Incentive Mechanism Design Based on Repeated Game Theory in Security Information Sharing

XIONG Qiang, CHEN Xiaoyan
School of management, Jiangsu University, Zhenjiang 212013, China

***Abstract*—In addition to the security investment, security information sharing among firms has been proved to be an effective measure. In order to enhance the level of information security and improve the social welfare, this paper studies how to promote sharing through a certain reasonable incentive mechanism. We adopt the repeated game theory to establish incentive mechanism and analyze how similarity, isolation period, discount factor, proportion of rational firms and so on effect the efficiency of this incentive mechanism. We finally conclude the conditions required by the effective mechanism.**

Keywords-Security Information; Repeated Game; Incentive Mechanism; Sharing

I.INTRODUCTION

In order to enhance the level of common information security, we certainly should invest enough in our own information security management. Besides that, strengthening the security information sharing with partners is equally important. This has led China to set up a national security vulnerabilities information sharing platform; U.S. federal government has encouraged the establishment of industry-based information sharing and analysis center to facilitate the sharing of security information to enhance and protect critical cyber infrastructures. A specific example of security information sharing is the Information Technology Information Sharing and Analysis Center (IT-ISAC) (https://www.it-isac.org) which aims at facilitating the sharing of information on cyber-security threats and vulnerabilities. Platform-building is only the beginning. The key problem is how to make the best use of the platform. The performance of platform depends on the willingness of members to share security information. In this context, our paper will design an incentive mechanism based on repeated game theory in order to enhance the willingness of security information sharing and ultimately maximize the effectiveness of sharing platform.

Questions on information sharing have been previously studied in different context of organizations. Information security is interdependent [1], security information is treated as a hybrid between public and private goods [2-3] and security strategies are divided into two components: self-protection (e.g., firewall, IDS) and self-insurance (e.g., having good backups). Self-protection denotes the ability to decrease the probability of successful attack by hackers [4].To improve the efficiency of self-protection, it is an effective way to share security information each other [5]. Designing incentive compatible mechanisms that lead to efficient production of public goods has long been an important topic in the theoretical literature on public economics. Mutuswami and Winter (2004) propose two sequential mechanisms for efficient production of public goods. As far as security information is concerned, Varian [3]points out that during the period of security information sharing the nature of information assets possessed by two firms, either complementary or substitutable, plays a crucial role in influencing decisions of sharing or not[6].So in order to improve the efficiency of security information platform, an incentive mechanism should be designed to promote the willingness of sharing.

II.INCENTIVE MECHANISM MODEL

In this model, we consider both the reputation factor and punishment mechanism. Firms' reputation is influenced by their strategies they choose, and the reputation will determine whether firms can participate in the next phase of sharing or not as well as the availability of sharing revenue.

Punishment Mechanism: Once firms have adopted a strategy of not sharing, then their rights of access to sharing revenue are cancelled. If they want to re-enter the shared system, they need to experience an isolation period r. During this isolation period they can only contribute sharing but can't share the contributions of other firms.

Reputation Mechanisms: we let the reputation be g for each firm who participates in sharing system, whereas $g \in [0,1]$. The initial default value of g is 1. If a firm refuses to share security information in any stage, the reputation g will switch to the value 0. Specific rules are as following:

We set $g_i(t-1)$ to denote firm i's initial reputation at stage t and $s_i(t)$ to denote the strategy adopted by the firm at this stage.

Step1. If t=1, namely firm i first come to the sharing platform, we assign the reputation of firm i is 1, i.e. $g_i(0)=1$. Otherwise go to next step; Step2. If $g_i(t-1)=1$, while $s_i(t)=No$, go to next step; and while $s_i(t)=Co$, its reputation keeps the same. Otherwise go to step4; Step3. If $g_j(t-1)=1$, then $g_i(t)=0$. Otherwise firm i's reputation keeps the same.Step4. At this point firm i is still in the isolated state. If $s_i(t)=No$, then firm i's reputation keeps the same, otherwise $g_i(t)=g_i(t-1)+1/r$.

If $r=\infty$, it indicates that a firm will not be permitted to share security information with the other forever who once

adopts the non-cooperative strategy. We name it the "cold strategy". If $r=1$, it means that the other firms' strategy is exactly the same one as adopted by firm i in the last round. We name it the "tit for tat strategy".

