Technology Analysis & Strategic Management

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ctas20

Decision making of optimal investment in information security for complementary enterprises based on game theory

Xiaotong Li

To cite this article: Xiaotong Li (2020): Decision making of optimal investment in information security for complementary enterprises based on game theory, Technology Analysis & Strategic Management, DOI: 10.1080/09537325.2020.1841158

To link to this article: https://doi.org/10.1080/09537325.2020.1841158

TECHNOLOGY ANALYSIS & STRATEGIC MANAGEMENT
https://doi.org/10.1080/09537325.2020.1841158

Decision making of optimal investment in information security for complementary enterprises based on game theory

Xiaotong Li[a,b]

[a]School of Economics and Management, Xi'an University of Posts and Telecommunications, Xi'an, People's Republic of China; [b]Xi'an University of Posts and Telecommunication, Western Institution for Digital Economy, Xi'an, People's Republic of China

ABSTRACT

With the development of information technology and the deepening of enterprise informatization, there are new challenges of enterprise information security investment decisions because of cooperative relationships among multi-enterprises. In this paper, the Gordon-Loeb model is extended to the multi-enterprise game environment, and combined with the probability of hacker invasion, which can stimulate enterprises to increase investment in information security and reduce costs, the game model of information security investment among complementary enterprises is constructed. Through this model, the impact of factors on optimal investment can be analyzed. It is found that the information security level of enterprises in cooperation situation is higher than that in the non-cooperation situation. Our research shows that the optimal investment will increase with the increase of the probability of one spread in cooperative situations, which is contrary to the changing trend of enterprises in non-cooperation situations, and there is a minimum expected cost threshold. According to the results, enterprise compensation mechanism and information sharing mechanism are designed to ensure the optimal level of social information security, it provides a new solution to deal with the information security investment decision of complementary enterprises under the characteristics of multi-enterprise and non-cooperative.

ARTICLE HISTORY
Received 16 March 2020
Revised 5 September 2020
Accepted 20 October 2020

KEYWORDS
Information security investment; decision making; economic incentive mechanisms; complementary enterprises

1. Introduction

With the continuous development of information and communication technology, the extensive application of e-commerce and the deepening of enterprise informatization, new information security issues are gradually emerging(Ahmad, Maynard, and Park 2014). At present, information security in the world is facing extremely severe challenges. Information security has not only affected the interests of individual enterprises or industries, but also affected social stability and national security, resulting in an increasingly urgent need for information security defense(Lowry, Dinev, and Willison 2017). In order to solve information security problems, enterprises will invest more in information security, but previous studies have shown that the greater the investment in information security, the more advanced the use of information security technology, the final result is not necessarily the best (Cavusoglu, Mishra, and Raghunathan 2005; Dor and Elovici 2016; Feng, Wang, and Li

CONTACT Xiaotong Li xtli@xupt.edu.cn School of Economics and Management, Xi'an University of Posts and Telecommunications, Xi'an, 710061, People's Republic of China; Western Institution for Digital Economy, Xi'an, 710121, People's Republic of China

2014; Qian et al. 2017). At the same time, the advanced information technology can contact the associated enterprises and integrate supply chain, such as the Continuous Replenishment Program (CRP), Electronic Data Interchange (EDI) and Vendor Managed Inventory (VMI), this technology can let enterprises to form close connections and information sharing with their upstream and downstream enterprises and even with their competitors, that is, the security of an enterprise information system can directly affect another enterprise (Gao, Zhong, and Mei 2015; Jeong, Lee, and Lim 2019). For example, on February 24, 2017, the 'Sunshine Integrity Alliance' was formally established at the initiative of JD.com, together with 14 well-known enterprises such as Tencent, Baidu, Wal-Mart China, Procter & Gamble, and the Criminal Law Science Research Center of Renmin University of China. The alliance aims to build a Great Wall of security for anti-corruption, anti-fraud and information security crime and create a commercial environment of safe consumption. It indicates that the occurrence of information security incidents among enterprises is correlated, and existing enterprises have reached cooperation on information security.

Due to the network connection, software system similarity, business contacts, and enterprise information assets, there may be some complementary relationships between enterprises' information assets (Chen, Kataria, and Krishnan 2011). Between complementary companies, hackers need to gain value by breaking into one company and then successfully breaking into another (Liu, Ji, and Mookerjee 2012). Due to the relation of information assets between complementary enterprises, if only one enterprise is invaded, the complementarity of information assets ensures that the hacker will not gain any gains and the enterprise will not suffer losses. The following two examples can better illustrate the complementarity of enterprise information assets (Gao, Zhong, and Mei 2014; Liu, Ji, and Mookerjee 2012): (a). When customer information overlaps between two enterprises, one enterprise stores customer names and id Numbers in its information system, and another enterprise stores customer names, addresses, and phone numbers in its information system. Only when the information systems of both companies are successfully invaded can the hacker fraudulently apply for a new credit card. (b). The large commercial aircraft manufacturing industry is a supply chain system formed by main manufacturers, sub-system suppliers and component suppliers. Major manufacturers may outsource the work of designing major components for new products to other companies, such as mitsubishi heavy industries, kawasaki heavy industries and Fuji heavy industries, which helped design the body parts for the Boeing 767 and 777, hackers who want to gain access to the overall design of the new aircraft will have to gain access to all the companies' design information. This characteristic of information assets greatly affects the motivation of hackers, thus affecting the information security investment decisions of enterprises.

In terms of information security investment decision-making among complementary enterprises, there have been relevant studies on two information security investment decision-making problems of complementary enterprises under the circumstance of information sharing (Gao, Zhong, and Mei 2014; Wu et al. 2017). The existing scholarship in this field, however, stays short of considering the effects of the quantity of multi-enterprise and the relationship of cooperative, they will affect the investment level of enterprise information security in reality. Therefore, it is of great practical significance to make a theoretical study on the optimal investment level of multi-enterprise with complementary information assets in non-cooperation situation and to make a comparative analysis with cooperation situation. The quantity of multi-enterprise and the relationship of cooperative make information security investment decision among complementary enterprises face new challenges. In this paper, the Gordon-Loeb model is extended to the multi-enterprise game environment, and combined with the probability of hacker invasion, which can stimulate enterprises to increase investment in information security and reduce costs, the game model of information security investment among complementary enterprises is constructed. Through this model, the impact of enterprise quantity, probability of one spread and probability of hacker invasion on optimal investment can be analyzed in the case of non-cooperation and cooperation situations. The previous researches seldom consider the problem of enterprise information security investment under the complementary of information assets, and this paper enriches the theory of enterprise information

security investment decision. Also, It provides a new solution to deal with the information security investment decision of complementary enterprises under the characteristics of multi-enterprise and cooperative relationships.

