Journal of Southeast University (English Edition) Vol. 33, No. 3, pp. 377 - 381 Sept. 2017 ISSN 1003—7985

Investment strategy analysis of information system security in consideration of attackers

Pan Chongxia Zhong Weijun Mei Shu'e

(School of Economics and Management, Southeast University, Nanjing 211189, China)

Abstract: In order to solve the problem of how a firm makes an optimal choice in developing information systems when faced with the following three modes: development by its own efforts, outsourcing them to a managed security service provider (MSSP) and cooperating with the MSSP, the firm's optimal investment strategies are discussed by modeling and analyzing the maximum expected utility in the above cases under the condition that the firm plays games with an attacker. The results show that the best choice for a firm is determined by the reasonable range of the cooperative development coefficient and applicable conditions. When the cooperative development coefficient is large, it is more rational for the firm to cooperate with the MSSP to develop the information system. When the cooperative development coefficient is small, it is more rational for the firm to develop the information system by its own efforts. It also shows that the attacker's maximum expected utility increases with the increase in the attacker's breach probability and cost coefficient when the cooperative development coefficient is small. On the contrary, it decreases when the cooperative development coefficient is large.

Key words: information security economics; information security investment; investment strategy; game theory

DOI: 10.3969/j.issn.1003 - 7985.2017.03.019

With the rapid development of network finance and e-commerce, the problems of network and information security are becoming more serious. Information security is not regarded as a purely technical problem any longer. However, it is regarded as a more complex system problem incorporating technology, management, economy and so on. At present, information security economics is one of the hot topics and it has attracted much attention. Also, information security investment is one part of information security economics.

Regarding information security investment, Gordon et al.[1] presented an economic model that determined the optimal investment amount. The model took the vulnerability of the information and the potential loss into account should such a breach occur. Cavusoglu et al.[2] introduced the game theory to determine the level of information security investment, system vulnerability, and the returns of investment and they also compared the obtained results with those derived from the decision theory. Utilizing a differential game framework in which hackers disseminated security knowledge within a hacker population over time, Gao et al.[3-4] analyzed dynamic interactions between a firm endeavoring to protect its information assets and a hacker seeking to misappropriate them. In Ref. [5], Gao et al. investigated information sharing and security investments by two firms provided that their information assets were complementary, which meant that their combined information assets were of significant value, whereas the information asset of a single firm is no value to an attacker. Gao et al.[6] discussed information security investment strategies under targeted attacks and mass attacks with considering strategic interactions between two competitive firms and a hacker. Huang et al.[7] analyzed information security investment from the perspective of a risk-averse decision maker. It is found that the maximum security investment increased with the potential loss and the investment in information security did not necessarily increase with the level of risk aversion of the decision maker.

The above mentioned articles are mainly about the development of information systems by the firm's own efforts. But in some cases, for example, a firm's development ability is not enough, so the firm has to outsource the information system security to the managed security service provider (MSSP), which is called information security service outsourcing. There is little literature about information security service outsourcing. Elitzur et al.[8] proposed a new information security service outsourcing contract by analyzing the disadvantages of an incentive mechanism of outsourcing the intrusion detection and protection functions of a MSSP, which can mitigate the problems. Lee[9] discussed the immoral problems in the bilateral contracts and put forward the multilateral contract to optimize investment. Hui et al.[10] analyzed how system interdependency risks interacting with a mandatory security requirement affected the equilibrium behaviors of the MSSP and its clients when organizations completely

Received 2016-10-20.

Biographies: Pan Chongxia (1977—), female, graduate; Zhong Weijun (corresponding author), male, doctor, professor, zhongweijun@seu.edu.cn.

Foundation item: The National Natural Science Foundation of China (No. 71371050).

Citation: Pan Chongxia, Zhong Weijun, Mei Shu'e. Investment strategy analysis of information system security in consideration of attackers [J]. Journal of Southeast University (English Edition), 2017, 33(3): 377 - 381. DOI: 10.3969/j.issn.1003 - 7985.2017.03.019.

outsourced security protection to a managed security service provider (MSSP). The literature showed that a mandatory security requirement will increase the MSSP's efforts and motivate it to serve more clients.

If firms outsource information system security to a MSSP completely, it will be subjected to greater system interdependency risks. Considering the interdependency risks or commercial secrets, some firms are reluctant to outsource. However, firms do not have enough ability to develop information systems by their own efforts and have to cooperate with the MSSP. Meanwhile, firms hope to train their own technicians to improve their ability in the process of cooperation and finally attain the ultimate goal of self-innovation.