Discount Factor: This parameter mainly captures the degree of patience of participants. If the game repeats infinitely and everyone has enough patience, any income from a short-term opportunistic behavior is negligible. Participants are motivated to build up own reputations of willingness to share. At same time, this parameter also punishes opportunistic behaviors. We set a discount factor $\delta, \delta \in (0,1)$. The greater δ is, the more attention of the firm to a long-term security benefits.

The best strategies adopted by firms in different phases of repeated game and corresponding payoffs are shown in Tabel 1.

Table 1 Strategies and Payoff

Phase	Reputation before decision	strategies	Expression of payoff	Value of payoff
Sharing	1	(Co_i, Co_j)	$U_i(C)$	$\alpha\sum_{j\neq i} x_j - x_i$
No Sharing	1	(No_i, Co_j)	$U_i(N)$	$\alpha\sum_{j\neq i} x_j$
Isolation	0	(Co_i, No_j)	$U_i(I_1)$	$-x_i$
	0	(No_i, No_j)	$U_i(I_2)$	0

III. Model Analysis

There are three different types of firms in the sharing group, namely: irrational well-meant firms, irrational malicious firms and rational firms. Irrational well-meant firms will share security information all the time in spite of other's strategies. We set its ratio be p_1. Irrational malicious firms are just opposite. They will share no security information in any case and its ratio is p_2. Rational firms make their decision based on the principle of maximizing the interests. Most firms fall into this type and its ratio is p_3. These three types cove all the firms, which means $p_1 + p_2 + p_3 = 1$.

Let us assume the mechanism works and all rational firms adopt sharing strategies in all stages. Firm i seeks to maximize the expected payoff from sharing. This expected payoff at the stage t is given by

$$U_i(t) = \frac{1}{1-\delta}[(1-p_2)(\alpha\sum_{j\neq i} x_j - x_i) - p_2 \bullet x_i] \quad (1)$$

If rational firm i does not share at the stage t, it has to go through a period of no sharing, in other words, r periods of isolation. If firm i wants to regain the revenue of security information from other rational firms, it must provide free shared information throughout the r periods but can't obtain security information from the others. Firm i's reputation g_i will resume to 1 after the isolation period. If firm i continues to adopt no sharing strategies and then will suffer the isolation continually. This process is repeatedly performed. But as we noted, there are still a proportion p_1 of irrational well-meant firms who still provide security information sharing service all the time even although firm i is in isolated period. Therefore when rational firm i adopts no sharing strategy, its expected return is given by:

$$U_i'(t) = \sum_{k=0}^{\infty}\delta^{k(r+1)}[(1-p_2)\bullet\alpha\sum_{j\neq i} x_j + \delta(p_1\alpha\sum_{j\neq i} x_j - x_i)\bullet\frac{1-\delta^{r-1}}{1-\delta}] \quad (2)$$

In order to constrain non-cooperative behavior of firm i, it is clear that the condition $U_i(t) > U_i'(t)$ should meet. Further, we define $U(t) = U_i(t) - U_i'(t)$, which is

$$U(t) = \frac{\alpha\sum_{j\neq i} x_j p_3(\delta - \delta^{r+1}) - x_i(1-\delta)}{(1-\delta)(1-\delta^{r+1})} \quad (3)$$

The incentive mechanism is efficient if $U(t) = U_i(t) - U_i'(t) > 0$.

This yields that $$\frac{\sum_{j\neq i} x_j}{x_i} > \frac{1-\delta}{\alpha p_3(\delta - \delta^{r+1})} \quad (4)$$

If the condition (4) satisfied, rational firms can get more revenue when they choose sharing strategy than no sharing strategy.

PROPOSITION 1: The firms who emphasis on the long-term interest are more eager to participate in security information sharing than those who emphasis on the short-term interest.

We differentiate eq. (3) and obtain that $\frac{\partial U(t)}{\partial \delta} > 0$

Which means $U(t)$ is increasing with δ. The higher the value of $U(t)$ is, the more willing of firms to share their security information. As mentioned above δ is a parameter reflecting how much importance firms attach to a long-term interest, the greater δ is, the more the importance are.

