Outsourcing Information Security: Contracting Issues and Security Implications

Asunur Cezar
(joint work with Huseyin Cavusoglu and Srinivasan Raghunathan)

Presentation Outline

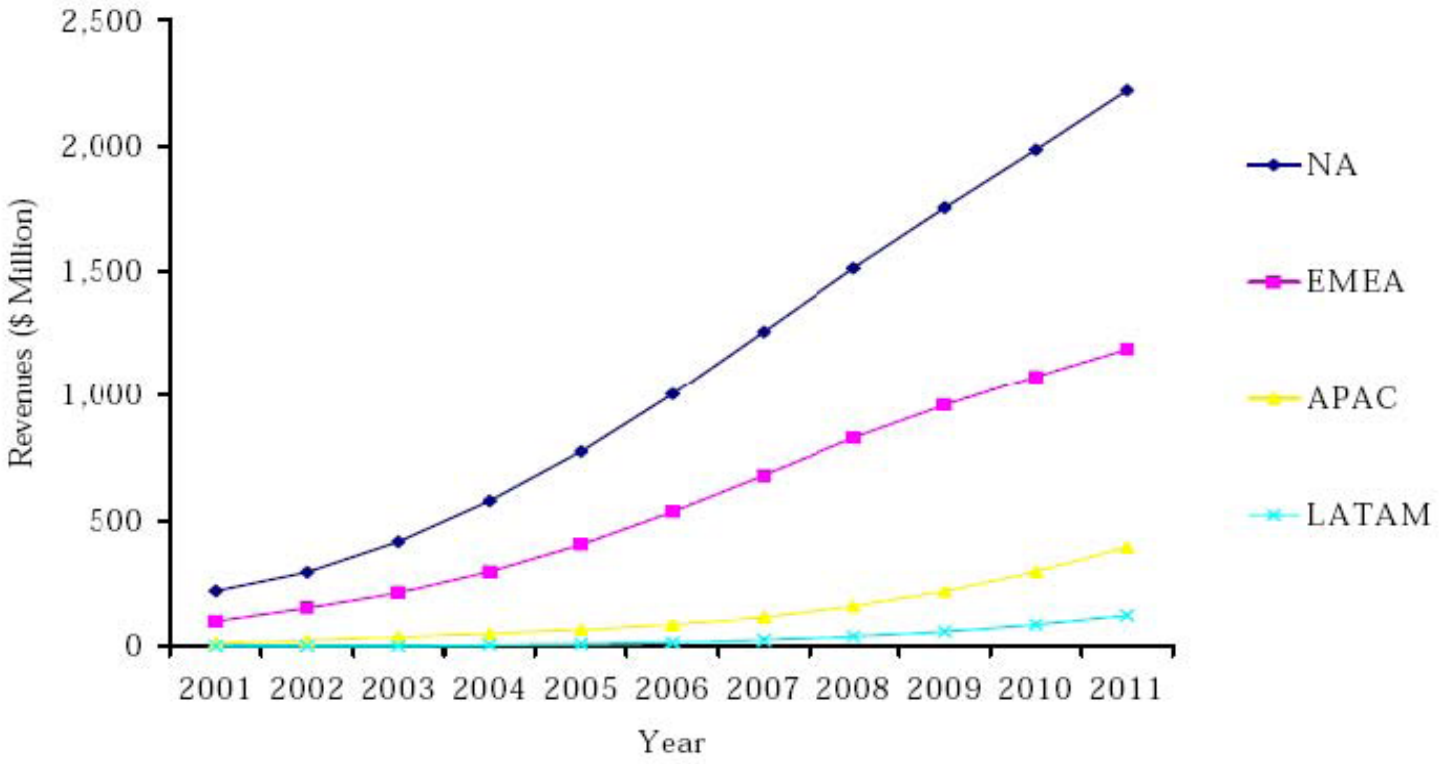
- Market for Outsourcing Information Security
- Research Questions
- Prior Literature
- Model
- Significant Findings
- Summary and Conclusions

Information Security Management

- Rising costs of security breaches
  - ranges from $90 to $305 for each breached customer record (Gaudin 2007)
- Increased security threats
  - attack patterns - scale, scope and sophistication, internal treats…
- Complex information technology environments
- Scarcity of security professionals
- Limited IT budgets
- Compliance and regulatory requirements
  - (SOX, GLBA, HIPPA, etc…)