In this paper, a literature review is presented in Section two. The proposed model is constructed in Section three. The results of the enterprises' information security investment decision in the case of non-cooperation and cooperation are analyzed in Section four and Section five. The enterprise compensation mechanism and information sharing mechanism are designed in Section six. Finally, managerial implications and conclusions are presented in Section seven and Section eight.

2. Related literature

This section reviews the enterprise information security investment issues from the perspective of risk management and security cost–benefit. Next, it reviews the decision-making issues of information security investment among related enterprises, and finally analyzes the contributions and shortcomings of existing achievements.

On the investment analysis of enterprise information security risk management, Wang and Song proposed an investment strategy using multi-objective model, the model uses opportunity cost to transform the risk of information, measures the efficiency of security-related tools and policies by influencing factors, and then obtains a number of alternative optimal investment strategies (Wang and Song 2008). Huang et al. analyzed the investment in information security from the perspective of a risk-averse decision-maker (Huang, Hu, and Behara 2008). Yong et al. proposed the profit optimisation model of information security investment based on value-at-risk and operational risk model of financial economics (Yong, Kauffman, and Sougstad 2011). Li et al. proposed a software process model with risk management and cost control modules to help improve software risk management (Li et al. 2012). On the cost–benefit aspect of security, Gordon and Loeb proposed an economic model to optimise enterprise investment in information security, it is found that for a given potential loss, the enterprise does not always need to invest it in the information assets with the greatest security risk (Gordon and Loeb 2002), and this model has been empirically tested by actual data from e-local governments in Japan (Tanaka, Matsuura, and Sudoh 2005). Anderson and Choobineh analyzed the optimal strategy of enterprise information security investment with investment budget constraints (Anderson and Choobineh 2008). Shirtz and Elovici propose a new framework for optimising investment decisions, this framework assumes that companies can come up with remedies that address established security issues (Shirtz and Elovici 2011). Bojanc et al. proposed an optimal investment evaluation and decision model of security technology based on quantitative analysis of information security risk and digital asset evaluation in enterprises (Bojanc, Jerman-Blažič, and Tekavčič 2012). Dor and Elovici propose a conceptual model based on the grounded theory, this model reflects the latest decision-making practices for information security investment in several industry organisations (Dor and Elovici 2016). Existing research points out that the greater the investment in information security, the more advanced the use of information security technology, the final effect is not necessarily the best, enterprises need to balance the relationship between security, cost and benefit to maximise the benefits of the whole system. The system vulnerability of enterprises is related to the investment efficiency, investment amount and the allocation of information systems. These research results provide a realistic background and basis for the research of enterprise information security investment decisions.

As for the information security investment decision among related enterprises, Hausken studied the information sharing and information security strategies of related enterprises, he analyzes the extent of information sharing, and how does each firm make a trade-off between information sharing and security investments (Hausken 2007). However, the findings of this paper have been altered in studies by Gao et al., they explored how to determine the security investment and information sharing of the two companies through the security default probability function (Gao, Zhong, and Mei 2015). Bandyopadhyay studied the information security investment strategy of two

enterprises, considered the network propagation and analyzed the optimal investment strategy (Bandyopadhyay, Jacob, and Raghunathan 2010). Liu et al. analyzed the relationship between information security investment and information sharing between two affiliated enterprises and found that complementary enterprises have a natural motivation for information sharing and do not need an external influence to induce sharing (Liu, Ji, and Mookerjee 2012). Gao et al. studied the security investment and information sharing of complementary enterprises based on game theory and analyzed the optimal choice of enterprises and hackers (Gao, Zhong, and Mei 2014). Using differential game theory, Gao and Zhong explore alternative dynamic strategies for security investment and information sharing under target attack. Based on this, both enterprises can influence the value of their information assets through internal pricing mechanism (Gao and Zhong 2016). Based on evolutionary game-theoretic approach, Zhu et al. studied the sustainability of investment security investment in online social networks (Zhu, Liu, and Feng 2019). Ezhei and Ladani analyzed the effects of interdependency in security investment of firms against strategic attackers, they proposed a differential game among the networked firms in which attackers act strategically (Ezhei and Ladani 2020).

The existing research provides the research background, research basis and research method for enterprise information security investment decision-making problem extraction, and points out the theoretical and practical significance of enterprise information security investment decision-making research. However, Due to the new enterprise information security problems, it is more necessary to systematically consider the influence of inter-enterprise relationship on enterprise group information security investment decisions. Previous studies focused on single or two enterprises, and did not consider the influence of network propagation on complementary enterprise information security investment strategy. In addition, because the hacker behaviour can directly affect the enterprise information security technology level and enterprise information security behaviour, thus it will affect the enterprise information security investment decision, but current researches generally assume that the probability of hacking by hackers is a fixed value, while the probability of hacking by hackers can stimulate enterprises to increase input in information security and reduce costs to some extent, so it is necessary to consider the probability of hacking by hackers as a variable and study its influence on the investment decision of enterprise information security. Therefore, how to carry out theoretical research on the optimal investment level of multi-enterprise with complementary information assets in non-cooperation situation, and compare with the optimal investment results in cooperation situation, so as to put forward effective incentive mechanism is a new challenge faced by information security investment decision-making among complementary enterprises.

3. The model

3.1. Notation

In this section, we consider information security investment decisions between two or more complementary enterprises in non-cooperative and cooperative situations. The variables and parameters involved are as shown below.

