

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

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

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

Fudenberg, D., Tirole, J. 1998. *Game Theory*. The MIT Press, Cambridge, Massachusetts.

Gaudin, S. 2007. "Security breaches cost \$90 to \$305 per lost record," *InformationWeek*.
<http://www.informationweek.com/news/showArticle.jhtml?articleID=199000222>. Accessed 6 July 2009

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

Grossman, S. J., and O. D. Hart. 1983. "An Analysis of the Principal-Agent Problem," *Econometrica*, 51, no 1, 7-45.

Harris, M. and Raviv, A. 1979. "Optimal incentive contracts with imperfect information," *Journal of Economic Theory*, 20, pp. 231-259.

Holmstrom, B., 1979. "Moral Hazard and Observability," *The Bell Journal of Economics*, (10:1), pp. 74-91.

Kavanagh, K. M., Pescatore, J. 2007. "Magic Quadrant for MSSPs, North America, 1H07", Gartner.

Panko 2009.

Lacity, M.C., Khan, S.A., Willcocks, L.P. 2009. "A review of the IT outsourcing literature: Insights for practice," *Journal of Strategic Information Systems*, 18 (3), pp. 130-146.

Rittinghouse, J., and Hancock, W. 2003. *Cybersecurity Operations Handbook*. Elsevier Digital Press.

Ross, S. A. 1973. "The Economic Theory of Agency: The Principal's Problem," *The American Economic Review*, (63:2), pp. 681-690. *Papers and Proceedings of the Eighty-fifth Annual Meeting of the American Economic Association*.

Schneier, B. 2001. "Managed Security Monitoring: Network Security for the 21st Century," *Computers & Security*, (20:6), pp. 491-503.

Schneier, B. 2002. "The Case for Outsourcing Security," *Computer*, (35:4), pp. 20-26.

Schneier, B. and Ranum, M. 2008. "Face-off: Is Security Market Consolidation a Plague or Progress," *Information Security*.

Sridhar, S. S., and Balachandran, B. V. 1997. "Incomplete Information, Task Assignment, and Managerial Control Systems," *Management Science*, (43:6), pp. 764-778.

Whang, S. 1992. "Contracting for Software Development," *Management Science*, (38), pp. 307-324.

Appendix A

PROOF OF PROPOSITION 1. Let c_p denote the parameter of the prevention cost $C_p(c_p, e_p)$ with

$$\frac{\partial C_p(c_p, e_p)}{\partial c_p} > 0 \text{ and } \frac{\partial^2 C_p(c_p, e_p)}{\partial e_p \partial c_p} > 0 \text{ and let } c_d \text{ denote the parameter of detection cost with}$$

$$C_d(c_d, e_d) \text{ with } \frac{\partial C_d(c_d, e_d)}{\partial c_d} > 0 \text{ and } \frac{\partial^2 C_d(c_d, e_d)}{\partial e_d \partial c_d} > 0. \text{ The prevention cost (detection cost) and the}$$

marginal prevention (detection) cost increase with increases in the prevention (detection) cost parameter.

To prove Proposition 1, we need to show that $\frac{\partial e_p^*}{\partial c_p} < 0$, $\frac{\partial e_d^*}{\partial c_p} > 0$, $\frac{\partial e_d^*}{\partial c_d} < 0$, and $\frac{\partial e_p^*}{\partial c_d} > 0$.

Differentiate (2) and (3) to obtain

$$-L(1-(1-\alpha)(\kappa+(1-\kappa)\phi(e_d)))\theta''(e_p)\frac{\partial e_p^*}{\partial c_p} + \theta'(e_p)L(1-\alpha)(1-\kappa)\phi'(e_d)\frac{\partial e_d^*}{\partial c_p} - C_p''(e_p, c_p)\frac{\partial e_p^*}{\partial c_p} - \frac{\partial^2 C_p(e_p, c_p)}{\partial e_p \partial c_p} = 0 \quad (\text{A1})$$

$$L(1-\kappa)(1-\alpha)\left(\phi'(e_d)\theta'(e_p)\frac{\partial e_p^*}{\partial c_p} + \theta(e_p)\phi''(e_d)\frac{\partial e_d^*}{\partial c_p}\right) - C_d''(c_d, e_d)\frac{\partial e_d^*}{\partial c_p} = 0 \quad (\text{A2})$$

Solving the above, we get

$$\frac{\partial e_p^*}{\partial c_p} = \frac{\frac{\partial^2 C_p(e_p, c_p)}{\partial e_p \partial c_p}}{-L(1-(1-\alpha)(\kappa+(1-\kappa)\phi(e_d)))\theta''(e_p) + \frac{(\theta'(e_p)L(1-\alpha)(1-\kappa)\phi'(e_d))^2}{C_d''(c_d, e_d) - L(1-\alpha)(1-\kappa)\theta(e_p)\phi''(e_d)} - C_p''(e_p, c_p)} < 0$$

where the last inequality follows from convexity of the cost functions and the second order conditions for an interior optimum. From (A2)

$$\frac{\partial e_d^*}{\partial c_p} = \left(\frac{L(1-\kappa)(1-\alpha)\phi'(e_d)\theta'(e_p)}{C_d''(c_d, e_d) - L(1-\alpha)(1-\kappa)\theta(e_p)\phi''(e_d)} \right) \frac{\partial e_p^*}{\partial c_p} > 0.$$

Following a similar procedure, $\frac{\partial e_d^*}{\partial c_d} < 0$ and $\frac{\partial e_p^*}{\partial c_d} > 0$ can be established.