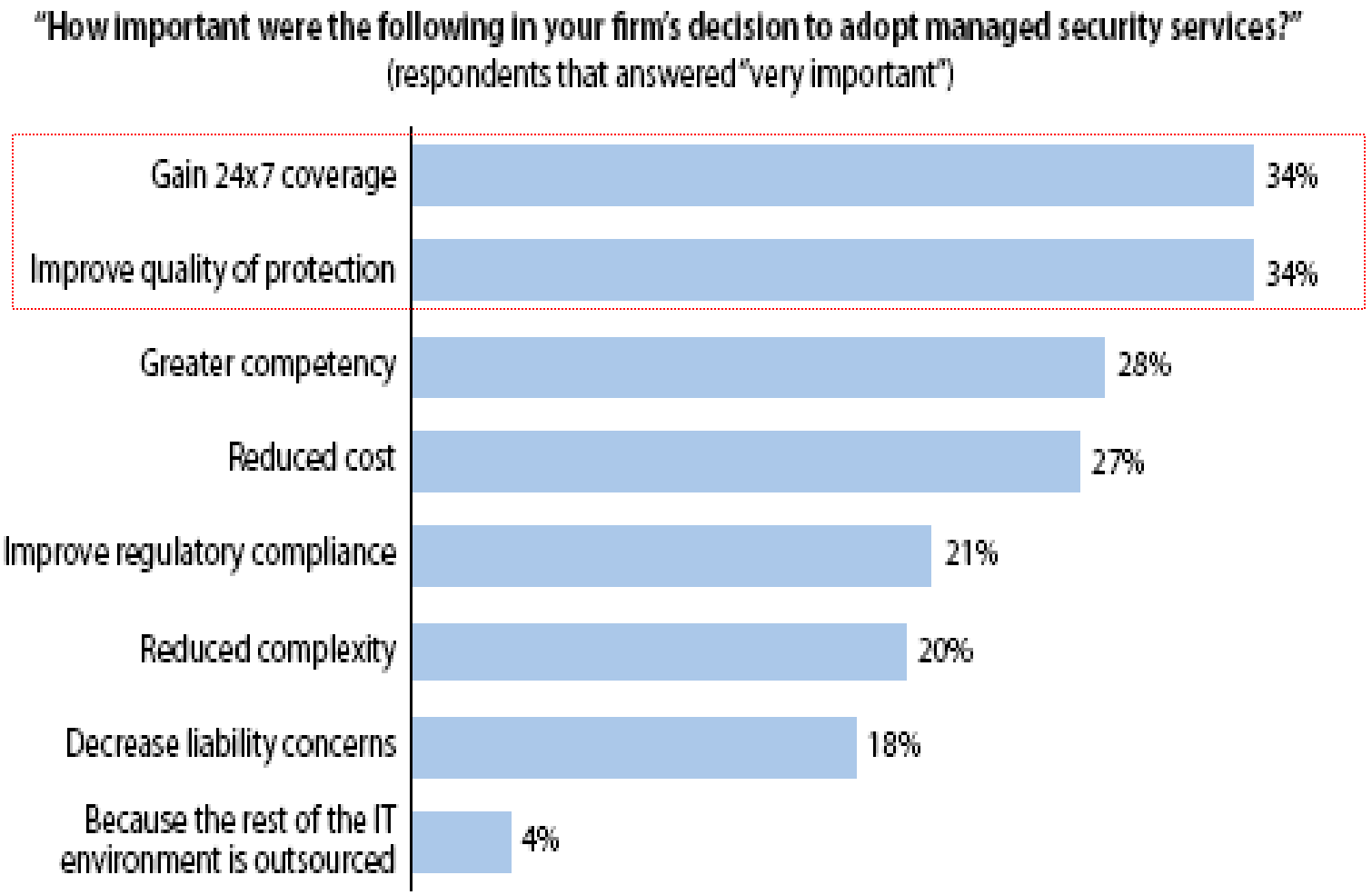
Managed Security Service Provider (MSSP) Market