- n the number of enterprises in the complementary enterprise group
- L the loss suffered by a single enterprise after the information system of the enterprise group is successfully invaded by hackers
- q probability of one spread between complementary enterprises
- p_i the probability of firm i being directly attacked by hackers, $i(i = 1, 2, \ldots, n)$
- δ the probability of hacking by hackers
- v the probability of successful direct invasion by hackers without information security investment
- x_i the information security investment of firm i, $i(i = 1, 2, \ldots, n)$
- β enterprise information security investment efficiency
- C_i the expected cost of firm i, $i(i = 1, 2, \ldots, n)$

3.2. Model description

According to previous studies (Gordon and Loeb 2002; Qian et al., 2017; Wu et al. 2015), the probability of enterprise information system being directly and successfully invaded by hackers is related to three parameters, therefore, the probability of the enterprise being successfully invaded by hackers can be expressed as $p(\delta, v, x)$. Where $\delta(0 < \delta < 1)$ is the probability of hacker invasion. If the enterprise's information security investment is confidential to hackers, then the enterprise's information security investment will not affect the probability of hacker invasion. $v(0 < v < 1)$ is the probability of direct successful invasion by hackers when the enterprise has no information security investment, which is mainly determined by the configuration of the information system (Huang, Hu, and Behara 2008). x is the information security investment. This paper extends the model of Gordon and Loeb (Gordon and Loeb 2002) to express the probability function of enterprise information system being directly and successfully invaded by hackers as $p_i = p(x_i) = \delta v^{\beta x_i + 1}$, where β is the information security investment efficiency of the enterprise.

In the complementary enterprise group, the two connecting enterprises may be directly or indirectly attacked by hackers. Direct attack refers to the successful hacker attack caused by the vulnerability of the enterprise's information system. Indirect attack refers to the fact that the hacker first successfully intruded into the complementary enterprises of the enterprise, because of the network's ability to exploit trusted links between complementary companies, the probability that other enterprises are successfully invaded by hackers due to inter-enterprise correlation is q.

The spread path of hacker attacks between complementary enterprises is shown in Figure 1. The hacker first successfully penetrated firm 1, while firm 2 was indirectly attacked due to its connection with firm 1, while firm 3 was successfully attacked due to its internal connection with firm 2. It can be seen from the figure that firm 1 was directly attacked, firm 2 was indirectly breached due to primary network transmission, firm 3 was successfully invaded due to secondary network transmission, and firm n was successfully invaded due to the $n-1$ spread. In a complementary situation, a hacker who successfully intrudes into one enterprise also needs to successfully intrude into other enterprises in the enterprise group to obtain value. If only one company is hacked, the complementarity of information assets ensures that the hacker will gain no value and the company will not lose.

Assuming that each enterprise in the complementary enterprise group is homogeneous, when the enterprise group information system is successfully invaded by hackers, the loss of each enterprise is L. Assuming that there is no prior information about the vulnerability of enterprises, it is reasonable to assume that the probability of each enterprise being attacked is equal. Then the probability of firm 1 being successfully invaded by hackers is

$$P_1 = 1 - (1 - p_1) \prod_{n=2}^{N} (1 - q^{n-1} p_n) \tag{1}$$

Where p_1 is the probability that firm 1 is successfully attacked directly by hackers, $q^{n-1}p_n$ is the probability that firm 1 is successfully attacked indirectly by hackers, and $(1 - p_1) \prod_{n=2}^{N} (1 - q^{n-1}p_n)$ is the probability that enterprise 1 is not successfully invaded by hackers.

Assuming that all enterprises are risk-neutral, the information security investment of firm $i(i = 1, 2, \ldots, n)$ is x_i and the initial investment is 0. The larger the enterprise information security investment, the higher the enterprise information security level.

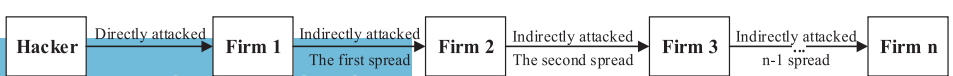

Figure 1. The spread path of hacker attacks.

4. Enterprise information security investment decision in the case of non-cooperation

This section analyzes the equilibrium strategy of a single enterprise in the case of non-cooperation in the complementary enterprise group, The probability of the firm $i(i = 1, 2, \ldots, n)$ being successfully invaded by hackers is $1 - (1 - p_i)\prod_{n=2}^{N}(1 - q^{n-1}p_n)$, and the objective of the enterprise is to minimise its expected cost, so the objective function of the firm i is

$$Min\ C_i = [1 - (1 - p_i)\prod_{n=2}^{N}(1 - q^{n-1}p_n)]L + x_i \tag{2}$$

According to formula (2), it can be obtained

$$\frac{\partial C_i}{\partial x_i} = \delta\beta L v^{\beta x_i + 1} \ln v \prod_{n=2}^{N}(1 - q^{n-1}p_n) + 1 \tag{3}$$

$$\frac{\partial^2 C_i}{\partial x_i^2} = \delta\beta^2 L v^{\beta x_i + 1} (\ln v)^2 \prod_{n=2}^{N}(1 - q^{n-1}p_n) \tag{4}$$

According to formula (4), $\frac{\partial^2 C_i}{\partial x_i^2} > 0$, the optimal information security investment of each enterprise can be obtained by lemma 4.1.

Lemma 4.1: *When the enterprises in the complementary enterprise group are not cooperative, the optimal investment of each enterprise is x^*, and the Nash equilibrium solution of each enterprise is $(x^*, x^*, \ldots, x^*)$, where x^* satisfies $x^* = \frac{-\ln(-\delta v \beta L \ln v \prod_{n=2}^{N}(1 - q^{n-1}p_n(x^*)))}{\beta \ln v}$.*

Based on the optimal security investment and Nash equilibrium solution given above, the influence of enterprise size, probability of primary spread between complementary enterprises and probability of direct invasion of hackers on the optimal security investment can be analyzed. Due to the security investment of each enterprise in the complementary enterprise group is equal, the probability of each enterprise being directly invaded by hackers is equal. It can be seen by lemma 4.1 that x^* should satisfy $\delta\beta L v^{\beta x_i + 1} \ln v \prod_{n=2}^{N}(1 - q^{n-1}p_n(x_i)) + 1 = 0$. Because $\frac{\prod_{n=2}^{N}(1 - q^n p_{n+1})}{\prod_{n=2}^{N}(1 - q^{n-1}p_n)} = 1 - q^n p_{n+1} < 1$, then $\prod_{n=2}^{N}(1 - q^{n-1}p_n)$ will decrease as the number of enterprises increases. For firm i, in order to satisfy $\delta\beta L v^{\beta x_i + 1} \ln v \prod_{n=2}^{N}(1 - q^{n-1}p_n(x_i)) + 1 = 0$, the value of $p(x_i) = \delta v^{\beta x_i + 1}$ needs to increase so that enterprises in the complementary enterprise group will reduce their information security investment. Thus, theorem 4.1 can be obtained.