PROOF OF LEMMA 1. (1) It follows from the fact that the expected future payoff to the MSSP when it reveals the breach $-mp$ is less than the expected future payoff of zero when it does not reveal the breach.

(2) Using (5), because the MSSP does not reveal breaches, we obtain the MSSP's expected payoff when the MSSP does not put any detection effort as $F - \theta(e_p)mp\kappa - C_p(e_p)$ which is greater than the MSSP's expected payoff when it spends detection effort $F - \theta(e_p)mp\kappa - C_p(e_p) - C_d(e_d)$

PROOF OF PROPOSITION 2. The result that the first-best solution is not achieved follows trivially from the fact $e_d^* > 0$ and $e_d^{1-MSSP-P} = 0$.

The Lagrangian of Program 1-MSSP-P with λ and μ as the Lagrange multipliers on IC_{e_p} and IR is

$$L^{1-MSSP-P} = -F - \theta(e_p)(L(1 - (1 - \alpha)\kappa) - \kappa pm) + \lambda(-\theta'(e_p)mp\kappa - C'_p(e_p)) + \mu(F - \theta(e_p)mp\kappa - C_p(e_p) - u)$$

The first-order conditions for optimality are

$$\frac{\partial L^{1-MSSP-P}}{\partial F} = -1 + \mu^{1-MSSP-P} = 0 \quad (A3)$$

$$\frac{\partial L^{1-MSSP-P}}{\partial p} = \theta(e_p^{1-MSSP-P})\kappa m - \lambda^{1-MSSP-P}\theta'(e_p^{1-MSSP-P})m\kappa - \mu^{1-MSSP-P}\theta(e_p^{1-MSSP-P})m\kappa = 0 \quad (A4)$$

$$\frac{\partial L^{1-MSSP-P}}{\partial \lambda} = -\theta'(e_p^{1-MSSP-P})mp^{1-MSSP-P}\kappa - C'_p(e_p^{1-MSSP-P}) = 0 \quad (A5)$$

$$\frac{\partial L^{1-MSSP-P}}{\partial \mu} = F^{1-MSSP-P} - \theta(e_p^{1-MSSP-P})mp^{1-MSSP-P}\kappa - C_p(e_p^{1-MSSP-P}) - u = 0 \quad (A6)$$

where the superscript 1-MSSP-P indicating the optimum.

Substituting $\mu^{1-MSSP-P} = 1$ from (A3) in (A4) we get $\lambda^{1-MSSP-P} = 0$. Using (A5), we get

$$p^{1-MSSP-P} = \frac{C'_p(e_p^{1-MSSP-P})}{-\theta'(e_p^{1-MSSP-P})m\kappa}, \quad (A7)$$

and using (A6), we get

$$F^{1-MSSP-P} = \theta(e_p^{1-MSSP-P})mp^{1-MSSP-P}\kappa + C_p(e_p^{1-MSSP-P}) + u \quad (A8)$$

Substituting (A7), A(8), $\mu^{1-MSSP-P} = 1$ and $\lambda^{1-MSSP-P} = 0$ in the firm's objective function and taking first derivative with respect to e_p we obtain

$$-C'_p(e_p^{1-MSSP-P}) - \theta'(e_p^{1-MSSP-P}) \left(L(1 - (1 - \alpha)\kappa) \right) = 0 \quad (A9)$$

Comparing (A9) with (A7), we obtain

$$p^{1-MSSP-P} = \frac{L(1 - (1 - \alpha)\kappa)}{m\kappa} \quad (A10)$$

Comparing $p^{1-MSSP-P}$ with L yields Proposition 2(4).

Further, comparing (A9) and (2), and noting that $\left(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d^*)) \right) < (1 - (1 - \alpha)\kappa)$, we get

$$e_p^{1-MSSP-P} > e_p^*.$$

PROOF OF PROPOSITION 3. The Lagrangian of Program 1-MSSP-P-R-R with λ_p , λ_d , μ and γ as the

Lagrange multipliers on IC_{e_p} , IC_{e_d} , IR and Revelation is

$$\begin{aligned} L^{1-MSSP-P-R-R} = & -F - \theta(e_p) \left(L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - \kappa pm - \phi(e_d)(1 - \kappa)(pm - r) \right) \\ & + \lambda_p \left(-\theta'(e_p)(mp\kappa + (1 - \kappa)\phi(e_d)(pm - r)) - C'_p(e_p) \right) + \lambda_d \left(-\theta(e_p)(1 - \kappa)\phi'(e_d)(pm - r) - C'_d(e_d) \right) \\ & + \mu \left(F - \theta(e_p^{1-MSSP}) \left(mp\kappa + (1 - \kappa)\phi(e_d^{1-MSSP})(pm - r) \right) - C_p(e_p^{1-MSSP}) - C_d(e_d^{1-MSSP}) - u \right) + \gamma(r - mp) \end{aligned}$$

From the first-order condition with respect to F , we obtain

$$\frac{\partial L^{1-MSSP-P-R-R}}{\partial F} = -1 + \mu^{1-MSSP-P-R-R} = 0. \quad (A11)$$

where the superscript 1-MSSP-P-R-R indicating the optimum. After substituting $\mu^{1-MSSP-P-R-R} = 1$ from