Total MSSP Market: Revenue Forecasts by Geographic Region (World), 2001-2011



Note: All figures are rounded. Source: Frost & Sullivan

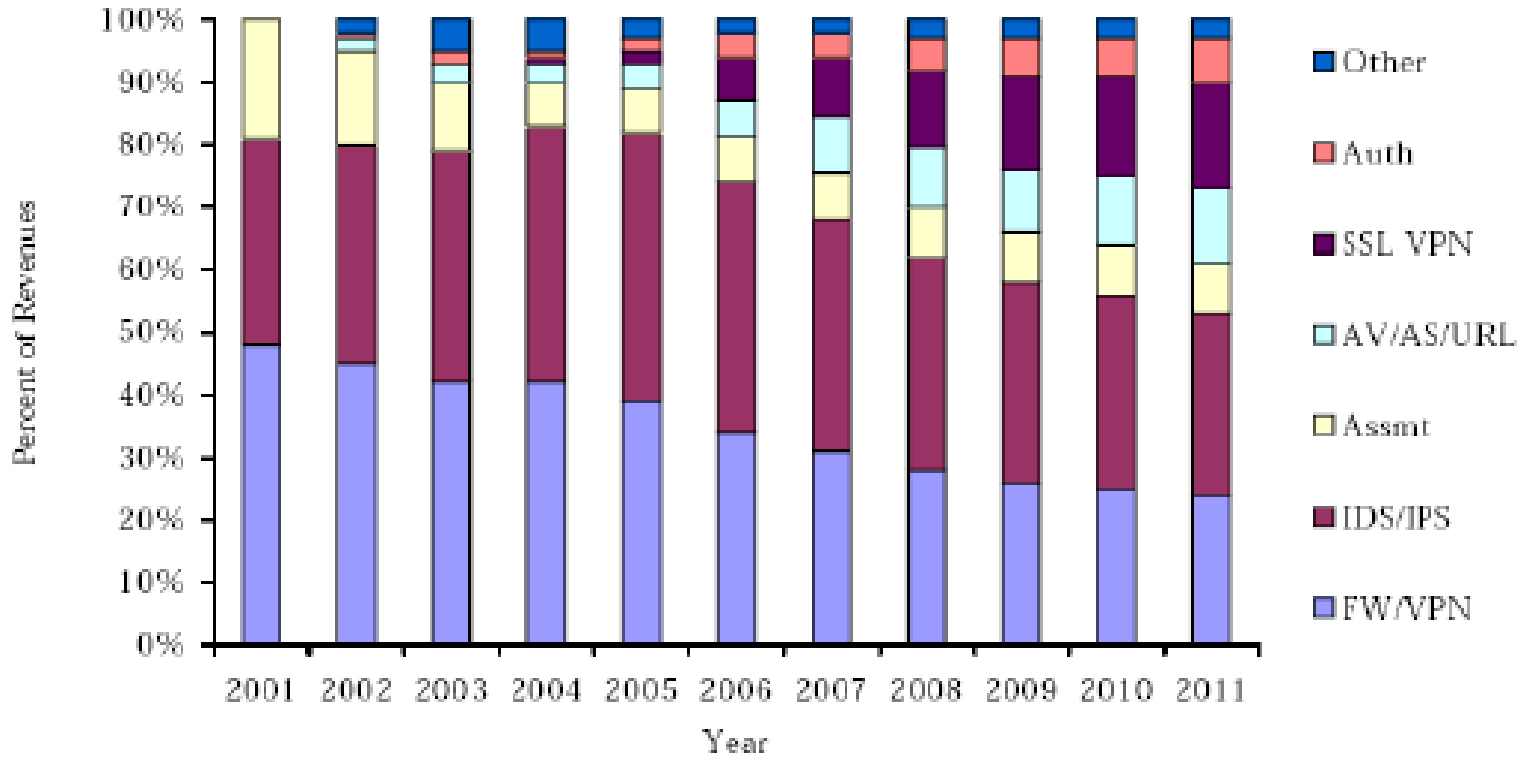
Reasons for Outsourcing Information Security



Base: 1,214 North American and European IT security decision-makers interested in managed security services
Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009

Market by Services Outsourced

Total MSSP Market: Percent of Revenues by Service (World), 2001-2011



Note: All figures are rounded; the base year is 2004. Source: Frost & Sullivan

Nature of Contracts in MSSP Market

- The MSSP offers a menu of services, which may include service bundles
- The firm chooses a service
- Services typically include Service Level Agreements (SLAs)
- Penalty (Refund) Based Contract
  - Upfront Fixed Fee paid by the firm to the MSSP
  - If the SLA is not met, the MSSP provides a refund or a credit to the firm

Sample SLAs

- IBM
  - 100% guarantee of prevention of attacks listed in IBM Internet Security Systems X-Force® Certified Attack List
- Megapath Premium Service:
  - Network Availability: 99.999%
  - Mean Time to Restore: 4 hours
  - Definition updates: 3 hours
  - Outage Notification: 10 minutes
- Verizon
  - Notification of Device Unavailability: 15 minutes

Sample Refunds

- IBM
  - *"Money-back payment*—Offering a unique preemptive protection, IBM ISS offers the industry's leading performance-based SLA with a cash-back payment of US$50,000 for any security breach resulting from a successful attack listed on the IBM Internet Security Systems X-Force® Certified Attack List."
- Verizon
  - Offers a credit equal to one month's fee for a device when a Verizon-managed device is breached
- Megapath
  - Detailed SLAs for various types of services; credit for not meeting standards

Challenges in Outsourcing Information Security

- MSSP's effort is unobservable to the firm
  - Traditional moral hazard problem
- Neither the firm nor the MSSP can observe the effort's outcome perfectly
  - Some breaches are observed by both parties
  - Some breaches are not observed by either party
  - Some are observed by the MSSP but not by the firm, and vice versa
- Even when a breach is observed, uncertainty regarding whether the MSSP met the SLA
  - Ambiguity in contract terms
  - Hackers often delete system logs to erase the evidence

Research Questions

- How should the contract be structured to provide incentives to the MSSP to exert optimum prevention and detection efforts?
  - Does the penalty-based contract offer appropriate incentives?
  - Can we identify other contracts that perform *better* than the penalty-based contracts?
    - Firm's payoff, Contract feasibility

- Feasibility: Based on a fairness criterion – the penalty does not exceed the firm's loss from a security breach.