Theorem *4.1:* *If the number of enterprises in the complementary enterprise group is n, in the case of non-cooperation, the optimal information security investment x^* is negatively correlated with the number of enterprises n.*

Theorem 4.1 shows that with the increase of the number of enterprises in the complementary enterprise group, the optimal investment of each enterprise will decrease, which will increase the probability of hacker's successful invasion and reduce the information security level of the enterprise group. Although the increase in the number of enterprises can make enterprises share risks, it is easy to reduce the level of enterprise information security. When the number of enterprises is greater

than a certain critical value, enterprises do not need to make an investment. Therefore, enterprises should balance the advantages and disadvantages brought by new entrants. For example, among the outsources of the Boeing Company, there are more airframe parts manufacturers but fewer engine manufacturers. In the outsourcing activities with other manufacturers, the Boeing Company could reduce the number of companies by simultaneously manufacturing certain airframe parts or outsourcing core parts.

As $\prod_{n=2}^{N}(1-q^{n-1}p_n)$ will decrease with the increase of the probability of one spread between complementary enterprises. For firm i, in order to satisfy $\delta\beta L v^{\beta x_i+1}\ln v\prod_{n=2}^{N}(1-q^{n-1}p_n(x_i))+1=0$, the value of $p(x_i)=\delta v^{\beta x_i+1}$ needs to increase, then each enterprise in the complementary enterprise group will reduce its information security investment. Thus, theorem 4.2 can be obtained.

Theorem 4.2: *For the probability of one spread $q \in (0, 1)$ between any enterprise, if each enterprise in the complementary enterprise group is not cooperative, the optimal information security investment x^* monotonically decreasing*.

Theorem 4.2 shows that with the increase of the probability of the first spread between complementary enterprises, its optimal information security investment will decrease. Bandyopadhyay et al. (Bandyopadhyay, Jacob, and Raghunathan 2010) proposed two complementary enterprise information security investment game models and found that network dissemination has a negative impact on the optimal investment strategy of enterprises. That means the increase of the probability of one spread between complementary enterprises will reduce the enterprise's information security investment motivation. So, in the case of non-cooperation, complementary enterprises can adjust the network structure of the enterprise group and reduce the connection with other enterprises. For example, if the information security investment of the Boeing Company and other enterprises is not cooperative, its industrial chain structure can be adjusted to the mode of secondary and tertiary contractors, so as to adjust the network connection.

Due to the increase of the number of enterprises or the probability of one spread between enterprises will increase the probability of successful invasion by hackers, however, the analysis shows that enterprises will not increase the investment in information security, but reduce the amount of investment, which further worsens the information security environment of enterprises, the reason for this phenomenon is the 'free-riding' behaviour among enterprises. Enterprise information security investment is not only beneficial to its own information system security but also beneficial to the security of other enterprise information systems. The increase of enterprise information security investment will cause the marginal benefit of its security investment to decrease. The marginal benefit of enterprise information security investment will decrease with the increase in the number of enterprises or the probability of one spread, as a result, enterprises will reduce their investment in information security. By analysing the influence of hacker invasion probability on the optimal investment of enterprises in the case of non-cooperation, theorem 4.3 can be obtained.

Theorem 4.3: *For any probability of hacker invasion $\delta \in (0, 1)$, if the enterprises in the complementary enterprise group are not cooperative, the optimal information security investment x^* among enterprises increases monotonically, that is* $\frac{dx}{d\delta} > 0$.

Theorem 4.3 shows that in the complementary enterprise group game model, the information security investment of each enterprise will increase with the probability of hacker's direct invasion. This is a counterintuitive conclusion, as the probability of hacker invasion increases, enterprises will face more risks and greater losses, but in fact, the increase of the probability of hacker invasion will stimulate enterprises to increase investment, and then improve the level of information security of enterprises. Next, the information security investment level and the influence of each parameter on the optimal investment can be analyzed under the condition of cooperation.

5. Enterprise information security investment decision in the case of cooperation

This section analyzes the optimal information security investment strategy of complementary enterprises in the case of cooperation. Minimising the expected cost of all enterprises is the goal of the enterprise group, so the objective function of the enterprise group is

$$Min\ C = [1 - (1 - p)\prod_{n=2}^{N}(1 - q^{n-1}p_n)]L + nx \tag{5}$$

According to formula (5), it can be obtained

$$\frac{\partial C}{\partial x} = \delta\beta L v^{\beta x+1} \ln v \prod_{n=2}^{N}(1 - q^{n-1}p_n) + n \tag{6}$$

$$\frac{\partial^2 C}{\partial x^2} = \delta\beta^2 L v^{\beta x_i+1} (\ln v)^2 \prod_{n=2}^{N}(1 - q^{n-1}p_n) \tag{7}$$

According to formula (7), $\frac{\partial^2 C_i}{\partial x_i^2} > 0$. For the optimal information security investment of enterprises, when formula (6) is 0, that is $\delta\beta L v^{\beta x+1} \ln v \prod_{n=2}^{N}(1 - q^{n-1}p_n) + n = 0$, lemma 5.1 can be obtained.

Lemma 5.1: *When all the enterprises in the complementary enterprise group cooperate completely, the optimal information security investment is* $x^{*'}$, *where* $x^{*'}$ *satisfies* $x^{*'} = \frac{\ln\frac{n}{v} - \ln(-\delta v\beta L \ln v \prod_{n=2}^{N}(1 - q^{n-1}p_n(x^{*'})))}{\beta \ln v}$.

By comparing x^* and $x^{*'}$, obviously, in the case of cooperation, the optimal investment of each complementary enterprise group is higher than that of non-cooperation, so the information security level of enterprises in cooperation is higher than that of enterprises in non-cooperation. By comparing the expected costs of enterprises in the case of cooperation with those in the case of non-cooperation, theorem 5.1 can be obtained.