(A11) in $L^{1-MSSP-P-R-R}$, Lagrangian simplifies as follows:

$$\begin{aligned} L^{1-MSSP-P-R-R} = & -\theta(e_p)L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - C_p(e_p) - C_d(e_d) - u + \\ & + \lambda_p \left(-\theta'(e_p)(mp\kappa + (1 - \kappa)\phi(e_d)(pm - r)) - C'_p(e_p) \right) + \lambda_d \left(-\theta(e_p)(1 - \kappa)\phi'(e_d)(pm - r) - C'_d(e_d) \right) + \gamma(r - mp) \end{aligned}$$

Continuing with

the remaining first-order conditions for optimality:

$$\frac{\partial L^{1-MSSP-P-R-R}}{\partial p} = \lambda_p \left(-\theta'(e_p)(m\kappa + (1-\kappa)\phi(e_d)m) \right) + \lambda_d \left(-\theta(e_p)(1-\kappa)\phi'(e_d)m \right) - \gamma m = 0 \quad (A12)$$

$$\frac{\partial L^{1-MSSP-P-R-R}}{\partial r} = \lambda_p \left(\theta'(e_p)((1-\kappa)\phi(e_d)) \right) + \lambda_d \left(\theta(e_p)(1-\kappa)\phi'(e_d) \right) + \gamma = 0 \quad (A13)$$

$$\frac{\partial L^{1-MSSP-P}}{\partial \lambda_p} = -\theta'(e_p)(mp\kappa + (1-\kappa)\phi(e_d)(pm-r)) - C'_p(e_p) = 0 \quad (A14)$$

$$\frac{\partial L^{1-MSSP-P}}{\partial \lambda_d} = -\theta(e_p)(1-\kappa)\phi'(e_d)(pm-r) - C'_d(e_d) = 0 \quad (A15)$$

$$\frac{\partial L^{1-MSSP-P}}{\partial \gamma} = r - mp = 0 \quad (A16)$$

Solving (A12) and (A13) simultaneously, we get

$\lambda_p^{1-MSSP-P-R-R} = 0$, $\lambda_d^{1-MSSP-P-R-R} = 0$, and $\gamma^{1-MSSP-P-R-R} = 0$. After substituting these parameters in the

Lagrangian, it further simplifies to

$L^{1-MSSP-P-R-R} = -\theta(e_p)L(1-(1-\alpha)(\kappa+(1-\kappa)\phi(e_d))) - C_p(e_p) - C_d(e_d) - u$ which is equal to joint

payoff Π of first-best problem minus u . Hence the first-best solution is achieved, i.e.,

$$e_p^{1-MSSP-P-R-R} = e_p^* \text{ and } e_d^{1-MSSP-P-R-R} = e_d^*.$$

Taking first order condition with respect to e_p and e_d we obtain

$$-\theta'(e_p)L(1-(1-\alpha)(\kappa+(1-\kappa)\phi(e_d))) - C'_p(e_p) = 0 \quad (A17)$$

$$\theta(e_p)L(1-\alpha)(1-\kappa)\phi'(e_d) - C'_d(e_d) = 0 \quad (A18)$$

$$\text{Comparing (A17) with (A14), we obtain } p^{1-MSSP-P-R-R} = \frac{L(1-(1-\alpha)\kappa)}{m\kappa} \quad (A19)$$

From the comparison of (A18) with (A15), we obtain $L(1-\alpha) = r^{1-MSSP-P-R-R} - p^{1-MSSP-P-R-R}m$ (A20).

$$\text{Substituting (A19) in (A20), we get } r^{1-MSSP-P-R-R} = \frac{L}{\kappa} \quad (A21)$$

Comparing $p^{1-MSSP-P-R-R}$ with L yields Proposition 3(3).

Proposition 3(4) directly follows from (A20) and (A21).

PROOF OF PROPOSITION 4. If a no-revelation equilibrium is induced, Lemma 1(2) holds. Further, because the MSSP does not obtain any reward because it does not reveal any breach, the penalty-and-reward-based contract reduces to the penalty-based contract. Therefore, Proposition 2 holds in a no-revelation equilibrium under the penalty-and-reward-based contract..

PROOF OF PROPOSITION 5. Since a revelation equilibrium induces the first-best efforts which maximizes the joint payoff as well as the firm's payoff (note that the firm's payoff is equal to the joint payoff minus the reservation utility of the MSSP), but a no-revelation equilibrium does not induce first-best efforts and results in a lower payoff for the firm, the firm prefers a revelation equilibrium.

PROOF OF PROPOSITION 6. The Lagrangian of Program 2-MSSP with λ_p , λ_d , μ_p and μ_D as the Lagrange multipliers on IC_{e_p} , IC_{e_d} , IR_p and IR_D is

$$\begin{aligned} L^{2-MSSP} = & -F_p - F_D - \theta(e_p) \left(L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - \kappa pm - \phi(e_d)(1 - \kappa)(pm - r) \right) \\ & + \lambda_p \left(-\theta'(e_p)mp(\kappa + (1 - \kappa)\phi(e_d)) - C'_p(e_p) \right) + \lambda_D \left(\theta(e_p)(1 - \kappa)\phi'(e_d)r - C'_d(e_d) \right) \\ & + \mu_p \left(F_p - \theta(e_p)mp(\kappa + (1 - \kappa)\phi(e_d)) - C_p(e_p) - u_p \right) + \mu_D \left(F_D + \theta(e_d)(1 - \kappa)\phi(e_d)r - C_d(e_d) - u_D \right) \end{aligned}$$

From the first-order condition with respect to F_p and F_D , we obtain

$$\frac{\partial L^{2-MSSP}}{\partial F_p} = -1 + \mu_p^{2-MSSP} = 0 \quad (A22)$$

$$\text{and } \frac{\partial L^{2-MSSP}}{\partial F_D} = -1 + \mu_D^{2-MSSP} = 0 \quad (A23)$$

where the superscript 2-MSSP indicating the optimum.

