Journal of Southeast University (English Edition) Vol. 30, No. 1, pp. 113 - 117 Mar. 2014 ISSN 1003—7985

Incentive mechanism analysis of information security outsourcing based on principal-agent model

Xiong Qiang[1,2] Zhong Weijun[1] Mei Shu'e[1]

([1]School of Economics and Management, Southeast University, Nanjing 211189, China)
([2]School of Management, Jiangsu University, Zhenjiang 212013, China)

Abstract: In order to solve principal-agent problems caused by interest inconformity and information asymmetry during information security outsourcing, it is necessary to design a reasonable incentive mechanism to promote client enterprises to complete outsourcing service actively. The incentive mechanism model of information security outsourcing is designed based on the principal-agent theory. Through analyzing the factors such as enterprise information assets value, invasion probability, information security environment, the agent cost coefficient and agency risk preference degree how to impact on the incentive mechanism, conclusions show that an enterprise information assets value and invasion probability have a positive influence on the fixed fee and the compensation coefficient; while information security environment, the agent cost coefficient and agency risk preference degree have a negative influence on the compensation coefficient. Therefore, the principal enterprises should reasonably design the fixed fee and the compensation coefficient to encourage information security outsourcing agency enterprises to the full extent.

Key words: principal agent; information security outsourcing; incentive mechanism

doi: 10.3969/j.issn.1003-7985.2014.01.021

With the rapid development of information technology (IT), the modern enterprises are relying on information technology increasingly and information security is particularly important. The defects in information confidentiality, integrity, availability, traceability have an extraordinary negative impact on the organization. In fact, numerous investments have been made in IT security to ensure the safe operation of the IT systems. But the effect is not significant. The 2011 Global Information Security Survey Report (released by PricewaterhouseCoopers annually) showed that information security incidents among Chinese enterprises were much higher than the global average level. According to this report, incidents related to network, data and system were the three common ones of information security faced by Chinese enterprises; and the occurrence rates were 51%, 45% and 40%, respectively, comparing to the worldwide level of 25%, 27% and 23%. The reason why many enterprises fail in IT security investment is mainly due to the increasingly higher degree of specialization, complexity, technical threshold in IT security technology, the continual emergence of new methods of attack, and the lack of professional enterprise information security management. So information security is increasingly difficult to guarantee, especially for the majority of small and medium-sized enterprises. So for firms who do not possess the know-how to manage their own information security functions, outsourcing the protection to a professional managed security service provider (MSSP) has become an attractive option. There are close to 50% of the enterprises which have outsourced system security to the MSSP in the United States according to "Information Week". The security services that are outsourced range from managing firewalls to implementing security architecture. The MSSP market in North America is expected to hit a revenue of $3.9 billion in 2016[1]. But just some of the large domestic enterprises are trying to outsource in the field of information security.

Why most enterprises are reluctant to outsource information security? The main reason is that the MSSP may not always deliver a high quality of service. The information asymmetry between the principal and the MSSP may cause the MSSP to shirk its duty and provide substandard security quality. User accounts of CardSystems which is expert in payment service was stolen in 2005. It was reported that over 400 thousands of user's credit numbers were leaked out. It was believed afterwards that although CardSystems passed the accreditation of computation and the network service provider Savvis, the latter did not strictly implement the code of certification towards the cardholder information security program (CISP), which reveals the truth that the service quality of the MSSP usually lacks in supervision. The objective of this paper is to design an effective incentive mechanism to ensure the success of information security outsourcing based on the principal-agent theory.

Received 2013-08-26.

Biographies: Xiong Qiang(1979—), male, graduate; Zhong Weijun (corresponding author), male, doctor, professor, zhongweijun@seu.edu.cn.

Foundation items: The National Natural Science Foundation of China (No. 71071033), the Youth Foundation of Humanity and Social Science of Ministry of Education of China (No. 11YJC630234).

Citation: Xiong Qiang, Zhong Weijun, Mei Shu'e. Incentive mechanism analysis of information security outsourcing based on principal-agent model. [J]. Journal of Southeast University (English Edition), 2014, 30(1): 113 - 117. [doi: 10.3969/j.issn.1003-7985.2014.01.021]