Theorem 5.1: *When the enterprise loses* $L > \frac{-1}{p' \prod_{n=2}^{N}(1 - q^{n-1}p_n)}$, $\frac{\partial C_i}{\partial x_i} < 0$, *and the investment of the enterprise in the case of full cooperation* $x^{*'}$ *is greater than that in the case of non-cooperation* x^*, *then the expected cost of the enterprise in cooperation* $C_i(x^{*'})$ *is less than that in the case of non-cooperation* $C_i(x^{*'})$.

Theorem 5.1 shows that when the loss of an enterprise is greater than a certain threshold, the investment of the enterprise in the case of cooperation is higher than that in the case of non-cooperation, and the expected cost is lower than that in the case of non-cooperation. In other words, under the condition of cooperation, enterprises can improve their information security level and reduce their expected cost. When the enterprise is in cooperation, there is a minimum expected cost threshold. When it is lower than this threshold, it is not necessary for the enterprise to make an investment. When it is higher than this threshold, the expected cost of the enterprise will increase with the increase of the enterprise investment. Therefore, not all risks are worthy of investment. If the expected cost of the enterprise is very small, the enterprise should bear a certain risk, so it is not necessary to make an investment. When the expected cost of an enterprise is very high and the enterprise is faced with a disastrous consequence, the optimal investment of the enterprise will reach a stable level. In this case, with the increase of the expected cost, the optimal investment of the enterprise will not increase significantly, the best solution for enterprises is not to overinvest, but to adopt other methods to transfer risks, such as information security outsourcing or purchase of commercial insurance. Based on the above optimal security investment of

complementary enterprises in the case of cooperation, the influence of each parameter on the optimal security investment can be analyzed, and theorem 5.2 can be obtained.

Theorem 5.2: *Complementary enterprise group in full cooperation, the optimal information security investment* $x^{*'}$ *is negatively correlated with the number of enterprises n, that is,* $\frac{dx}{dn} < 0$.

According to theorem 4.1 and theorem 5.2, each enterprise in the complementary enterprise group, whether in the case of non-cooperation or cooperation, although increasing the number of enterprises can bring more shared information to the group, its optimal information security investment decreases with the increase of the number of enterprises, which will increase the probability of hacker's successful invasion and reduce the information security level of the group of enterprises. Therefore, no matter in the case of non-cooperation or cooperation, the enterprise group should balance the advantages and disadvantages of the new entrants. As for the influence of the probability of one spread on the optimal security investment, theorem 5.3 can be obtained.

Theorem 5.3: *For the probability of one spread* $q \in (0, 1)$ *between any enterprise, in the case of cooperation, the optimal information security investment* $x^{*'}$ *is positively correlated with the probability of one spread q, that is,* $\frac{dx}{dq} > 0$.

Theorem 5.3 proves that under the condition of cooperation, the optimal investment will increase with the increase of the probability of one spread between enterprises, which is contrary to the changing trend of enterprises under the condition of non-cooperation. The increase in the probability of one spread between enterprises will lead to the information system of the enterprise group is more likely to be successfully invaded by hackers. In the case of non-cooperation, enterprises do not care whether their information system will 'infect' other enterprises if it is successfully invaded by hackers. As a result, it has a negative impact on enterprise strategy. The reason for this phenomenon is that there may be free-riding behaviour among complementary enterprises.

Therefore, when each enterprise in the complementary enterprise group makes independent decisions, enterprises only consider their own interests and do not consider that when hackers invade other enterprises through the probability of spread between enterprises, they will cause losses to the whole. If the enterprise group makes the collaborative decision, its goal is to minimise the overall expected cost, which encourages the enterprise to reduce the expected loss of the enterprise group by increasing information security investment. It can be seen that the optimal investment in cooperation between enterprises can increase the level of information security and reduce the overall expected cost. Therefore, in order to promote the cooperation between enterprises, it is necessary to design enterprise compensation mechanism and information sharing mechanism.

6. Design of incentive mechanism

6.1. Enterprise compensation mechanism

Due to the optimal security investment of each enterprise in the complementary enterprise group in the non-cooperative case is less than the optimal security investment in the cooperative case, and the expected cost in the non-cooperative case is higher than the expected cost in the full cooperative case. Therefore, a social planner is needed to take the place of enterprises to make joint decisions, through the design of enterprise compensation mechanism to encourage enterprises to increase their investment in information security in order to reach the optimal level.

It is assumed that the enterprise can detect the hacker's intrusion and identify whether it is direct or indirect. If the enterprise is caused by the indirect intrusion of hackers, then the connected enterprise should pay some compensation to the enterprise. It is assumed that the enterprise indirectly

invaded by hackers can obtain λL from the enterprise connected with it, where λ is the compensation coefficient.

When firm j is successful indirect invaded by hackers just because of firm i, firm i needs to compensate firm j. Under this mechanism, the objective function of the firm i is

$$Min\ C_B = x + [1 - (1 - p_i)\prod_{n=2}^{N}(1 - q^{n-1}p_n)]L + \sum_{j=1,j\neq i}^{n} p_i q(1 - p_j)\lambda L - \sum_{j=1,j\neq i}^{n} p_j q(1 - p_i)\lambda L \quad (8)$$

In formula (5), the first item is the information security investment of firm i, the second item is the expected cost of firm i, the third item is the compensation that firm i needs to be paid to other enterprises when they are successfully invaded due to indirect intrusion of firm i, the fourth item is the compensation that firm i received from other enterprises when firm i is successfully invaded due to indirect invasion of other enterprises. After simplifying (8), it can be obtained

$$Min\ C_B = x + [1 - (1 - p_i)\prod_{n=2}^{N}(1 - q^{n-1}p_n)]L + \sum_{j=1,j\neq i}^{n}(p_i - p_j)q\lambda L \quad (9)$$