After substituting $\mu_p^{2-MSSP} = 1$ and $\mu_D^{2-MSSP} = 1$ from (A22) and (A23) in L^{2-MSSP} , it simplifies as follows:

$$\begin{aligned} L^{2-MSSP} = & -\theta(e_p)L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - C_p(e_p) - C_d(e_d) - u_p - u_D + \\ & + \lambda_p \left(-\theta'(e_p)mp(\kappa + (1 - \kappa)\phi(e_d)) - C'_p(e_p) \right) + \lambda_D \left(\theta(e_p)(1 - \kappa)\phi'(e_d)r - C'_d(e_d) \right) \end{aligned}$$

Continuing with the remaining first-order conditions for optimality:

$$\frac{\partial L^{1-MSSP-P-R-R}}{\partial p} = -\lambda_p \theta'(e_p) m(\kappa + (1-\kappa)\phi(e_d)) = 0 \quad (A24)$$

$$\frac{\partial L^{1-MSSP-P-R-R}}{\partial r} = \lambda_D \theta(e_p) (1-\kappa)\phi'(e_d) = 0 \quad (A25)$$

$$\frac{\partial L^{1-MSSP-P}}{\partial \lambda_p} = -\theta'(e_p) m p (\kappa + (1-\kappa)\phi(e_d)) - C_p'(e_p) = 0 \quad (A26)$$

$$\frac{\partial L^{1-MSSP-P}}{\partial \lambda_D} = \theta(e_p) (1-\kappa)\phi'(e_d) r - C_d'(e_d) = 0 \quad (A27)$$

From (A24) and (A25), we get $\lambda_p^{2-MSSP} = 0$, and $\lambda_D^{2-MSSP} = 0$. After substituting these parameters in the Lagrangian, it further simplifies to

$L^{1-MSSP-P-R-R} = -\theta(e_p) L(1 - (1-\alpha)(\kappa + (1-\kappa)\phi(e_d))) - C_p(e_p) - C_d(e_d) - u_p - u_D$ which is equal to joint payoff Π of first-best problem minus $(u_p + u_D)$. Hence the first-best solution is achieved, i.e.,

$$e_p^{2-MSSP} = e_p^* \text{ and } e_d^{2-MSSP} = e_d^*.$$

Taking first order condition with respect to e_p and e_d we obtain

$$\theta(e_p) L(1-\alpha)(1-\kappa)\phi'(e_d) - C_d'(e_d) = 0 \quad (A28)$$

$$-\theta'(e_p) L(1 - (1-\alpha)(\kappa + (1-\kappa)\phi(e_d))) - C_p'(e_p) = 0 \quad (A29)$$

$$\text{Comparing (A29) with (A26), we obtain } p^{2-MSSP} = \frac{L(1 - (1-\alpha)(\kappa + (1-\kappa)\phi(e_d^*)))}{m(\kappa + (1-\kappa)\phi(e_d^*))} \quad (A30)$$

$$\text{From the comparison of (A28) with (A27), we obtain } r^{2-MSSP} = L(1-\alpha) \quad (A31).$$

Comparing p^{2-MSSP} with L yields Proposition 6(3).

Comparison of (A20) with $L(1-\alpha) + mp^{2-MSSP}$, and L yields Proposition 6(4).

PROOF OF COROLLARY 1.

Proof is omitted because simple algebraic manipulations of the relevant expressions provided in other propositions show the result.

PROOF OF PROPOSITION 7.

Proposition 7(1) follows from Proposition 2(1) and Lemma 1.

A sketch of the proof for Proposition 7(2) is as follows. Suppose the firm induces a no-revelation equilibrium. In this case, the reward r does not play a role in either the MSSP's or the firm's decision. Therefore, the firm's problem under a penalty constraint becomes program 1-MSSP-P with the additional constraint $p \leq P$. We can show that this constraint will be binding in the equilibrium.

Now, suppose the firm induces a revelation equilibrium. The firm's problem under a penalty constraint becomes program 1-MSSP-P-R-R with the additional constraint $p \leq P$. Again, we can show that this constraint will be binding in the equilibrium.

When $p = P$, we find that the firm's optimum payoff under program 1-MSSP-P-R-R is at least as high as its optimum payoff under program 1-MSSP-P. Therefore, the firm prefers the revelation equilibrium even under a penalty constraint.

It is straightforward to see that when $p \neq L \frac{1-(1-\alpha)\kappa}{m\kappa}$, the prevention effort is not equal to e_p^* , and therefore first-best solution is not achieved.

The proof for Proposition 7(3) follows directly from p^{2-MSSP} given in Proposition 6(2)).

PROOF OF PROPOSITION 8.

The proof for Proposition 8(1) follows from the revelation condition. From Proposition 6, we know that in 2-MSSP outsourcing, the firm induces first-best solution if it can offer a reward of $L(1-\alpha)$. Hence in 2-MSSP outsourcing, under given reward limit, the firm still can induce first-best solution if $L(1-\alpha) \leq R$.

PROOF OF PROPOSITION 9.

Proposition 9(1) follows from Proposition 3(2).

