Expert Systems with Applications 42 (2015) 6132–6146

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

Game of information security investment: Impact of attack types and network vulnerability

Yong Wu [a,b], Gengzhong Feng [a,c], Nengmin Wang [a,c,*], Huigang Liang [d]

[a] School of Management, Xi'an Jiaotong University, 710049, No. 28 Xiannin Road, Xi'an, Shaanxi, China
[b] Department of Systems Engineering and Engineering Management, City University of Hong Kong, Hong Kong, China
[c] The Key Lab of the Ministry of Education for Process Control & Efficiency Engineering, 710049, No. 28 Xiannin Road, Xi'an, Shaanxi, China
[d] Department of Management Information Systems, College of Business, East Carolina University, Greenville, NC 27858, United States

ARTICLE INFO

Article history:
Available online 8 April 2015

Keywords:
Information security investment
Attack types
Network vulnerability
Game theory
Economic incentives

ABSTRACT

The level of firms' information security investment has recently become a critical issue in the management of IT infrastructure. Prior studies have not considered attack types and firms interconnection simultaneously when investigating the optimisation of such investment. Using game theory, we demonstrate that the optimal security investment level of an interconnected firm against targeted attacks is different from that against opportunistic attacks. Our model shows that not all information security risks are worth fighting against. As the potential loss increases, it is unadvisable to increase the security investment proportionately. Firms should increase investments with intrinsic vulnerability when facing target attacks, but focus on those systems that fall into the midrange of intrinsic vulnerability when facing opportunistic attacks. Firms are unwilling to invest in security and often offload reliability problems onto others when the trusted interdependence relationship becomes tighter in the absence of economic incentives. Thus we also discuss two economic incentives to motivate firms: liability and security information sharing. We find that if the rules are set properly, both economic incentives are effective to not only internalise the negative externality and improve a firm's security level, but also reduce the total expected cost. We show that firms' optimal investments of liability always increase with the increasing number of firms, but the optimal investments on security information sharing increase only when the number of firms is large enough. These insights draw attention to many trade-offs firms often face and the importance of accurate assessment of firms' security environment. Future research directions are discussed based on the limitations and possible extensions of this study.

1. Introduction

Information security investments are usually decided based on various economic models which assume that there is no difference in attack types and firms' information systems are independent of each other. However, these two assumptions deviate from the reality that firms usually face different types of attacks and their systems are interconnected with one another. The security of information systems can be seriously affected by attack types and firms interconnection. For example, according to the CSI (Computer Security Institute) survey (Richardson, 2011), the respondents who suffer from malware infections is four times as many as those who suffer from denial of service, and the loss from theft of information is three times as much as that from virus. Another survey by PWC shows that 22% of the respondents have begun to conduct incident response planning with their partners, in which they agree to share information or allow network access with each other (PWC, 2013). In December 2013, the security breach of the giant US retailer, Target Corporation, exposed credit card and personal data of more than 110 million consumers. It started with a malware-laced phishing email sent to employees at an HVAC firm that is a vendor of Target (Krebs, 2014). Because Target's information systems are difficult to breach, the hackers chose to attack the HVAC firm's information systems that are connected with the Target's but easier to breach. Thus, the effect of attack types and system interconnection is not limited to a single firm's security but also the security of its partners.

Firms continuously face many different types of attacks. CSI classifies attacks into three categories: basic attacks, malware attacks and attack 2.0 (Attack 2.0 refers to the advanced persistent

* Corresponding author at: School of Management, Xi'an Jiaotong University, 710049, No. 28 Xiannin Road, Xi'an, Shaanxi, China.
E-mail addresses: wuyong1202@sina.com (Y. Wu), gzfeng@mail.xjtu.edu.cn (G. Feng), wangnm@mail.xjtu.edu.cn (N. Wang), huigang.liang@gmail.com (H. Liang).

http://dx.doi.org/10.1016/j.eswa.2015.03.033
0957-4174/

threats) (Richardson, 2011). Another research segregates attacks into two types: "High-Frequency-Low-Impact" and "Low-Frequency-High-Impact" attacks (Wang, Chaudhury, & Rao, 2008). This classification is similar to many other researchers': they segregate attacks into two categories, targeted attack and opportunistic attack, based on whether the attacks have a specific target (targeted attack) or a number of intermediate targets to fulfil the hacker's end goal (opportunistic attack) (Casey, 2003; Collins, Gates, & Kataria, 2006; Huang & Behara, 2013; Huang, Hu, & Behara, 2008). For instance, denial of service, website defacement and a purposeful penetration into a bank's system to steal money are typical targeted attacks, while a virus, worm, malware infection and spam e-mail are typical opportunistic attacks (Huang & Behara, 2013).