Prior Literature

- IT Outsourcing (Whang 1992, Wang, Barron, and Seidmann 1997, Dey, Fan, and Zhang 2009) and Information Security Outsourcing (Ding et al. 2005, 2006)
  - Outsourcing a single function, viz., software development, prevention services
  - Single Principal, Single Agent

- Manufacturing (Sridhar and Balachandran 1997)
  - Outsourcing sequentially dependent services
  - Single Principal, Two agents

- Auditing/Contracting (Grossman and Hart 1983, Antle 1982, Baiman et al, 1987)
  - Single Principal, one agent, one auditor
  - Misreporting by the agent, auditing effort is unproductive on its own

Model

- A single firm has decided to outsource prevention and detection services
- Loss from a security breach:
  - L if undetected
  - αL, $0 \leq \alpha \leq L$, if detected
- Probability of breach $\theta(e_p)$; $\theta'(e_p)<0$, $\theta''(e_p)>0$
- Probability of detecting a breach $\nearrow(e_d)$; $\nearrow'(e_d)>0$, $\nearrow''(e_d)<0$
  - $\kappa< 1$ is the probability that the breach is publicly observable and does not require detection effort
- Cost of prevention (detection) effort $C_p(e_p)$; $C_p'(e_p)>0$, $C_p''(e_p)>0$ ($C_d(e_d)$; $C_d'(e_d)$)>0, $C_d''(e_d)>0$)

Benchmark: First-Best Efforts

$$\underset{e_p,\, e_d}{\text{Max}}\ \Pi = -\theta(e_p)L\Big(1-(1-\alpha)\big(\kappa+(1-\kappa)\phi(e_d)\big)\Big)-C_p(e_p)-C_d(e_d)$$

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

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

First-Best Efforts

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.*

Prevention effort and detection effort are substitutes from the social welfare perspective

Penalty-Based contract

- The penalty-based contract is defined by [F, p]
  - F is the up-front fee paid by the firm to the MSSP
  - 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.

- Investigation by an independent third-party decides whether the MSSP is responsible for the breach
  - The probability of finding the MSSP responsible for a breach is m
  - m is independent of e_p in the base model, but results do not change qualitatively when m is a function of e_p.

Penalty-based contract: Sequence of Events

1. Firm offers [F, p]
2. 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 firm. If the breach is revealed, then an investigation occurs and the MSSP pays the firm p if the MSSP is held responsible.

Penalty-Based Contract: Sub-Game Perfect Equilibrium

LEMMA 1.

(1) *The MSSP does not reveal security breaches it detects to the firm.*

(2) *The MSSP does not spend any detection effort.*

Program 1-MSSP-P:

$$\text{Max}_{F,\,p} \; -F-\theta(e_p)\left(L\left(1-(1-\alpha)\kappa\right)-\kappa pm\right)$$

$$\text{s.t.} \quad -\theta'(e_p)mp\kappa - C'_p(e_p) = 0 \qquad (IC_{e_p})$$

$$F-\theta(e_p)mp\kappa - C_p(e_p) \geq u \qquad (IR)$$

Penalty-based contract creates a conflict of interest for the MSSP

"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?... Outsourcers offering combined management and monitoring services will be among the next to disappear." (Schneier 2002)

Penalty-based contract: Solution

PROPOSITION 2. *When the contract includes a fixed fee and a penalty for breaches, the solution has the following properties.*

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

Implications of Penalty-Based Contract

- The penalty-based contract does not maximize the firm's payoff
- The penalty-based contract that offers the maximum payoff to the firm is likely to be infeasible when
  - the probability of finding the MSSP responsible for the breach is low
  - the probability of the firm detecting a breach on its own is low
- A feasible penalty-based contract will increase the gap between the firm's actual payoff and the maximum possible firm's payoff

Penalty-and-Reward-Based Contract

- The penalty-and-reward-based contract is defined by [F, p, r]
  - r is the reward offered to the MSSP if the firm becomes aware of the breach because the MSSP reveals the breach to the firm

Sequence of Events:

1. The firm and the MSSP agree on [F, p, r].
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 firm. If the breach is revealed, the firm pays the MSSP r; an investigation occurs and the MSSP pays the firm p if the MSSP is held responsible.