Proposition 9(2) follows from the following expression.

$$\frac{\partial p^{2-MSSP}}{\partial c_p} = \frac{-L(1-\kappa)\phi'(e_d^*) \frac{\partial e_d^*}{\partial c_p}}{m((\kappa + (1-\kappa)\phi(e_d^*)))^2} < 0, \text{ since from Proposition 1 we know that } \frac{\partial e_d^*}{\partial c_p} > 0.$$

The proof for the impact of detection cost is analogous to that of the impact of prevention cost.

Appendix B

Proposition B1: Lemma 1, Proposition 2-6 hold when there is a cost complementarity between prevention and detection efforts.

Proof:

(i) The proof that LEMMA 1 holds is the same as that for Lemma 1

(ii) When the firm uses penalty-based contract, the complementarity does not affect firm's and MSSP's payoffs, hence Proposition 2 holds under cost complementarity.

(iii) The Lagrangian of Program 1-MSSP-P-R-R under cost complementarity with $\lambda_p, \lambda_d, \mu$ and γ as

the Lagrange multipliers on IC_{e_p}, IC_{e_d}, IR and Revelation is

$$\begin{aligned} L_B^{1-MSSP-P-R-R} = & -F - \theta(e_p) \left(L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - \kappa pm - \phi(e_d)(1 - \kappa)(pm - r) \right) \\ & + \lambda_p \left(-\theta'(e_p)(mp\kappa + (1 - \kappa)\phi(e_d)(pm - r)) - C_p'(e_p) + \rho C_p'(e_p)C_d(e_d^{1-MSSP}) \right) \\ & + \lambda_d \left(-\theta(e_p)(1 - \kappa)\phi'(e_d)(pm - r) - C_d'(e_d) + \rho C_d'(e_d)C_p(e_p^{1-MSSP}) \right) \\ & + \mu \left(F - \theta(e_p^{1-MSSP})(mp\kappa + (1 - \kappa)\phi(e_d^{1-MSSP})(pm - r)) - C_p(e_p^{1-MSSP}) - C_d(e_d^{1-MSSP}) + \rho C_p(e_p^{1-MSSP})C_d(e_d^{1-MSSP}) - u \right) + \gamma \left(\right) \end{aligned}$$

From the first-order condition with respect to F , we obtain

$$\frac{\partial L_B^{1-MSSP-P-R-R}}{\partial F} = -1 + \mu^{1-MSSP-P-R-R} = 0. \quad (B1)$$

where the superscript 1-MSSP-P-R-R indicating the optimum. After substituting $\mu^{1-MSSP-P-R-R} = 1$ in

$L_B^{1-MSSP-P-R-R}$, Lagrangian simplifies as follows:

$$\begin{aligned} L_B^{1-MSSP-P-R-R} = & -\theta(e_p)L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - C_p(e_p) - C_d(e_d) + \rho C_p(e_p^{1-MSSP})C_d(e_d^{1-MSSP}) - u + \\ & + \lambda_p \left(-\theta'(e_p)(mp\kappa + (1 - \kappa)\phi(e_d)(pm - r)) - C_p'(e_p) + \rho C_p'(e_p)C_d(e_d^{1-MSSP}) \right) \\ & + \lambda_d \left(-\theta(e_p)(1 - \kappa)\phi'(e_d)(pm - r) - C_d'(e_d) + \rho C_d'(e_d)C_p(e_p^{1-MSSP}) \right) + \gamma(r - mp) \end{aligned}$$

Continuing with

the remaining first-order conditions for optimality:

$$\frac{\partial L_B^{1-MSSP-P-R-R}}{\partial p} = \lambda_p \left(-\theta'(e_p)(m\kappa + (1-\kappa)\phi(e_d)m) \right) + \lambda_d \left(-\theta(e_p)(1-\kappa)\phi'(e_d)m \right) - \gamma m = 0 \quad (B2)$$

$$\frac{\partial L_B^{1-MSSP-P-R-R}}{\partial r} = \lambda_p \left(\theta'(e_p)(1-\kappa)\phi(e_d) \right) + \lambda_d \left(\theta(e_p)(1-\kappa)\phi'(e_d) \right) + \gamma = 0 \quad (B3)$$

$$\frac{\partial L_B^{1-MSSP-P}}{\partial \lambda_p} = -\theta'(e_p)(mp\kappa + (1-\kappa)\phi(e_d)(pm-r)) - C_p'(e_p) + \rho C_p'(e_p)C_d(e_d^{1-MSSP}) = 0 \quad (B4)$$

$$\frac{\partial L_B^{1-MSSP-P}}{\partial \lambda_d} = -\theta(e_p)(1-\kappa)\phi'(e_d)(pm-r) - C_d'(e_d) + \rho C_d'(e_d)C_p(e_p^{1-MSSP}) = 0 \quad (B5)$$

$$\frac{\partial L_B^{1-MSSP-P}}{\partial \gamma} = r - mp = 0 \quad (B6)$$

Solving (B2) and (B3) simultaneously, we get $\lambda_p^{1-MSSP-P-R-R} = 0$, $\lambda_d^{1-MSSP-P-R-R} = 0$, and $\gamma^{1-MSSP-P-R-R} = 0$.