According to formula (9), $\frac{\partial^2 C_B}{\partial x^2} > 0$, So when x_B^* satisfies $\frac{\partial C_B}{\partial x} = 0$, that is, when x_B^* satisfies $1 + \delta\beta L v^{\beta x+1}\ln v\prod_{n=2}^{N}(1 - q^{n-1}p_n) + n\delta\beta\lambda L v^{\beta x+1}\ln v = 0$, the optimal investment of each enterprise in the complementary enterprise group can be obtained. By comparing the optimal investment of the enterprise with the non-cooperative situation, we can get $x_B^* > x_i^*$, that is, the optimal investment in the enterprise compensation mechanism is higher than the investment in the case of non-cooperation. Therefore, the level of enterprise information security under the enterprise compensation mechanism is higher than that under the non-cooperative situation. Next, the expected cost under the enterprise compensation mechanism and the non-cooperative condition are compared. Since each enterprise in the complementary enterprise is homogeneous, the expected cost of the enterprise under the enterprise compensation mechanism can be expressed as $Min\ C_B = x + [1 - (1 - p_i)\prod_{n=2}^{N}(1 - q^{n-1}p_n)]L$. When L satisfies $L > \frac{-1}{\delta\beta v^{\beta x+1}\ln v\prod_{n=2}^{N}(1 - q^{n-1}p_n)}$, $\frac{\partial C_B}{\partial x} < 0$, then $C_B(x_B^*) < C_i(x_i^*)$, that is, the expected cost under the enterprise compensation mechanism is less than the expected cost under the non-cooperative situation. Thus theorem 6.1.1 can be obtained.

Theorem 6.1.1: *When the loss of enterprise* $L > \frac{-1}{\delta\beta v^{\beta x+1}\ln v\prod_{n=2}^{N}(1 - q^{n-1}p_n)}$, *if firm i is directly invaded by hackers, and firm j is indirectly invaded by hackers due to firm i, the firm i needs to pay* λL *to firm j. Under the enterprise compensation mechanism, the optimal investment of the enterprise* x_B^* *is greater than the investment* x_i^* *in the case of non-cooperation, and the expected cost* $C_B(x_B^*)$ *is less than the expected cost* $C_i(x_i^*)$ *in the case of non-cooperation.*

Therefore, under the enterprise compensation mechanism, enterprises can not only improve the information security level of complementary enterprise groups but also reduce their expected costs, which is an effective economic incentive measure. Then the relationship between the optimal investment amount and the compensation coefficient under the enterprise compensation mechanism can be inferred. Due to $\frac{dx_B}{d\lambda} = -\frac{n\delta\beta v^{\beta x+1}\ln v}{\delta\beta^2 L v^{\beta x+1}(\ln v)^2\prod_{n=2}^{N}(1 - q^{n-1}p_n) + n\delta\beta^2\lambda L v^{\beta x+1}(\ln v)^2} > 0$, so the

optimal investment increases with the increase of compensation coefficient. It can also be concluded that when $\lambda < -\frac{1+\delta\beta Lv^{\beta x+1}\ln v\prod_{n=2}^{N}(1-q^{n-1}p_n)}{n\delta\beta Lv^{\beta x+1}\ln v}$, enterprise investment is insufficient, when $\lambda > -\frac{1+\delta\beta Lv^{\beta x+1}\ln v\prod_{n=2}^{N}(1-q^{n-1}p_n)}{n\delta\beta Lv^{\beta x+1}\ln v}$, the enterprise will overinvest. Therefore, under the enterprise compensation mechanism, when $\lambda = -\frac{1+\delta\beta Lv^{\beta x+1}\ln v\prod_{n=2}^{N}(1-q^{n-1}p_n)}{n\delta\beta Lv^{\beta x+1}\ln v}$, the underinvestment and overinvestment can be avoided. The compensation mechanism of enterprises shows that the enterprises responsible for the indirect breach of other enterprises should compensate the enterprise that is breached indirectly, which is reasonable and increases the enthusiasm of enterprises for security investment.

6.2. Information sharing mechanism

In order to promote the sharing of security information among enterprises, the US government has established a number of agencies, such as the National Internet Emergency Center (CONCERT), United States Secret Service Electronic Crime Working Group and so on. At the same time, industry-based Information Sharing and Analysis Center (ISAC) has been established, including information technology, supply chain, aviation, financial services, public transportation, etc. Information Technology-Information Sharing and Analysis Centre (IT-ISAC) promotes Information Sharing about cybersecurity threats and vulnerabilities. The centre provides a neutral forum for members to share and learn non-public details about threats and vulnerabilities with their counterparts at other member companies. When enterprises share security information through such organisations, they can analyze and classify the information, quickly disseminate physical and cyber threat alerts, and recommend security solutions to member enterprises to protect their information systems as soon as possible. This section discusses the benefits of information sharing and deeply studies the investment decisions of complementary enterprises under the information sharing mechanism.

Assuming that enterprises do not consider the risk of information leakage when sharing information security, an enterprise can get security information from other enterprises, then other enterprises of information security investment will be shared with the enterprise. In other words, firm *i* will receive $\theta\sum_{n=2}^{N}x_n$ investment from other enterprises, where θ represents the information sharing rate between firm *i* and other enterprises. Under the information sharing mechanism, the objective function of firm *i* is

$$Min\ C_s = [1-(1-p_i(x_i+\theta\sum_{n=2}^{N}x_n))\prod_{n=2}^{N}(1-q^{n-1}p_n(x_i+\theta\sum_{n=2}^{N}x_n))]L+x_i \tag{10}$$

According to formula (10), the optimal information security investment of the enterprise under the information sharing mechanism can be obtained as $x_S^* = \frac{\theta\ln\frac{n}{v}-\ln(-\delta v\beta L\ln v\prod_{n=2}^{N}(1-q^{n-1}p_n))}{\beta\ln v}$.

By comparing with the optimal investment in the case of non-cooperation, it can be obtained that $x_S^* > x^*$, then the optimal investment in the information sharing mechanism is greater than the non-cooperation situation. Therefore, the information security level of enterprises under the information sharing mechanism is higher than that under the non-cooperative condition. Next, the expected costs of enterprises under the information sharing mechanism and the non-cooperative condition

are compared. When L satisfies $L > \frac{-1}{p' \prod_{n=2}^{N}(1-q^{n-1}p_n)}$, $\frac{\partial C_S}{\partial x} < 0$, then $C_S(x_S^*) < C_S(x_i^*)$, that is, the expected cost under the enterprise information sharing mechanism is less than the non-cooperative situation. Then, under the enterprise information sharing mechanism, the enterprise can not only improve the information security level of the complementary enterprise group but also reduce its expected cost. Thus, theorem 6.2.1 can be obtained.