1 Related Work

Gordon and Loeb[2] studied information system security investment decision issues from the perspective of safety economics early. After a research on the vulnerability of information assets and potential losses after invasion, they held that it is unnecessary for enterprises to make security investment in information assets with the lowest vulnerability under the given level of potential loss. Instead, enterprises should make investments in information assets with medium vulnerability, and there exists an optimal level for enterprise information security investment. Using the expected utility theory, Huang et al. [3] found that for risk-averse decision makers, security investment increases with, but never exceeds, the potential loss from a security breach while they are making decisions on information security investment, and there exists a minimum potential loss below which the security investment is zero. Thus, enterprises should balance the relationship between security investment and expected secure loss. According to the transaction cost theory, however, enterprises can outsource information security defense to professional enterprises so as to improve security investment efficiency. This has been verified from similar IT outsourcing[4-5], which is the theoretical basis of the model in this paper. Fenn et al. [6] analyzed model selection and relevant risks of information security outsourcing, while Rowe[7] mainly studied the social benefits of information security outsourcing, analyzed whether different outsourcing decisions have an influence on spillover effects and how much influence it has through investigating positive spillover effects of information security outsourcing, and also made policy proposals that can promote information security outsourcing of enterprise level. Hui et al. [8], on the other hand, studied the influence of the relationship between each principal during information security outsourcing on the performance of the overall information security outsourcing from the perspective of agents. However, the success of outsourcing is constantly puzzled by dual moral hazard[9-11] problems during the outsourcing process. Through the research of contract design of information security outsourcing, Ding et al. [12] indicated that the optimal contract should be based on safety performance. This paper uses this viewpoint for reference and builds a model based on the principal-agent theory to research how to set up a reasonable incentive mechanism so as to guarantee the development of an information security outsourcing business, fully considering uncertain factors such as speculation, information security environment and so on during information security outsourcing.

2 Model Design and Analysis

2.1 Model description

The principal-agent theory is used to analyze how the principal promotes the MSSP to select action according to its interests. The question lies in that the principal cannot observe directly the extent of the efforts made by the MSSP in the process of providing security services, but only can observe some variables such as security or defense effects which may not only relate with MSSP's action but also with the exogenous random variable in the external security environment. So actually there is information asymmetry between the principal and the agent. In this setting, the principal needs to design the right incentive mechanism to promote the MSSP to make the greatest efforts to maintain the security of information. Our model encompasses the following assumptions.

Assumption 1 There is one principal and one MSSP. The principal values its information assets at v.

Assumption 2 A hacker attacks the principal's information assets with probability α, $\alpha \in [0, 1]$.

Assumption 3 While the principal outsources information security to the MSSP, the level of security defense is denoted as p, $p \in [0, 1]$, which represents the probability that the principal's system can deter the hacker's attack. It primarily depends on the MSSP's efforts q in the outsourcing service and the external uncertainties in the security environment θ.

$$p = q + \theta$$

where θ is the variable following a normal distribution, $\theta \sim (0, \sigma^2)$, and it is a nature factor measuring the risk uncertainty in the external security environment. The success of outsourcing is closely related to the environment factor. Even if the MSSP works hard, the information security outsourcing can still fail for the risk factor θ.

The MSSP's cost of providing security protection service is an increasing convex function $C(q)$.

$$C(q) = \frac{1}{2}cq^2$$

where c is the cost coefficient.

Assumption 4 The contract between the principal and the MSSP includes a fixed reward b and a compensation term (liability) β, $\beta \in [0, 1]$, which denotes the intensity of the incentive mechanism. If the principal suffers a loss of v because of the hacker's attack, then the MSSP has to compensate the principal by βv. The net reward which the principal pays for information security outsourcing to the MSSP is

$$s = b - \alpha(1 - p)\beta v$$

Assumption 5 If the MSSP slacks off in speculation during the information security outsourcing service, it will benefit. Given the level of slacking off of the MSSP $1 - q$, the principal has the probability $1 - \alpha$ of not being attacked, and the utility of the MSSP is $(1 - q)(1 - \alpha)A$. This utility is inversely proportional to the effort that the

MSSP made and the probability of hackers. A is the utility efficiency of speculation, while $(1-\alpha)A$ is the opportunity income.

Assumption 6 v, c are public information.

During outsourcing, the game consequence between the principal and the MSSP is shown in Fig. 1.

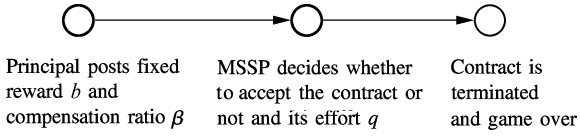

Fig. 1 Game consequence

If the principal outsources its information security defense, its net utility is

$$u_s = [1-\alpha(1-p)]v + \alpha(1-p)\beta v - b \tag{1}$$

The second term in Eq. (1) is the expected compensation receivable by the principal.