The models proposed by Hui et al.[10] showed how such system interdependency risks interacting with a mandatory security requirement affected the equilibrium behaviors of the MSSP and its clients, and the clients had two choices to completely outsource the information system security to the MSSP or not. According to the above models, firms have three choices in this paper: development by the firm's own efforts, outsourcing it to a MSSP or cooperating with a MSSP. By establishing models determining firm's optimal investment strategies, value ranges and conditions are given under which the above three cases are applicable. Also, rational suggestions are given for the firms.

1 Modeling

Suppose that a firm and a MSSP cooperate to develop the information system jointly; that is, a whole information system is developed by both the firm and MSSP. Assuming that the quality of the information system developed by the firm is $q_k(0 \leqslant q_k \leqslant 1)$, the quality of the information system developed by the MSSP is $q_s(0 \leqslant q_s \leqslant 1$ and $q_s > q_k)$ and the information system's security quality is $q = \alpha^2 q_k q_s$ (α^2 can assure $0 \leqslant q \leqslant 1$) when the firm and the MSSP cooperate to develop information system jointly.

In Ref. [10], Hui et al. defined the expected utility function u_k when the firm chooses to develop information systems by its own efforts as follows:

$$u_k = [1 - a(1 - q_k)]v - \frac{1}{2}c_k q_k^2 \tag{1}$$

where v denotes the system value; $a(0 \leqslant a \leqslant 1)$ is the attacker's breach probability; $c_k(c_k \geqslant 0)$ is the firm's cost coefficient; $1/2c_k q_k^2$ is the firm's cost when the system is developed by the firm's own efforts. According to Eq. (1), the optimal security quality of the information system is $q_k^* = av/c_k$ when the firm attains the maximum utility.

Firm's expected utility u_s completely outsourcing to the MSSP is as follows:

$$u_s = [1 - a(1 - q_s)]v + a\beta v(1 - q_s) - p = [1 - a(1 - q_s)]v + a\beta v(1 - q_s) - \left(\frac{1}{2}c_s q_s^2 + \pi_{MSSP}\right) \tag{2}$$

where β denotes the compensation portion received from the MSSP when the system is compromised due to interdependency risks; $1/2c_s q_s^2$ means the cost outsourcing to the MSSP; $p = 1/2c_s q_s^2 + \pi_{MSSP}$ means the cost function outsourcing to the MSSP; and $c_s(c_k > c_s)$ means the cost coefficient outsourcing to the MSSP. According to Eq. (2), Hui et al.[10] gave the solution of the optimal security quality of the information system as $q_s^* = av/c_s$ and $c_k > c_s$ at the maximum utility when the firm outsources the information system security completely to the MSSP and the MSSP obtains profit $\pi_{MSSP}(\pi_{MSSP} \geqslant 0)$. Firm's expected utility u_{ks} when the firm and the MSSP cooperate to develop the information system is as follows:

$$u_{ks} = (1 - a(1 - q))v - p - \frac{1}{2}c_k q_k^2 = (1 - a(1 - \alpha^2 q_k q_s))v - \frac{1}{2}c_s q_s^2 - \pi_{MSSP} - \frac{1}{2}c_k q_k^2$$

Solve $\frac{\partial u_{ks}}{\partial q_k} = av\alpha^2 q_s - c_k q_k$, $\frac{\partial^2 u_{ks}}{\partial q_k^2} = -c_k < 0$, $\frac{\partial u_{ks}}{\partial q_s} = av\alpha^2 q_k - c_s q_s$, $\frac{\partial^2 u_{ks}}{\partial q_s^2} = -c_s < 0$ and set $\frac{\partial u_{ks}}{\partial q_k} = 0$, $\frac{\partial u_{ks}}{\partial q_s} = 0$.

According to the above calculations and analysis, when the firm attains the maximum utility, the cost coefficient relationship of the firm and the MSSP is as follows: $c_k = \frac{(av\alpha^2)^2}{c_s}$ or $c_s = \frac{(av\alpha^2)^2}{c_k}$. The firm's cost coefficient is greater than that of the MSSP, that is, $c_k > c_s$. So, $c_k > \frac{(av\alpha^2)^2}{c_k}$, $\frac{(av\alpha^2)^2}{c_s} > c_s$. It concludes that the value range of firm's cost coefficient and MSSP's is $c_s < av\alpha^2 < c_k$. The optimal security quality of the information system is $q_k^* = \frac{av}{c_k}$ when the firm develops the information system by its own efforts and $q_s^* = \frac{av}{c_s}$ when the firm completely outsource the information system security to the MSSP. So, $c_s = \frac{(av\alpha^2)^2}{c_k} = \frac{av}{c_k} av\alpha^4 = q_k^* av\alpha^4$, $c_k = \frac{(av\alpha^2)^2}{c_s} = \frac{av}{c_s} av\alpha^4 = q_s^* av\alpha^4$. Substituting c_s and c_k into the above equation, we obtain the following firm's expected utility when the firm chooses to cooperate with the MSSP:

$$u_{ks} = (1 - a(1 - q_k q_s))v - \frac{1}{2}c_s q_s^2 - \pi_{MSSP} - \frac{1}{2}c_k q_k^2 = v - av(1 - q_k^* q_s^*)) - \frac{1}{2}q_s^{*2} q_k^* av\alpha^4 - \pi_{MSSP} - \frac{1}{2}q_k^{*2} q_s^* av\alpha^4 \frac{\partial u_{ks}}{\partial q_k} = avq_s^* - \frac{1}{2}q_s^{*2} av\alpha^4 - q_s^* q_k^* av\alpha^4$$

Solve $\frac{\partial^2 u_{ks}}{\partial q_k^2} = -q_s^* av\alpha^4 < 0$, $\frac{\partial u_{ks}}{\partial q_s} = avq_k^* - \frac{1}{2}q_k^{*2}av\alpha^4 - q_s^* q_k^* av\alpha^4$, $\frac{\partial^2 u_{ks}}{\partial q_s^2} = -q_k^* av\alpha^4 < 0$, and set $q_s^* = \frac{2}{3\alpha^4}$, $q_k^* = \frac{1}{3\alpha^4}$. Substituting $c_k = q_s^* av = \frac{2}{3\alpha^4}av$, $c_s = q_k^* av = \frac{1}{3\alpha^4}av$, $q_s^* = \frac{2}{3\alpha^4}$, $q_k^* = \frac{1}{3\alpha^4}$ into the equation of the expected utility of cooperating development, yields

$$u_{ks} = v - av(1 - q_k^* q_s^*) - \frac{1}{2}q_s^{*2}q_k^* av - \pi_{MSSP} - \frac{1}{2}q_k^{*2}q_s^* av = v - \frac{7}{9\alpha^{16}}av - \frac{2}{27\alpha^{64}}av - \frac{1}{27\alpha^{64}}av - \pi_{MSSP} = v - \frac{7}{9\alpha^{16}}av - \frac{1}{27\alpha^{64}}av - \pi_{MSSP} \quad (3)$$

When the firm and the MSSP cooperate to develop the information system, the system security quality is q and the attacker's expected utility is as follows: $u_a = a(1 - q)v - \frac{1}{2}c_h a^2$, where $c_h(c_h \geqslant 0)$ represents the attacker's cost coefficient and $1/2c_h a^2$ represents the attacker's cost function. Substituting $q_s^* = \frac{2}{3\alpha^4}$ and $q_k^* = \frac{1}{3\alpha^4}$ into the following equation: $u_a = av(1 - q_s q_k) - \frac{1}{2}c_h a^2 = av\left(1 - \frac{2}{9\alpha^{16}}\right) - \frac{1}{2}c_h a^2$. We obtain $\frac{\partial u_a}{\partial a} = v\left(1 - \frac{2}{9\alpha^{16}}\right) - c_h a$. Let $\frac{\partial u_2}{\partial a} = 0$ and $a = \frac{v}{c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)$. This leads to the following attacker's maximum expected utility:

$$\max u_a = a(1 - q_s q_k)v - \frac{1}{2}c_h a^2 = av\left(1 - \frac{2}{9\alpha^{16}}\right) - \frac{v^2}{2c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)^2 \quad (4)$$

$\frac{\partial u_a}{\partial a} = v\left(1 - \frac{2}{9\alpha^{16}}\right)$ when $(2/9)^{1/16} < \alpha < 1$, $\frac{\partial u_a}{\partial a} > 0$, when $0 < \alpha \leqslant (2/9)^{1/16}$, $\frac{\partial u_a}{\partial a} \leqslant 0$.