After substituting these parameters in the Lagrangian, it further simplifies to

$$L_B^{1-MSSP-P-R-R} = -\theta(e_p)L(1-(1-\alpha)(\kappa+(1-\kappa)\phi(e_d))) - C_p(e_p) - C_d(e_d) + \rho C_p(e_p^{1-MSSP})C_d(e_d^{1-MSSP}) - u$$

which is equal to joint payoff Π of first-best problem. Hence the first-best solution is achieved, i.e.,

$$e_p^{1-MSSP-P-R-R} = e_p^* \text{ and } e_d^{1-MSSP-P-R-R} = e_d^*.$$

Taking first order condition with respect to e_p and e_d we obtain

$$-\theta'(e_p)L(1-(1-\alpha)(\kappa+(1-\kappa)\phi(e_d))) - C_p'(e_p) + \rho C_p'(e_p)C_d(e_d) = 0 \quad (B7)$$

$$\theta(e_p)L(1-\alpha)(1-\kappa)\phi'(e_d) - C_d'(e_d) + \rho C_d'(e_d)C_p(e_p^{1-MSSP}) = 0 \quad (B8)$$

$$\text{Comparing (B4) with (B7), we obtain } p^{1-MSSP-P-R-R} = \frac{L(1-(1-\alpha)\kappa)}{m\kappa} \quad (B9)$$

From the comparison of (B5) with (B8), we obtain $L(1-\alpha) = r^{1-MSSP-P-R-R} - p^{1-MSSP-P-R-R}m$ (B10).

$$\text{Substituting (B9) in (B10), we get } r^{1-MSSP-P-R-R} = \frac{L}{\kappa} \quad (B11)$$

$$F^{1-MSSP-P-R-R} = \theta(e_p^{1-MSSP-P-R-R})L(1-(1-\alpha)(\kappa+(1-\kappa)\phi(e_d^{1-MSSP-P-R-R}))) + C_p(e_p^{1-MSSP-P-R-R}) + C_d(e_d^{1-MSSP-P-R-R}) - \rho C_p(e_p^{1-MSSP})C_d(e_d^{1-MSSP}) + u$$

(iv) When the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches, and the firm induces a no-revelation equilibrium, the complementarity does not affect firm's and MSSP's payoffs; hence Proposition 4 holds under cost complementarity.

(v) When the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches, and the firm does not face a limit on contract terms, the firm induces a revelation equilibrium and first-best efforts. The proof for Proposition 5 holds for any cost function, and hence applies when there is cost complementarity..

(vi) When the firm uses 2-MSSP contract, since the prevention and detection services are provided by different MSSPs, complementarity has no impact on the optimal solution, hence Proposition 6 holds under cost complementarity.

Appendix C

Analysis of the contracts when m is a function of e_p

PROPOSITION C1. (1) *When the cost of prevention effort increases, the first-best prevention effort decreases and the first-best detection effort increases.*

(2) *When the cost of detection effort increases, the first-best prevention effort increases and the first-best detection effort decreases.*

Proof: The expected joint payoff does not contain $m(e_p)$, hence the proof is identical to that of

Proposition 1.

Penalty-based contract

We have the following payoff functions for the firm and the MSSP.

$$\pi_F = \begin{cases} -F - \theta(e_p) \left(L(1 - (1 - \alpha)(\kappa + (1 - \kappa)\phi(e_d))) - \kappa pm(e_p) - \phi(e_d)(1 - \kappa) pm(e_p) \right) & \text{if the MSSP reveals the breach} \\ -F - \theta(e_p) \left(L(1 - (1 - \alpha)\kappa) - \kappa pm(e_p) \right) & \text{if the MSSP does not reveal the breach} \end{cases} \quad (C1)$$

$$\pi_M = \begin{cases} F - \theta(e_p) (m(e_p) p\kappa + (1 - \kappa)\phi(e_d) pm(e_p)) - C_p(e_p) - C_d(e_d) & \text{if the MSSP reveals the breach} \\ F - \theta(e_p) m(e_p) p\kappa - C_p(e_p) & \text{if the MSSP does not reveal the breach} \end{cases} \quad (C2)$$

LEMMA C1. (1) *The MSSP does not reveal a security breach it detects to the firm.*
(2) *The MSSP does not put any detection effort.*

Proof: Same as that for Lemma 1

Knowing that the MSSP will only put prevention effort, the firm's problem is provided in Program C1-MSSP-P.

Program C1-MSSP-P

$$\begin{aligned} \text{Max}_{F, p} \quad & -F - \theta(e_p) \left(L(1 - (1 - \alpha)\kappa) - \kappa p m(e_p) \right) \\ \text{s.t.} \quad & - \left(\theta'(e_p) m(e_p) + \theta(e_p) m'(e_p) \right) p \kappa - C'_p(e_p) = 0 \quad (IC_{e_p}) \\ & F - \theta(e_p) m(e_p) p \kappa - C_p(e_p) \geq u \quad (IR) \end{aligned}$$

PROPOSITION C2. *When the contract includes a fixed fee and a penalty for breaches, the solution to Program 1-MSSP-P has the following properties.*

- (1) *The first-best solution is not achieved.*
- (2) *The optimum prevention (detection) effort is higher than the first-best optimum prevention (detection) effort.*

$$\begin{aligned} (3) \quad p^{C1-MSSP-P} &= \frac{L(1 - (1 - \alpha)\kappa)}{\left(m(e_p^{C1-MSSP-P}) + \frac{\theta(e_p^{C1-MSSP-P})}{\theta'(e_p^{C1-MSSP-P})} m'(e_p^{1-MSSP-P}) \right) \kappa}, \\ F^{C1-MSSP-P} &= \theta(e_p^{C1-MSSP-P}) m(e_p^{C1-MSSP-P}) \frac{L(1 - (1 - \alpha)\kappa)}{\left(m(e_p^{C1-MSSP-P}) + \frac{\theta(e_p^{C1-MSSP-P})}{\theta'(e_p^{C1-MSSP-P})} m'(e_p^{1-MSSP-P}) \right)} + C_p(e_p) + u \end{aligned}$$