The MSSP's profit is

$$u_m = b - \alpha\beta v(1-p) + (1-q)(1-\alpha)A - \frac{1}{2}cq^2 \tag{2}$$

The actual rewards of the principal and the MSSP are random variables which are influenced by the external uncertainties of security environment θ. Now we assume that the principal is risk averse and the MSSP is risk neutral. Then all risk will be undertaken by the MSSP and the principal will not bear any risk.

So the excepted utility of the principal is

$$E(u_s) = [1-\alpha(1-q)]v + \alpha(1-q)\beta v - b \tag{3}$$

The utility of the MSSP will be calculated with the expected utility theory. Assuming that its expected utility function is

$$W_p = -e^{-\rho u_m}$$

where ρ denotes the risk aversion factor of the MSSP, $0 < \rho < 1$.

The MSSP's uncertain expected utility can be equivalent to a certain utility added with risk premium.

$$W_p = E(u_m) - R, R > 0 \tag{4}$$

where R denotes the risk premium. According to the expected utility function and random variable θ which follows normal distribution, the risk premium is

$$R = \frac{1}{2}\rho(\alpha\beta v\sigma)^2 \tag{5}$$

Then substituting Eqs. (2) and (5) into Eq. (4), we can obtain that

$$W_p = b - \alpha\beta v(1-q) - \frac{1}{2}cq^2 + (1-q)(1-\alpha)A - \frac{1}{2}\rho(\alpha\beta v\sigma)^2$$

2.2 Game model analysis

2.2.1 Decision analysis of MSSP

In the incentive mechanism given by the principal enterprise, the MSSP seeks the hard-working level with utility maximization, namely,

$$\max W_p = b - \alpha\beta v(1-q) - \frac{1}{2}cq^2 + (1-q)(1-\alpha)A - \frac{1}{2}\rho(\alpha\beta v\sigma)^2 \tag{6}$$

It can be obtained from the first derivation of Eq. (6) that

$$\frac{\partial E(u_m)}{\partial q} = \alpha\beta v - cq - (1-\alpha)A = 0$$

$$q = \frac{\alpha\beta v - (1-\alpha)A}{c} \tag{7}$$

Since $0 \leqslant q \leqslant 1$, it can be seen from Eq. (5) that, the MSSP chooses the following behavioral strategies according to its expectation for enterprise income after the principal enterprise offers an incentive contract.

1) If $\alpha\beta v < (1-\alpha)A$, then $q^* = 0$.

$\alpha\beta v$ is the expected value of the MSSP for a security incident under complete speculation, because when the compensation of the security incident is less than the opportunity benefit, the incentive mechanism provided by the principal enterprise will hardly work. Besides, the MSSP will completely slack off in speculation and make no effort for information security defense.

2) If $\alpha\beta v > (1-\alpha)A + c$, then $q^* = 1$.

When the compensation limit expected by the MSSP is higher than the sum of the opportunity benefit and the defense cost coefficient, the incentive mechanism provided by the principal enterprise will fully work and the MSSP will make every effort to implement information security defense.

3) If $(1-\alpha)A \leqslant \alpha\beta v \leqslant (1-\alpha)A + c$, then $q^* = (\alpha\beta v - (1-\alpha)A)/c$.

When the compensation proportion expected by the MSSP falls in $\left[\frac{(1-\alpha)A}{\alpha V}, \frac{(1-\alpha)A + c}{\alpha V}\right]$, the incentive mechanism partially works and the MSSP makes part of efforts during the implementation of information security defense.

Therefore, $(1-\alpha)A/(\alpha v)$ is the minimum threshold of the MSSP as compensation standard to the principal enterprise after security incident while $((1-\alpha)A + c)/(\alpha v)$ is the maximum threshold for the compensation standard; i. e., the maximum and minimum thresholds of contract incentive intensity.

2.2.2 Decision analysis of principal enterprise

Based on the principal-agent theory, the principal enterprise will choose the optimal behavioral strategy according to the prospective behavioral strategy of the

agent. The main decision variables of the principal enterprise are fixed fee b and contract incentive intensity β. Suppose that the reservation utility of the MSSP is zero, and the participation constraint of the MSSP is

$$b-\alpha\beta v(1-q)-\frac{1}{2}cq^2+(1-q)(1-\alpha)A-\frac{1}{2}\rho(\alpha\beta v\sigma)^2\geqslant 0$$

1) The MSSP completely slacks and speculates; i.e., $q^*=0$.

The optimization problem of information security outsourced by the principal enterprise is

$$\begin{aligned}&\max_{b,\beta}\{[1-\alpha(1-q)]v+\alpha(1-q)\beta v-b\}\\ &\text{s.t. (IR)}\quad b-\alpha\beta v(1-q)-\frac{1}{2}cq^2+(1-q)(1-\alpha)A-\\ &\qquad\frac{1}{2}\rho(\alpha\beta v\sigma)^2\geqslant 0\\ &\text{(IC)}\quad q=0\end{aligned}$$

Hence, $\beta^*=0, b^*=(1-\alpha)A$.