Substituting $q_k^* = \frac{1}{3\alpha^4}$, $q_s^* = \frac{2}{3\alpha^4}$, $c_s = q_k^* av = \frac{1}{3\alpha^4}av$, $c_k = q_s^* av = \frac{2}{3\alpha^4}av$, $a = \frac{v}{c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)$ into Eqs. (1), (2) and (3), we obtain the firm's maximum utility as $\max u_k$ when the firm develops the information system by its own efforts, the firm's maximum utility is $\max u_s$ when the firm outsources it to the MSSP completely and the firm's maximum utility is $\max u_{ks}$ when the firm and the MSSP cooperate to develop the information system jointly.

$$\max u_k = [1 - a(1 - q_k)]v - \frac{1}{2}c_k q_k^2 = v - av(1 - q_k) - \frac{1}{2}c_k q_k^2 = v - \frac{v^2}{c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)\left(1 - \frac{1}{3\alpha^4} + \frac{1}{27\alpha^{64}}\right)$$

$$\max u_{ks} = v - av(1 - q_k^* q_s^*)) - \frac{1}{2}q_s^{*2}q_k^* av - \pi_{MSSP} - \frac{1}{2}q_k^{*2}q_s^* av = v - \frac{v^2}{c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)^2 - \frac{v^2}{9\alpha^{20}c_h}\left(1 - \frac{2}{9\alpha^{16}}\right) - \pi_{MSSP}$$

$$\max u_s = [1 - a(1 - q_s)]v + a\beta v(1 - q_s) - \left(\frac{1}{2}c_s q_s^2 + \pi_{MSSP}\right) = v - \frac{v^2}{c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)\left(1 - \frac{2}{3\alpha^4}\right)(1 - \beta) - \frac{2v^2}{27\alpha^{20}c_h}\left(1 - \frac{2}{9\alpha^{16}}\right) - \pi_{MSSP}$$

2 Analysis

According to the above calculations, the firm's maximum utility is as follows when the firm develops the information system by its own efforts:

$$\max u_k = v - \frac{v^2}{c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)\left(1 - \frac{1}{3\alpha^4} + \frac{1}{27\alpha^{64}}\right)$$

The firm's maximum utility of outsourcing to the MSSP completely is as follows:

$$\max u_s = v - \frac{v^2}{c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)\left(1 - \frac{2}{3\alpha^4}\right)(1 - \beta) - \frac{2v^2}{27\alpha^{20}c_h}\left(1 - \frac{2}{9\alpha^{16}}\right) - \pi_{MSSP}$$

The firm's maximum utility when the firm and the MSSP cooperate to develop the information system jointly is as follows:

$$\max u_{ks} = v - \frac{v^2}{c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)^2 - \frac{v^2}{9\alpha^{20}c_h}\left(1 - \frac{2}{9\alpha^{16}}\right) - \pi_{MSSP}$$

The attacker's maximum expected utility is

$$\max u_a = av\left(1 - \frac{2}{9\alpha^{16}}\right) - \frac{v^2}{2c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)^2$$

Comparing the following results of $\max u_{ks}$, $\max u_s$, $\max u_k$, $\max u_{ks} - \max u_s$ with each other and according to Ref. [10], we obtain the following conclusions.

Proposition 1 When the firm cooperates with the MSSP to develop the information system, the firm's maximum expected utility is $\max u_{ks} = v - \frac{v^2}{c_h}\left(1 - \frac{2}{9\alpha^{16}}\right)^2 - \frac{v^2}{9\alpha^{20}c_h}\left(1 - \frac{2}{9\alpha^{16}}\right) - \pi_{MSSP}$ at the firm's maximum security quality of the information system with $q_s^* = \frac{av}{c_s}$. The MSSP's maximum security quality of the information system $q_s^* = \frac{av}{c_s}$, the firm's cost and the MSSP's cost are c_k and $c_s(c_k > c_s)$ respectively, and their cooperative effi-

ciency coefficient range is $(2/9)^{1/16} < \alpha < 1$. The comparison result of the three patterns of the maximum expected utility is $\max u_{ks} > \max u_s > \max u_k$ without considering compensation; that is, the firm's cooperative maximum expected utility is greater than the utility under the conditions that the firm outsources to the MSSP or the firm develops by its own efforts. In this case, it is reasonable for the firm to cooperate with the MSSP to develop the information system when the compensation is small.

Proposition 2 When the cooperative efficiency coefficient is $\alpha = (2/9)^{1/16}$ or $\alpha = 0.641\ 28$ or $\alpha = 0.889\ 2$. The comparison result of the three cases is $\max u_{ks} = \max u_s = \max u_k$; that is, the firm's cooperative maximum expected utility is equal to the maximum expected utility outsourcing to the MSSP and equal to the maximum expected utility when the firm develops by its own efforts. In this case, three choices are all applicable to the firm.

Proposition 3 When the cooperative efficiency coefficient value range is $0 < \alpha < (2/9)^{1/16}$, the comparison result of the three cases is $\max u_{ks} < \max u_k < \max u_s$; that is, the firm's cooperative maximum expected utility is less than the maximum expected utility when the firm develops by its own efforts and less than the maximum expected utility outsourcing to the MSSP. In this case, it is rational to outsource to the MSSP when the MSSP's profit is not so large.