- (4) *The optimum penalty on the MSSP is greater than the damage that the firm incurs from a detected breach; furthermore, the optimum penalty could be greater than the damage the firm incurs from an undetected breach. Technically, $p^{1-MSSP-P} > \alpha L$, and $p^{1-MSSP-P} > L$ if and only if $\kappa(1 + m - \alpha) < 1$.*

Proof: Following the same line of reasoning used to prove proposition 2, we find that IR constraint will be binding in the optimum for the program C1-MSSP-P. So, substituting

$\theta(e_p) m(e_p) p \kappa = F - C_p(e_p) - u$ in the firm's objective function, we obtain the following problem for the firm.

$$\text{Max}_{F,p} -C_p(e_p) - u - \theta(e_p)L(1-(1-\alpha)\kappa)$$

$$\text{s.t.} \quad -(\theta'(e_p)m(e_p) + \theta(e_p)m'(e_p))p\kappa - C'_p(e_p) = 0$$

Solving the above problem, we obtain

$$p^{C1-MSSP-P} = \frac{L(1-(1-\alpha)\kappa)}{\left(m(e_p^{C1-MSSP-P}) + \frac{\theta(e_p^{C1-MSSP-P})}{\theta'(e_p^{C1-MSSP-P})} m'(e_p^{1-MSSP-P}) \right) \kappa} \quad \text{and}$$

$$F = \theta(e_p^{C1-MSSP-P})m(e_p^{C1-MSSP-P}) \frac{L(1-(1-\alpha)\kappa)}{\left(m(e_p^{C1-MSSP-P}) + \frac{\theta(e_p^{C1-MSSP-P})}{\theta'(e_p^{C1-MSSP-P})} m'(e_p^{1-MSSP-P}) \right)} + C_p(e_p) + u$$

Penalty-and-Reward-based Contract

The expected payoff for the firm and the MSSP are

$$\pi_F = \begin{cases} -F - \theta(e_p) \left(L(1-(1-\alpha)(\kappa + (1-\kappa)\phi(e_d))) - \kappa pm(e_p) - \phi(e_d)(1-\kappa)(pm(e_p) - r) \right) & \text{if the MSSP reveals the breach} \\ -F - \theta(e_p) \left(L(1-(1-\alpha)\kappa) - \kappa pm(e_p) \right) & \text{if the MSSP does not reveal the breach} \end{cases} \quad (C3)$$

$$\pi_M = \begin{cases} F - \theta(e_p)(m(e_p)p\kappa + (1-\kappa)\phi(e_d)(pm(e_p) - r)) - C_p(e_p) - C_d(e_d) & \text{if the MSSP reveals the breach} \\ F - \theta(e_p)m(e_p)p\kappa - C_p(e_p) & \text{if the MSSP does not reveal the breach} \end{cases} \quad (C4)$$

Under the revelation regime, the firm's problem is provided in Program C1-MSSP-P-R-R.

Program C1-MSSP-P-R-R

$$\begin{aligned}
& \text{Max}_{F,p,r} -F - \theta(e_p) \left(L(1-(1-\alpha)(\kappa+(1-\kappa)\phi(e_d))) - \kappa pm(e_p) - \phi(e_d)(1-\kappa)(pm(e_p)-r) \right) \\
& \text{s.t.} \quad -\theta'(e_p)(m(e_p)p\kappa+(1-\kappa)\phi(e_d)(pm(e_p)-r)) - \theta(e_p)m'(e_p)p(\kappa+(1-\kappa)\phi(e_d)) - C_p'(e_p) = 0 \quad (IC_{e_p}) \\
& \quad -\theta(e_p)(1-\kappa)\phi'(e_d)(pm(e_p)-r) - C_d'(e_d) = 0 \quad (IC_{e_d}) \\
& \quad F - \theta(e_p^{1-MSSP})(m(e_p)p\kappa+(1-\kappa)\phi(e_d^{1-MSSP})(pm(e_p)-r)) - C_p(e_p^{1-MSSP}) - C_d(e_d^{1-MSSP}) \geq u \quad (IR) \\
& \quad r \geq m(e_p)p \quad (\text{Revelation})
\end{aligned}$$

PROPOSITION C3. *When the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches, and the firm induces a revelation equilibrium, the solution to Program 1-MSSP-P-R has the following properties.*

(1) *The first-best solution is achieved, i.e., $e_p^{1-MSSP-P-R-R} = e_p^*$ and $e_d^{1-MSSP-P-R-R} = e_d^*$*

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

$$p^{C1-MSSP-P-R-R} = \frac{L(1-(1-\alpha)\kappa)}{\left(m(e_p^*)\kappa + \frac{\theta(e_p^*)}{\theta'(e_p^*)} m'(e_p^*) (\kappa + (1-\kappa)\phi(e_d^*)) \right)}, \quad r^{1-MSSP-P-R-R} = m(e_p^*)p^{C1-MSSP-P-R-R} + L(1-\alpha), \text{ and}$$

$$F^{1-MSSP-P-R-R} = \theta(e_p^*)L \left(\frac{m(1-(1-\alpha)\kappa)}{m(e_p^*)\kappa + \frac{\theta(e_p^*)}{\theta'(e_p^*)} m'(e_p^*) (\kappa + (1-\kappa)\phi(e_d^*))} - (1-\kappa)(1-\alpha)\phi(e_d^*) \right) + C_p(e_p^*) + C_d(e_d^*) + u$$