The optimal solution satisfies $\alpha\beta v<(1-\alpha)A$. At this time, the principal enterprise only offers a fixed fee equivalent to its opportunity benefit. After an information security incident happens, the MSSP will completely speculate when the MSSP need not compensate the principal enterprise.

2) The MSSP makes every effort to offer the outsourcing service; i.e., $q^*=1$.

The optimization problem of information security outsourced by the principal enterprise is

$$\begin{aligned}&\max_{b,\beta}\{[1-\alpha(1-q)]v+\alpha(1-q)\beta v-b\}\\ &\text{s.t. (IR)}\quad b-\alpha\beta v(1-q)-\frac{1}{2}cq^2+(1-q)(1-\alpha)A-\\ &\qquad\frac{1}{2}\rho(\alpha\beta v\sigma)^2\geqslant 0\\ &\text{(IC)}\quad q=1\end{aligned}$$

This optimization problem has no solution. Since natural information asymmetry exists between the MSSP and the principal enterprise. So no matter how severe the punishment given by the principal may be, the MSSP will not spare full effort to complete information security defense to guarantee absolute information security.

3) The MSSP partially slacks and speculates; i.e., $q^*=(\alpha\beta v-(1-\alpha)A)/c$.

$$\begin{aligned}&\max_{b,\beta}\{[1-\alpha(1-q)]v+\alpha(1-q)\beta v-b\}\\ &\text{s.t. (IR)}\quad b-\alpha\beta v(1-q)-\frac{1}{2}cq^2+(1-q)(1-\alpha)A-\\ &\qquad\frac{1}{2}\rho(\alpha\beta v\sigma)^2\geqslant 0\\ &\text{(IC)}\quad q=\frac{\alpha\beta v-(1-\alpha)A}{c}\end{aligned}$$

After solution,

$$\beta^*=\frac{\alpha v}{\alpha v+c\rho\sigma},\ \frac{(1-\alpha)A}{\alpha v}\leqslant\beta^*\leqslant\frac{(1-\alpha)A+c}{\alpha v}$$

$$b^*=\frac{2A(-1+\alpha)B+v^2\alpha^2D}{2c(v\alpha+c\rho\sigma)^2}-\frac{A^2(-1+\alpha)^2}{2c}$$

where

$$B=(-v^3\alpha^3+2c^2v\alpha\rho\sigma+c^3\rho^2\sigma^2+cv^2\alpha^2(1-\rho\sigma))$$
$$D=(-v^2\alpha^2+2c^2\rho\sigma+cv\alpha(2+v\alpha\rho\sigma^2))$$

2.2.3 Model optimal solution analysis

Next, the optimal incentive mechanism for the universal part of slacking will be analyzed.

1) $\frac{\partial\beta^*}{\partial c}<0$ indicates that the optimal compensation coefficient has a reverse relationship with the effort cost coefficient of the MSSP. Under the same effort, the higher the effort cost, the higher the negative utility. Therefore, the MSSP is less and less willing to strive. At this time, the incentive effort under the same incentive intensity will be reduced, so the optimal incentive intensity to the MSSP will also be reduced.

2) $\frac{\partial\beta^*}{\partial\rho}<0$ shows that the optimal incentive intensity has a reverse relationship with the risk aversion coefficient of the MSSP. The higher the risk aversion coefficient, the more scared of the occurrence of a security incident. Therefore, the MSSP will be less willing to take risk and the optimal incentive intensity will be lower.

3) $\frac{\partial\beta^*}{\partial\sigma}<0$ indicates that the optimal incentive intensity has a reverse relationship with the uncertainty of enterprise information security environment. The greater the uncertainty of the information security environment, the higher the probability of a security incident arising from uncertain factors. The environment variable is beyond full control of the MSSP, so the higher the uncertainty is, the less the willingness the MSSP will have to bear the loss of the security incident and the lower the compensation coefficient will be.

4) $\frac{\partial b^*}{\partial v}>0$ and $\frac{\partial\beta^*}{\partial v}>0$ indicate that the higher the information assets value the principal enterprise has, the higher fixed fee the enterprise will be willing to pay so that the MSSP will have enough impetus to guarantee the security of information assets. In the meantime, the principal party requires the MSSP to give a higher compensation coefficient so as to prevent heavy losses of information assets arising from slacking behavior of the MSSP during outsourcing service. The principal enterprise also enables the MSSP to make more effort to guarantee outsourcing service quality by promoting incentive intensity.