Theorem 6.2.1: *Under the enterprise information sharing mechanism, when the enterprise loses* $L > \frac{-1}{p' \prod_{n=2}^{N}(1-q^{n-1}p_n)}$, *the optimal investment* x_S^* *is greater than the investment* x^* *in the case of non-cooperation, and the expected cost* $C_S(x_S^*)$ *is less than the expected cost* $C_S(x_i^*)$ *in the case of non-cooperation.*

According to theorem 6.2.1, when the loss of an enterprise by hackers is greater than a certain threshold, under the information sharing mechanism, the enterprise can not only improve the information security level of the complementary enterprise group but also reduce its expected cost, which is an effective economic incentive measure. According to this, the relationship between the optimal investment amount and the probability of one spread can be inferred, and theorem 6.2.2 can be obtained.

Theorem 6.2.2: *When the information sharing efficiency* $\theta > -\beta \ln v \prod_{n=2}^{N}(1-q^{n-1}p_n)$, *the optimal investment* x_S^* *of complementary enterprises is positively correlated with the probability of one spread* q *between enterprises, that is,* $\frac{dx_S}{dq} > 0$.

Theorem 6.2.2 shows that when the information sharing efficiency is greater than a certain effective value, the optimal investment of complementary enterprises will increase with the increase of the probability of one spread between enterprises. In other words, when the efficiency of information sharing is greater than a certain effective value, the probability of one spread between enterprises plays a positive role in the information security investment decision of enterprises, which can ensure the effectiveness of the information sharing mechanism. When $\theta > -\beta \ln v \prod_{n=2}^{N}(1-q^{n-1}p_n)$, $\frac{dx}{d\theta} = -\frac{1-\delta v^{\beta x+1}}{\beta^2 \delta v^{\beta x+1}(\ln v)^2 \prod_{n=2}^{N}(1-q^{n-1}p_n) + \beta\delta\theta v^{\beta x+1}\ln v} > 0$, from this, theorem 6.2.3 can be obtained.

Theorem 6.2.3: *Under the information sharing mechanism, when the information sharing efficiency* $\theta > -\beta \ln v \prod_{n=2}^{N}(1-q^{n-1}p_n)$, *the optimal investment* x_S^* *of complementary enterprises is positively correlated with the enterprise information sharing efficiency* θ, *that is* $\frac{dx}{d\theta} > 0$.

Under the information sharing mechanism, when $\theta = 0$, $x_S^* = x^*$; when $\theta = 1$, $x_S^* = x^{*'}$. That is, when the efficiency of information sharing is 0, the optimal investment amount of enterprise information security is equal to the investment amount of enterprise decision-making alone; when the efficiency of information sharing is 1, the optimal investment of enterprise information security reaches the socially optimal investment level. Therefore, the information sharing mechanism is an effective economic incentive mechanism.

7. Managerial implications

This paper considers the influence of the enterprises' quantity, the probability of one spread and the probability of hacker invasion on the investment decision of enterprise information security, and studies the information security investment decision of complementary enterprises. By comparing the investment level and expected cost of information security in non-cooperative and cooperative situations, there are two effective economic incentive mechanisms are proposed. The following management implications can be obtained from the research results.

(1) Complementary enterprise groups should strengthen cooperation in information security to improve the level of information security.

Firstly, the investment level of each enterprise does not reach the optimal level of society, and each enterprise underinvests in security in the non-cooperative situation; the information security level of each enterprise in cooperation situation is higher than that in non-cooperation situation, and its expected cost is lower than that in non-cooperation situation. Secondly, when an enterprise is in cooperation, the optimal investment will increase with the increase of the probability of one spread, which is contrary to the changing trend of enterprises in non-cooperation. As a result, it has a negative impact on corporate strategy. The reason for this phenomenon is that there may be free-riding behaviour between complementary enterprises. When the enterprise is in cooperation, its goal is to minimise the overall expected cost, which encourages the enterprise to increase the investment in information security to reduce the expected loss. Thus, the optimal investment in cooperation situation can increase the level of information security and reduce the overall expected cost.

(2) Complementary enterprise groups should control the number of enterprises internally to reduce information security risks.

Although increasing the number of enterprises can bring more shared information to the group, its optimal investment in information security decreases with the increase of the number of enterprises whether in the non-cooperative cases or in cooperation cases, this will increase the probability of hacker invasion and reduce the information security level.

(3) Complementary enterprise groups should take appropriate risks to avoid overinvestment.

When the enterprise is in cooperation, there is a minimum expected cost threshold. When it is lower than this threshold, the enterprise does not need to invest. When it is higher than this threshold, the expected cost of the enterprise will increase with the increase of the enterprise investment. When the expected cost of the enterprise is too high that the enterprise is faced with a disastrous consequence, the optimal investment of the enterprise will reach a stable level. At this point, the optimal investment of the enterprise will not increase significantly as the expected cost increases, then the best solution for enterprises is not to overinvest, but to adopt other methods to transfer risks, such as information security outsourcing or commercial insurance.

(4) The government and relevant departments should establish an enterprise compensation mechanism and information sharing mechanism to promote the cooperation of enterprises.

From the perspective of social planners, this paper puts forward the compensation mechanism and information sharing mechanism to promote the cooperation of enterprises. These two mechanisms can improve the information security level of enterprise groups and reduce the expected cost, which are effective economic incentive measures. Through modelling analysis, it is necessary to set an

appropriate compensation coefficient to ensure the effectiveness of the enterprise compensation mechanism. If the compensation coefficient is less than a certain threshold, it will lead to insufficient investment; if the compensation coefficient is greater than a certain threshold, it will lead to excessive investment.

8. Conclusion

With the development of information technology and the deepening of enterprise informatization, enterprises are facing more and more threats in information security. Information security problems gradually evolve from isolated and individual enterprise problems to security problems with public characteristics, the multi-enterprise and ways of cooperation make information security investment decision among complementary enterprises face new challenges. This paper studies the information security investment decision-making problem between enterprises with complementary information assets in non-cooperation and cooperation situation. This study makes significant contributions to the current scholarly literature. Firstly, it points out the significance of enterprise information security investment decision research in theory and practice. Secondly. it provides the new solution for the multi-enterprise information security investment decision. The existing research indicates that the more investment enterprises make in information security, the better the result will be, however, the enterprise's system vulnerability is related to the number of enterprise, the enterprise's investment efficiency, investment amount and the configuration of information system. These research results provide the realistic background and basis for the enterprise information security investment decision research.