(3) *The optimum penalty on the MSSP is greater than the damage that the firm incurs from a detected breach; furthermore, the optimum penalty could be greater than the damage the firm incurs from an undetected breach. Technically, $p^{C1-MSSP-P-R} > \alpha L$, and $p^{C1-MSSP-P-R} > L$ if and only if*

$$\left(m(e_p^*)\kappa + \frac{\theta(e_p^*)}{\theta'(e_p^*)} m'(e_p^*) (\kappa + (1-\kappa)\phi(e_d^*)) \right) + \kappa(1-\alpha) < 1.$$

(4) *The optimum reward is greater than the damage the firm incurs from a breach, but is equal to the benefit the firm obtains from the detection of the breach. Technically,*

$$r^{C1-MSSP-P-R-R} = (1-\alpha)L + mp^{C1-MSSP-P-R-R} > L.$$

Proof: The proof follows the same reasoning as that for Proposition C2.

PROPOSITION C4. *When the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches, and the firm induces a no-revelation equilibrium, the properties of the optimum contract are characterized in Proposition C2.*

Proof: Same as that for Proposition 4.

PROPOSITION C5. *When the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches, the firm induces the first-best efforts from the MSSP and a revelation equilibrium.*

Proof: Same as that for Proposition 5.

Two-MSSP Contract

The expected payoff for the firm and the MSSPs are

$$\pi_F = -F_P - F_D - \theta(e_p) \left(L \left(1 - (1 - \alpha) (\kappa + (1 - \kappa) \phi(e_d)) \right) - \kappa p m(e_p) - \phi(e_d) (1 - \kappa) (p m(e_p) - r) \right) \quad (C5)$$

$$\pi_{M_P} = F_P - \theta(e_p) m(e_p) p (\kappa + (1 - \kappa) \phi(e_d)) - C_p(e_p) \quad (C6)$$

$$\pi_{M_D} = F_D + \theta(e_p) (1 - \kappa) \phi(e_d) r - C_d(e_d). \quad (C7)$$

The firm's problem is provided in Program 2-MSSP.

Program C2-MSSP

$$\begin{aligned} \text{Max}_{F, p, r} \quad & -\theta(e_p) (L((1 - \phi(e_d))(1 - \kappa) + \alpha(\kappa + \phi(e_d)(1 - \kappa))) - \kappa p m(e_p) - \phi(e_d)(1 - \kappa)(p m(e_p) - r)) - F_P - F_D \\ \text{s.t.} \quad & -(\theta'(e_p) m(e_p) + \theta(e_p) m'(e_p)) p (\kappa + (1 - \kappa) \phi(e_d)) - C_p'(e_p) = 0 \quad (IC_{e_p}) \\ & \theta(e_p) (1 - \kappa) \phi'(e_d) r - C_d'(e_d) = 0 \quad (IC_{e_d}) \\ & F_P - \theta(e_p) m(e_p) p (\kappa + (1 - \kappa) \phi(e_d)) - C_p(e_p) \geq u_P \quad (IR_P) \\ & F_D + \theta(e_p) (1 - \kappa) \phi(e_d) r - C_d(e_d) \geq u_D \quad (IR_D) \end{aligned}$$

PROPOSITION C6. *When the firm uses different MSSPs for prevention and detection services, and the contracts include a fixed fee, a penalty for breaches, and a reward for detecting breaches, the solution to Program 2-MSSP has the following properties.*

- (1) *The first-best solution is achieved, i.e., $e_p^{C2-MSSP} = e_p^*$ and $e_d^{C2-MSSP} = e_d^*$.*
- (2) *The optimal contract is given by the following*

$$p^{C2-MSSP} = L \frac{1-(1-\alpha)\left(\kappa+(1-\kappa)\phi(e_d^*)\right)}{\left(m(e_p) + \frac{\theta(e_p)}{\theta'(e_p)} m'(e_p)\right)\left(\kappa+(1-\kappa)\phi(e_d^*)\right)}, \quad r^{C2-MSSP} = L(1-\alpha),$$

$$F_p^{C2-MSSP} = \theta(e_p^*)L\left(1-(1-\alpha)\left(\kappa+(1-\kappa)\phi(e_d^*)\right)\right) \frac{m(e_p)}{\left(m(e_p) + \frac{\theta(e_p)}{\theta'(e_p)} m'(e_p)\right)} + C_p(e_p^*) + u_p,$$

$$F_D^{C2-MSSP} = -\theta(e_p^*)(1-\kappa)\phi(e_d^*)L(1-\alpha) + C_d(e_d^*) + u_D$$

(3) The optimum penalty on the MSSP is greater than the damage that the firm incurs from a detected breach; furthermore, the optimum penalty could be greater than the damage the firm incurs from an undetected breach. Technically, $p^{C2-MSSP} > \alpha L$, and $p^{C2-MSSP} > L$ if and only if

$$\left(\kappa+(1-\kappa)\phi(e_d^*)\right)\left(1+\left(m(e_p) + \frac{\theta(e_p)}{\theta'(e_p)} m'(e_p)\right) - \alpha\right) < 1.$$

(4) The optimum reward is less than the damage the firm incurs from a breach as well as the benefit the firm obtains from the detection of the breach. Technically, $r^{C2-MSSP} < (1-\alpha)L + mp^{C2-MSSP} < L$.

Proof: The proof follows the same reasoning as that for Proposition C2.