Penalty-and-Reward-Based Contract (continued)

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

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

In Step 3.3, the MSSP will reveal the breach iff $r >= mp$

Revelation Equilibrium: $r >= mp$

No-Revelation Equilibrium: $r < mp$

Penalty-and-Reward-Based Contract: Revelation Equilibrium

Program 1-MSSP-P-R-R

$$\text{Max}_{F,p,r} \; -F-\theta(e_p)\Big(L\big(1-(1-\alpha)(\kappa+(1-\kappa)\phi(e_d)\big)-\kappa pm-\phi(e_d)(1-\kappa)(pm-r)\Big)$$

$$\text{s.t.} \quad -\theta'(e_p)(mp\kappa+(1-\kappa)\phi(e_d)(pm-r))-C_p'(e_p)=0 \qquad (IC_{e_p})$$

$$-\theta(e_p)(1-\kappa)\phi'(e_d)(pm-r)-C_d'(e_d)=0 \qquad (IC_{e_d})$$

$$F-\theta(e_p^{1-MSSP})(mp\kappa+(1-\kappa)\phi(e_d^{1-MSSP})(pm-r))-C_p(e_p^{1-MSSP})-C_d(e_d^{1-MSSP})\geq u \quad (IR)$$

$$r \geq mp \qquad \text{(Revelation)}$$

Penalty-and-Reward-Based Contract: Revelation Regime

PROPOSITION 3. *When the contract includes a fixed fee, a penalty for breaches, and a reward for detecting breaches the solution has the following properties.*

(1) *The first-best solution is achieved*

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

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

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

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

(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,*

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

Penalty-and-Reward-Based Contract: No-Revelation Equilibrium

- Lemma 1 holds – MSSP does not exert any detection effort
- The optimum contract structure is identical to that under penalty-based contract

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 reward component 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
  - force the MSSP to internalize the substitution between prevention and detection efforts.
- The penalty-and-reward-based contract imposes the same penalty as in the penalty-based contract
  - the penalty-and-reward contract and the penalty-based contract are identical on the feasibility dimension.
- The optimum penalty and reward are independent of cost parameters

2-MSSP contract

- The firm outsources the prevention function to one MSSP, M_P, and the detection function to a different MSSP, 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.

2-MSSP contract: Sequence of Events

1. Firm and M_P agree on [F_P , p]; firm and M_D agree on [F_D , r]
2. M_P chooses e_p; M_D e_d chooses
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 firm. An investigation occurs and M_P pays p if held responsible.

2-MSSP contract

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

(1) *The first-best solution is achieved*

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

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

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

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

(3) *The optimum penalty could be greater than the damage L that firm incurs from an undetected breach, iff* $\left(\kappa+(1-\kappa)\phi(e_d^*)\right)\left(1+m-\alpha\right)<1$

(4) *The optimum reward is less than the damage L firm incurs from an undetected breach as well as the expected benefit firm obtains from the detection of the breach,* $r^{2-MSSP} < (1-\alpha)L + mp^{2-MSSP} < L$

2-MSSP Contract

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.

Intuition:

In a single MSSP contract, both penalty and reward play a dual and conflicting role

- a reward reduces the effective penalty and a penalty reduces the effective reward

In a two-MSSP contract, each plays its intended role

Feasibility of Contracts

- *Definition*: A contract is feasible if penalty imposed on the MSSP for a security breach is less than L.

- The penalty-based and the penalty-and-reward-based contracts are identical on the feasibility dimension

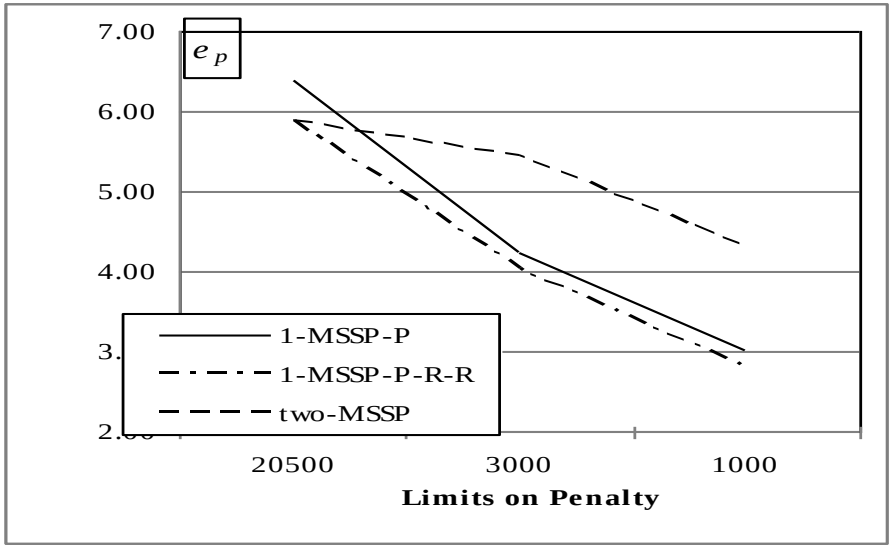
- The two-MSSP contract is at least as good as the other two contracts on the feasibility dimension