5) $\frac{\partial b^*}{\partial\alpha}>0$ and $\frac{\partial\beta^*}{\partial\alpha}>0$ show that the higher the frequency of illegal invasion the principal enterprise faces, the higher fixed fee the principal enterprise will be willing

to pay so that the MSSP will have enough impetus to information security defense and a higher compensation coefficient so as to prevent heavy losses of information assets arising from slacking behavior of the MSSP during outsourcing service.

3 Conclusion

To promote the enterprise information security level, information security outsourcing is an effective way for enterprises to realize information security. There are still principal-agent problems for principal enterprises during information security outsourcing, so they should adopt effective measures to avoid moral risk and opportunistic behavior of information security outsourcing providers. This paper designs an incentive mechanism from a material aspect, which mainly includes fixed income and a compensation mechanism of information security outsourcing. Enterprise information assets value and invasion probability have a positive influence on the fixed fee and the compensation coefficient while information security environment, agent cost coefficient and agency risk preference degree have negative influences on the compensation coefficient. A reasonably designed mechanism can push the MSSP to promote information security outsourcing service level and thus guarantee and promote the information security level of enterprises.

References

[1] Schwartz M J. More firms outsourcing security to MSSPs [EB/OL]. (2010) [2013-08-09]. http://www.informationweek.com/security/management/more-firms-outsourcing-security-to-mssps/225700537.

[2] Gordon L A, Loeb M P. The economics of information security investment[J]. *ACM Transactions on Information and System Security*, 2002, **5**(4): 438 - 457.

[3] Huang C D, Hu Q, Behara R S. An economic analysis of the optimal information security investment in the case of a risk-averse firm[J]. *International Journal of Production Economics*, 2008, **114**(2): 793 - 804.

[4] Willcocks L P, Lacity M C, Kern T. Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA[J]. *The Journal of Strategic Information Systems*, 1999, **8**(3): 285 - 314.

[5] Lee Jae-Nam, Miranda S M, Kim Yong-Mi. IT outsourcing strategies: universalistic, contingency, and configurational explanations of success[J]. *Information Systems Research*, 2004, **15**(2): 110 - 131.

[6] Fenn C, Shooter R, Allan K. IT security outsourcing: how safe is your IT security?[J]. *Computer Law & Security Review*, 2002, **18**(2): 109 - 111.

[7] Rowe B R. Will outsourcing IT security lead to a higher social level of security?[C]//*Workshop on the Economics of Information Security* (*WEIS*). Pittsburgh: Carnegie Mellon University, 2007: 1 - 37.

[8] Hui K, Hui W, Yue W T. Information security outsourcing with system interdependency and mandatory security requirement[J]. *Journal of Management Information Systems*, 2012, **29**(3): 117 - 156.

[9] Koh C, Soon A, Straub D W. IT outsourcing success: a psychological contract perspective[J]. *Information Systems Research*, 2004, **15**(4): 356 - 373.

[10] Reid T, Campbell K. IT outsourcing: success or disaster [J]. *Canadian Underwriter*, 2004, **71**(10): 64 - 66.

[11] Lee C H, Geng X, Raghunathan S. Contracting information security in the presence of double moral hazard[J]. *Information Systems Research*, 2013, **24**(2): 295 - 311.

[12] Ding W, Yurcik W. Outsourcing internet security: the effect of transaction costs on managed service providers [C]//*The International Conference on Telecommunication Systems—Modeling and Analysis*. Dallas, TX, USA, 2005: 17 - 20.

基于委托代理理论的信息安全外包激励机制分析

熊 强[1,2] 仲伟俊[1] 梅姝娥[1]

([1] 东南大学经济管理学院, 南京 211189)

([2] 江苏大学管理学院, 镇江 212013)

摘要:为了解决企业信息安全外包过程中由于利益不一致和信息不对称产生的委托代理问题,需要设计合理的激励机制来促使代理企业积极地完成外包服务. 基于委托代理理论对信息安全外包激励机制进行建模,分析信息资产价值、入侵概率、信息安全环境、代理人成本系数及代理人的风险偏好度等因素对激励机制的影响,得出企业信息资产价值和入侵概率对固定酬金及补偿系数有着正向的影响,而企业的信息安全环境、代理人成本系数以及代理的风险偏好度等因素均对补偿系数呈负向的影响. 委托企业可以据此合理设定外包合约中的固定酬金及补偿系数,以最大限度激励信息安全外包代理企业提升服务水平.

关键词:委托代理;信息安全外包;激励机制

中图分类号:F270