PROPOSITION 2: We let isolation period r tend to be 0 to obtain

$$\lim_{r \to o} U(t) = -\frac{x_i}{1-\delta} < 0$$

In this case the incentive mechanism becomes invalid. This situation is similar to aforementioned "Prisoner's Dilemma". All rational firms will choose not to share. If we let isolation r tend to infinite and derive

$$\lim_{r \to \infty} U(t) = \frac{\alpha \delta p_3 \sum_{j \neq i} x_j - (1-\delta) x_i}{1-\delta}$$

At this point incentive mechanism has reached the maximum punishment. The condition of $\lim_{r \to \infty} U(t) > 0$ yields that $\delta > \frac{x_i}{\alpha p_3 \sum_{j \neq i} x_j + x_i}$.

So minimum of discount factor is $\frac{x_i}{\alpha p_3 \sum_{j \neq i} x_j + x_i}$. Otherwise the mechanism fails to work.

PROPOSITION 3: The higher similarity leads to the more intense of share. We differentiate eq. (3) to obtain $\frac{\partial U(t)}{\partial \alpha} > 0$.

When firms apply same hardware, software, management information system and so on, there is much security problem in common. So sharing among them can induce the spill-over effect. Obviously they are more willing to share with others about security information.

PROPOSITION 4: The proportion of rational firms has an impact on efficiency of the mechanism.

We differentiate eq. (3) to obtain $\frac{\partial U(t)}{\partial p_3} > 0$.

And the condition $U(t) > 0$ yields that $p_3 > \frac{(1-\delta) x_i}{\alpha(\delta - \delta^{r+1}) \sum_{j \neq i} x_j}$.

The above results illustrate that rational firms' impetus of sharing is in increase with the proportion of rational firm. Only in the case that proportion of rational firms is greater than a critical value, which is $\frac{(1-\delta) x_i}{\alpha(\delta - \delta^{r+1}) \sum_{j \neq i} x_j}$, the mechanism we designed comes into effect.

IV. CONCLUSION

In order to improve efficiency of sharing we design an incentive mechanism based on multi-stage game and discuss the factors which influence the efficiency of mechanism. Several main conclusions are drawn. First, the proportion of rational firms plays a positive role on incentive effect. Second, when isolation period tends to be zero, the incentive mechanism fails to work. Only when isolation period exceeds a certain critical value, the mechanism can work. Third, the similarity level of firms group also affects their sharing enthusiasm. Similarity among firms can give rise to positive spillover effects. So they are more willing to take the strategy of share. In addition, firms' patience which refers to their attention on the future earning also impacts firms' enthusiasm. Further, this paper aims at studying the qualitative aspect of incentive mechanism of security information share but lacking of the quantitative empirical analysis. A specific quantitative research on the mechanism is an interesting future work to do.

ACKNOWLEDGMENTS

This work was supported in part by Youth Foundation of Humanity and Social Science of Ministry of Education in China (NO. 11YJC630234) and Innovation Plan for Postgraduates of Jiangsu Province (CXZZ11_0594).

REFERENCE

[1]HOWARD KUNREUTHER, GEOFFREY HEAL. Interdependent Security. The Journal of Risk and Uncertainty，2003（26:2/3）：231-249

[2]J. Hirshleifer. From weakest-link to best-shot: the voluntary provision of public goods. Public Choice，1983（January41(3):371–386）：371-386

[3]Hal Varian. SYSTEM RELIABILITY AND FREE RIDING. Fifth International Conference on Electronic Commerce, N.

Sadeh, ed., ACM Press, 2003, pp. 355–366，2003

[4]Jens Grossklags, Nicolas Christin, John Chuang. Secure or insure? a game-theoretic analysis of information security games. Proceeding of the 17th International Conference on World Wide Web 2008, WWW'08，2008（2008）：209-218

[5]Esther Gal-Or, Anindya Ghose. The Economic Incentives for Sharing Security Information. Information Systems Research，2005，16（2）：186-208

[6]Dengpan Liu, Yonghua Ji, Vijay Mookerjee. Knowledge sharing and investment decisions in information security. Decision Support Systems，2011，52（1）：95-107