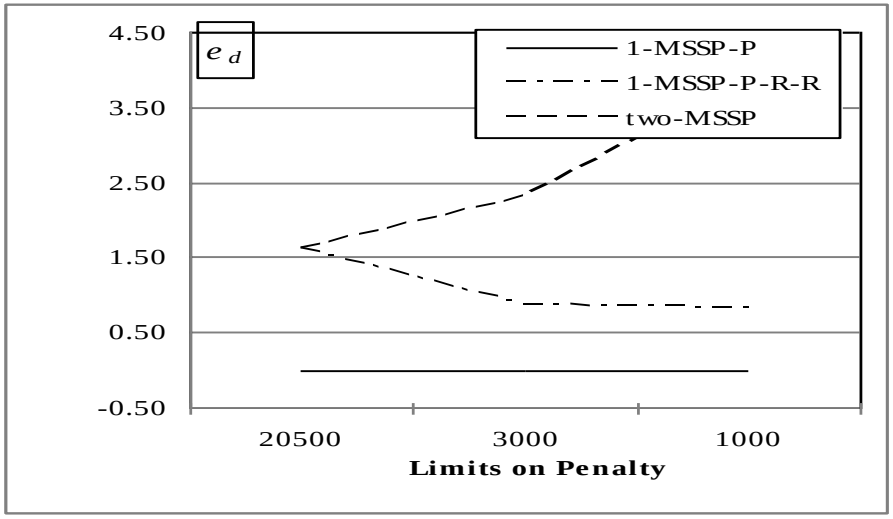
- When the value of detection is very small, none of the contracts is feasible

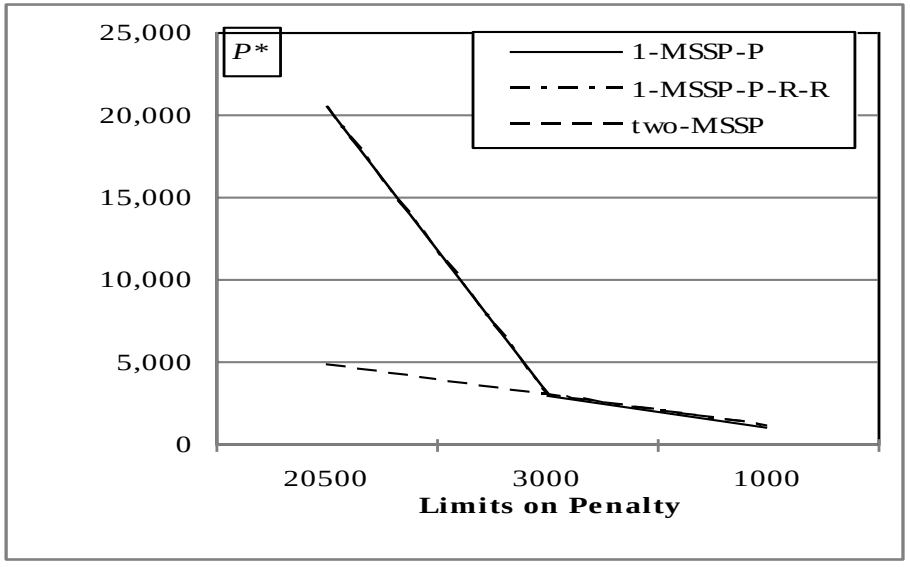
Comparison of Penalty-Based, Penalty-and-Reward-Based, and two-MSSP Contracts

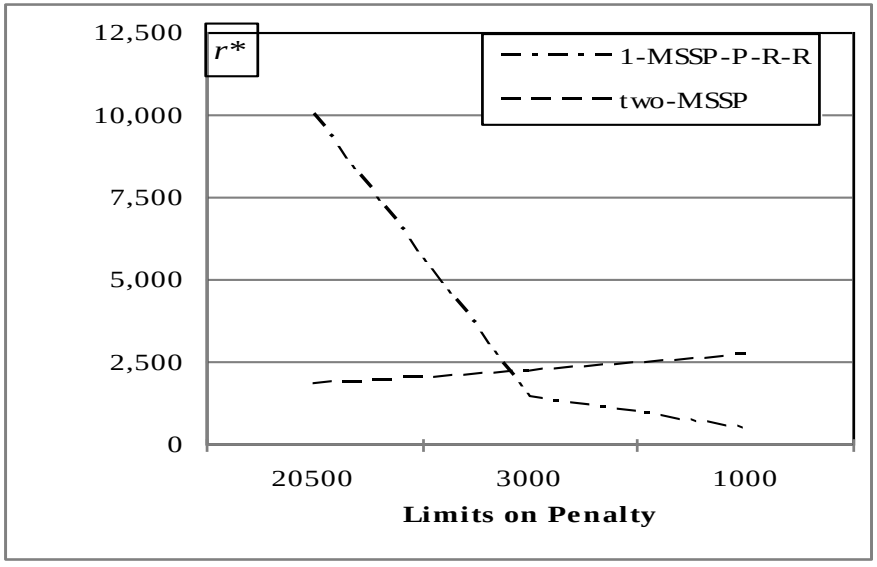
- Efforts and Firm's payoff
  - Penalty-based contract < penalty-and-reward-based contract = two-MSSP contract
- Feasibility
  - Penalty-based contract = penalty-and-reward-based contract < two-MSSP contract
- Penalty and Reward Amounts
  - smaller when the firm uses two MSSPs than when it uses a single MSSP.
- Reward Amount
  - greater than L when it uses a single MSSP
  - less than L when it uses two MSSPs.
- Optimum Penalty and Reward Amounts
  - Two-MSSP contract requires knowledge of private cost parameters
  - The other two contracts do not require such knowledge