In the research on information security investment decision of complementary enterprises, only the negative impact brought by the increase of the number of enterprises is considered, but in fact, the new enterprise can bring new knowledge to the existing enterprise and have a positive impact on the existing enterprise, so this factor can be taken into account in the future. In addition, different types of hackers have different attack frequency, consequences, and necessary defensive measures. In the future, we can further study the investment problem of enterprise information security under different attack modes of hackers, analyze the optimal investment strategy of enterprises and propose an effective incentive mechanism.

Acknowledgment

We thank the editor and reviewers for helpful comments.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research has been supported by the Doctoral Scientific Research Start-up Foundation from Xi'an University of Posts and Telecommunications Program (Program No. 105/205020015) and Scientific Research Program Funded by Shaanxi Provincial Education Department(Program No. 20JK0361).

Notes on contributor

Xiaotong Li was born in China in 1988. She received the M.S. degree from Northwest Agriculture and Forestry University in 2014 and the Ph.D. degree from Xidian University in 2019. She is currently a lecturer with the College of Economics and Management, Xi'an University of Posts and Telecommunications. Research interests grey systems theory, fuzzy theory, game theory, information security investment, and sharing.

Reference

Ahmad, A., S. B. Maynard, and S. Park. 2014. "Information Security Strategies: Towards an Organizational Multi-Strategy Perspective." *Journal of Intelligent Manufacturing* 25: 357–370.

Anderson, E. E., and J. Choobineh. 2008. "Enterprise Information Security Strategies." *Computers & Security* 27: 22–29.

Bandyopadhyay, T., V. Jacob, and S. Raghunathan. 2010. "Information Security in Networked Supply Chains: Impact of Network Vulnerability and Supply Chain Integration on Incentives to Invest" *Information Technology and Management* 11 (1): 7–23.

Bojanc, R., B. Jerman-Blažič, and M. Tekavčič. 2012. "Managing the Investment in Information Security Technology by use of a Quantitative Modeling." *Information Processing & Management* 48: 1031–1052.

Cavusoglu, H., B. Mishra, and S. Raghunathan. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture." *Information Systems Research* 16: 28–46.

Chen P. Y., G. Kataria, and R. Krishnan. 2011. "Correlated Failures, Diversification, and Information Security Risk Management." *MIS Quarterly* 35 (2): 397–422.

Dor, D., and Y. Elovici. 2016. "A Model of the Information Security Investment Decision-Making Process." *Computers & Security* 63: 1–13.

Ezhei, M., and B. T. Ladani. 2020. "Interdependency Analysis in Security Investment Against Strategic Attacks." *Information System Frontiers* 22: 187–201.

Feng, N., H. J. Wang, M. Q. Li. 2014. "A Security Risk Analysis Model for Information Systems: Causal Relationships of Risk Factors and Vulnerability Propagation Analysis." *Information Sciences* 256: 57–73.

Gao, X., and W. J. Zhong. 2016. "A Differential Game Approach to Security Investment and Information Sharing in a Competitive Environment." *IIE Transactions* 48: 511–526.

Gao, X., W. Zhong, and S. Mei. 2014. "A Game-Theoretic Analysis of Information Sharing and Security Investment for Complementary Firms." *Journal of the Operational Research Society* 65: 1682–1691.

Gao, X., W. Zhong, and S. Mei. 2015. "Security Investment and Information Sharing Under an Alternative Security Breach Probability Function." *Information Systems Frontiers* 17: 423–438.

Gordon, L. A., and M. P. Loeb. 2002. "The Economics of Information Security Investment." *Acm Transactions on Information & System Security* 5: 438–457.

Hausken, K. 2007. "Information Sharing among Firms and Cyber Attacks." *Journal of Accounting & Public Policy* 26: 639–688.

Huang, C. D., Q. Hu, and R. S. Behara. 2008. "An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-Averse Firm." *International Journal of Production Economics* 114: 793–804.

Jeong, C. Y., S. Y. T. Lee, and J. H. Lim. 2019. "Information Security Breaches and IT Security Investments: Impacts on Competitors." *Information & Management* 56: 681–695.

Li, J., M. Li, D. Wu, and H. Song. 2012. "An Integrated Risk Measurement and Optimization Model for Trustworthy Software Process Management." *Information Sciences* 191: 47–60.

Liu, D., Y. Ji, and V. Mookerjee. 2012. "Knowledge Sharing and Investment Decisions in Information Security." *Decision Support Systems* 52: 95–107.

Lowry, P. B., T. Dinev, and R. Willison. 2017. "Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda." *European Journal of Information Systems* 26: 546–563.

Qian, X. F., X. B. Liu, J. Pei, P. M. Pardalos, and L. Liu. 2017. "A Game-Theoretic Analysis of Information Security Investment for Multiple Firms in a Network." *Journal of the Operational Research Society* 68: 1290–1305.

Shirtz, D., and Y. Elovici. 2011. "Optimizing Investment Decisions In Selecting Information Security Remedies." *Information Management & Computer Security* 19: 95–112.

Tanaka, H., K. Matsuura, and O. Sudoh. 2005. "Vulnerability and Information Security Investment: An Empirical Analysis of e-Local Government in Japan." *Journal of Accounting and Public Policy* 24: 37–59.

Wang Z., and H. Song. 2008 "Towards an Optimal Information Security Investment Strategy." 2008 IEEE International Conference on Networking, Sensing and Control, Sanya, 756–761.

Wu, Y., G. Feng, N. Wang, and H. Liang. 2015. "Game of Information Security Investment: Impact of Attack Types and Network Vulnerability." *Expert Systems with Applications* 42: 6132–6146.

Wu, Y., R. Y. Fung, G. Feng, and N. Wang. 2017. "Decisions Making in Information Security Outsourcing: Impact of Complementary and Substitutable Firms." *Computers & Industrial Engineering*, 1–f12.

Yong, J. L., R. J. Kauffman, and R. Sougstad. 2011. "Profit-Maximizing Firm Investments in Customer Information Security." *Decision Support Systems* 51: 904–920.

Zhu, G., H. Liu, and M. N. Feng. 2019. "Sustainability of Information Security Investment in Online Social Networks: An Evolutionary Game-Theoretic Approach." *Mathematics* 6: 177.