Proposition 4 The maximum expected utility of the attacker is $\max u_a$ which increases with the increase in the attacker's breach probability and the attacker's cost coefficient when the cooperative efficiency coefficient value range is $0 < \alpha < (2/9)^{1/16}$, while it decreases with the decrease in the attacker's breach probability and attacker's cost coefficient when the cooperative efficiency coefficient value range is $(2/9)^{1/16} < \alpha < 1$. The attacker's maximum expected utility changes with the value of the information system and the attacker's cost coefficient.

3 Conclusion

How does a firm make optimal choices in developing information systems under certain conditions when faced with the following three modes: development by its own efforts, outsourcing them to a MSSP or cooperating with the MSSP? This paper gives the firm's optimal investment strategies by modeling and analyzing the maximum expected utility in the above three cases and takes into account the condition that the firm plays games with an attacker simultaneously. When the cooperative efficiency is within a reasonable range, and the firm and the MSSP obtain the optimal security quality of the information system, the firm can attain the maximum expected utility. In some cases, the best choice for firms is to outsource to the MSSP or to develop by its own efforts. In the game between the firm and attacker, the attacker's maximum expected utility increases with the increase in the breach probability and the attacker's cost coefficient, while it decreases in some other cases. The maximum expected utility of the attacker changes with the information system value and cooperative efficiency coefficient.

The security investment regarding multiple firms and MSSPs will become more complex and it will draw different conclusions. Also, dynamic games between multiple firms and attackers need to be discussed in future research.

References

[1] 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. DOI: 10.1145/581271.581274.

[2] Cavusoglu H, Raghunathan S, Yue W T. Decision-theoretic and game-theoretic approaches to it security investment[J]. *Journal of Management Information Systems*, 2008, **25**(2): 281 − 304. DOI: 10.2753/MIS0742-1222250211.

[3] Gao X, Zhong W J, Mei S E. Information security investment when hackers disseminate knowledge[J]. *Decision Analysis*, 2013, **10**(4): 352 − 368. DOI: 10.1287/deca.2013.0278.

[4] Gao X, Zhong W J, Mei S E. A differential game approach to information security investment under hackers' knowledge dissemination[J]. *Operations Research Letters*, 2013, **41**(5): 421 − 425. DOI: 10.1016/j.orl.2013.05.002.

[5] Gao X, Zhong W J, Mei S E. A game-theoretic analysis of information sharing and security investment for complementary firms[J]. *Journal of the Operational Research Society*, 2014, **65**(11): 1682 − 1691. DOI: 10.1057/jors.2013.133.

[6] Gao X, Zhong W J. Information security investment for competitive firms with hacker behavior and security requirements[J]. *Annals of Operations Research*, 2015, **235**(1): 277 − 300. DOI: 10.1007/s10479-015-1925-2.

[7] Huang C D, Hu Q, Behara R S. An economic analysis of the optimal information security investment in the case of a risk-averse firms[J]. *International Journal of Production Economics*, 2008, **114**(2): 793 − 804. DOI: 10.1016/j.ijpe.2008.04.002.

[8] Elitzur R, Gavious A, Wensley A K P. Information systems outsourcing projects as a double moral hazard problem[J]. *Omega*, 2012, **40**(3): 379 − 389. DOI: 10.1016/j.omega.2011.06.005.

[9] 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. DOI: 10.1287/isre.1120.0447.

[10] Hui K L, 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. DOI: 10.1287/isre.1120.0447.

考虑黑客攻击下的信息系统安全投资策略分析

潘崇霞　仲伟俊　梅姝娥

（东南大学经济管理学院，南京 211189）

摘要：为解决企业面对自主研发、把信息安全完全外包给安全服务外包提供商 MSSP 和企业与 MSSP 合作共同开发 3 种模式下如何作出最优选择问题，在考虑企业与黑客博弈的情况下，通过对企业期望效用的建模与分析对企业在 3 种情况下的最优安全投资策略进行了讨论. 结论表明，企业的最优选择取决于合作开发系数的取值范围及其适用条件. 当合作开发系数较高时，企业与 MSSP 合作开发更为理性；当合作开发系数较低时，企业选择自主研发更为理性. 当企业与 MSSP 的合作开发系数较小时，黑客的最大期望效用随着入侵概率与成本系数的增大而增大，而在当企业与 MSSP 的合作开发系数较大时则相反.

关键词：信息安全经济学；信息安全投资；投资策略；博弈论

中图分类号：TP309