Impact of Penalty Limit

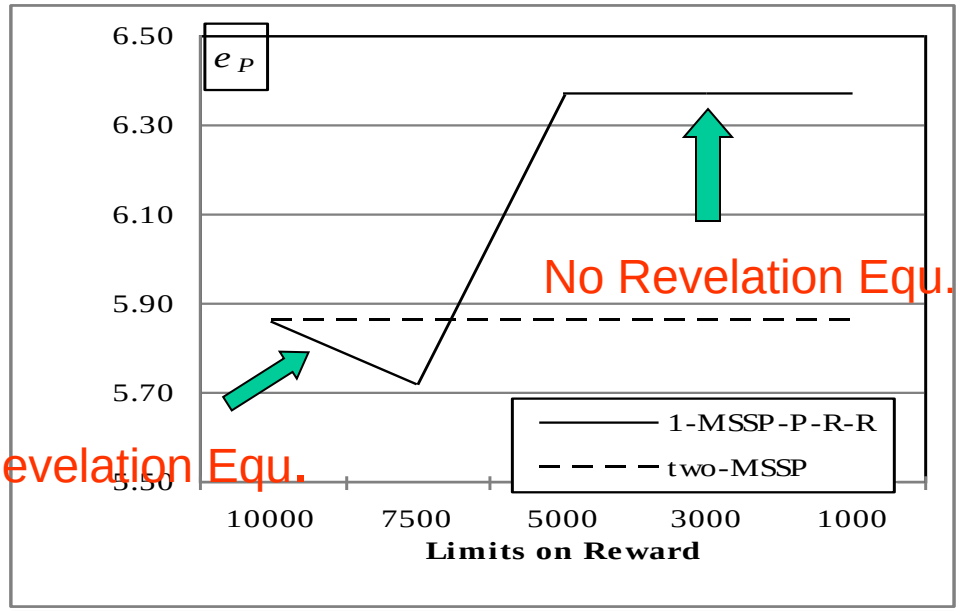


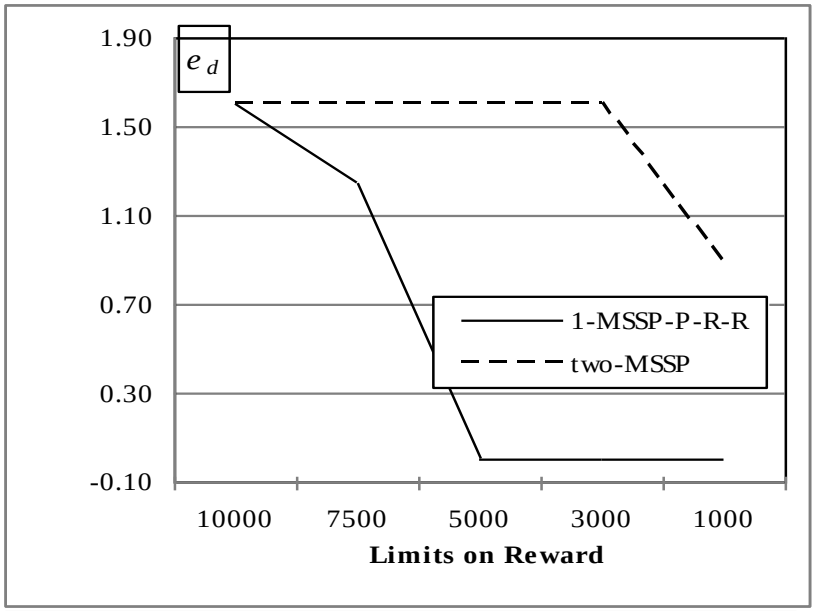


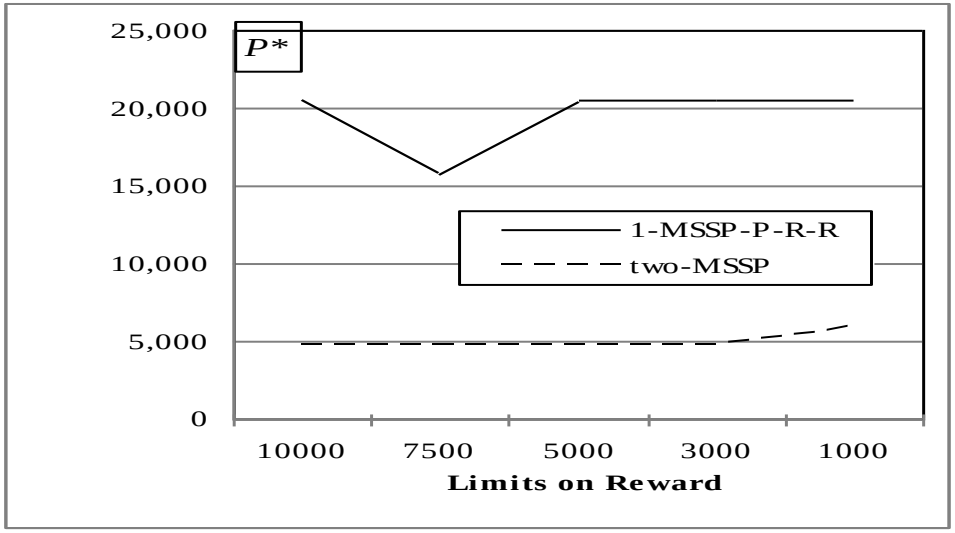


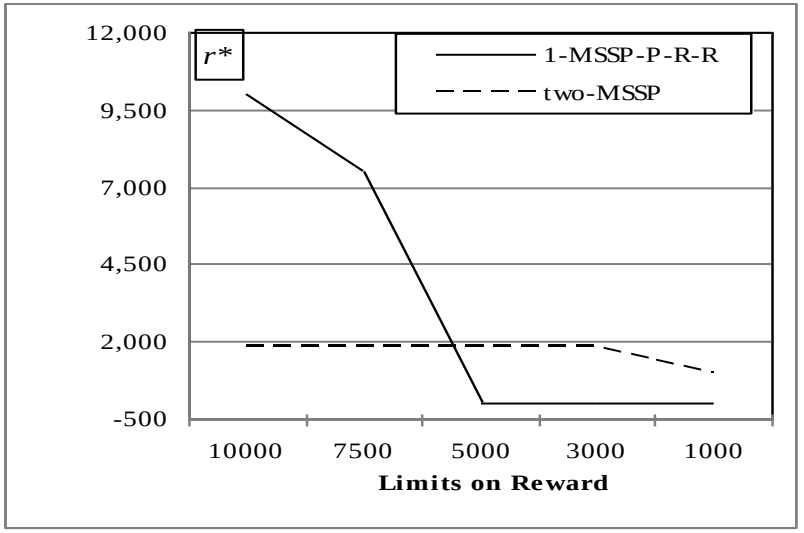


Impact of Reward Limit









Complementarity Between Prevention and Detection Efforts

When both prevention and detection efforts are exerted by the same agent, each decreases the marginal cost of the other.

$$C(e_p, e_d) = C_p(e_p) + C_d(e_d) - \rho C_p(e_p) C_d(e_d), \rho > 0$$

$$\frac{\partial^2 C(e_p, e_d)}{\partial e_d \partial e_p} = -\rho \frac{\partial C_p(e_p)}{\partial e_p} \frac{\partial C_d(e_d)}{\partial e_d} \leq 0$$

Finding:

Complementarity does not affect the optimum penalty and reward amounts in any of the contracts; further, it does not affect the fixed fee in the 2-MSSP and penalty-based contracts. However, the fixed fee decreases in the penalty-and-reward-based contract.

Complementarity between Prevention and Detection Efforts

The firm realizes the maximum payoff when it uses a single MSSP and the penalty-and-reward-based contract. However, the 2-MSSP contract is superior on the feasibility dimension.

An Illustration of the tradeoff between payoff and Feasibility

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

Summary of Findings

- The penalty-based contract creates a conflict of interest between the prevention and detection functions if both are outsourced to the same MSSP, as suggested by some security experts
- However, this need not be the reason to outsource prevention and detection functions to separate MSSPs, contrary to recommendations of security experts
  - The conflict of interest can be eliminated by adding a reward
- But, outsourcing to a single MSSP may suffer from infeasibility if there are limits on the MSSP's liability
- 2-MSSP contract is less likely to suffer from the feasibility problem, without exacerbating the moral hazard issue
- However, it cannot exploit complementarity between the prevention and detection functions, if it exists
- The tradeoff between payoff and feasibility determines the optimum contract for the firm

Thank you!