The trusted interdependence relationship between firms is reflected in two ways based on the PWC survey (PWC, 2013): network connection and information sharing. First, firms' information systems are physically interconnected via a trusted network such as a joint design network. Because the configuration of a network is composed of various interconnected systems, the network becomes vulnerable if any one of the systems is insecure. An organisation's system is at risk if a hacker gains access to its partner's system (Zhao, Xue, & Whinston, 2013). For instance, Walmart allows Proctor & Gamble (P&G) to access information in Walmart's information system via a trusted point-to-point Electronic Data Interchange (EDI), and vice versa. Their ongoing communication and collaboration are conducted through the EDI. This makes it possible that a virus or a hacker breaches the information systems of P&G through the Internet firstly, and then probabilistically break into Walmart's systems via the EDI link. This is possible because Walmart trusts the EDI connection with P&G and therefore will not reject the access request. Second, many firms achieve product innovation or value creation via network economy. As a result, many firms' information is shared with their partners. These firms could suffer information loss together because of information sharing. For example, Walmart and P&G share retail sales information on P&G products at Walmart stores. The retail sales information is stored on servers of both firms. If hackers breach Walmart's server, they can obtain Walmart's private information, which causes losses to Walmart directly, as well as the retail sales information of P&G, which imposes losses on P&G indirectly. Thus sharing valued information is also a form of the trusted interdependence relationship between firms.

Given that the consequences of security breaches are influenced by attack types (Ponemon, 2013) and the interconnectivity of information systems has increased their insecurity (Gordon, Loeb, & Lucyshyn, 2003), this research investigates the impacts of attack types and firms interconnection on the information security investments. In this study we use game theory to model the information security investment problem for two firms that attempt to minimise their total expected losses from security breaches. Because of the prisoner's dilemma[1] in the information security investment game, firms are not always willing to invest in security and often offload reliability problems onto others. The only way to encourage firms to invest in security when they face the possibility of contamination from others is to develop a set of economic incentives (either positive or negative) that make it more attractive for firms to make more investments (Kunreuther & Heal, 2003). Therefore, after investigating the features of optimal information security investment, we also discuss two effective economic incentives: liability and security information sharing to solve the prisoner's dilemma.

Our findings shed light on firms' information security investment behaviours. First, we demonstrate that the optimal security investment level of an interconnected firm against targeted attacks is different from that against opportunistic attacks. Second, in the absence of economic incentives, an interconnected firm is unwilling to increase its security investment when its trusted interdependence relationship with partners becomes tighter. In addition, if the rules of economic incentives are set properly, both liability and security information sharing are effective to not only internalise the negative externality and improve a firm's security level, but also reduce the total expected cost. We find that the firm's optimal investment of liability always increase as the number of firms increases, but the optimal investment of security information sharing increases only when the number of firms is large enough.

The rest of the paper is organised as follows. In Section 2, we review the literature on the economics of information security. In Section 3, we introduce the features of information systems, attack types and network vulnerability. In Section 4, we investigate the features of an interconnected firm's optimal information security investment for both attack types. In Section 5, we discuss two economic incentives for information security investments. We extend our model to the case of three or more firms in Section 6. We present the study's conclusions in Section 7.

2. Literature review

Information security has been a focus of the information systems discipline since the 1990s and become a main stream topic recently (e.g. Parker, 1997; Straub, 1990; Straub, Goodman, & Baskerville, 2008). Although research into the information security has received some attention, economics considerations related to information security investments are rare. As an important decision of information security, information security investments face many uncertainties and should be taken seriously. Since attack types play an important role in information security investment decision, many researchers have studied this issue. Gordon and Loeb (2002) use an economic benefit maximisation method to analyse a firm that faces two different breach probability functions. They show that a firm's optimal information security investment would not exceed 36.8% of the potential loss. Extending the Gordon and Loeb model, Huang et al. (2008) use expected utility theory to analyse a firm facing two attack types: targeted attack and distributed attack. They identify a minimum potential loss, below which a firm does not necessarily invest in information security, and indicate that the information security investment does not necessarily increase with a higher level of risk aversion. Huang and Behara (2013) study the allocation mechanism of a firm's limited information security budget to concurrently defend against two attack types (targeted and opportunistic attack). They find that a firm with a limited security budget should allocate most or all of the investment to prevent one type of attack, even when they simultaneously face different attack types. Cezar, Cavusoglu, and Raghunathan (2014) group the nature of security function into two categories (prevention and detection) and propose a complementarity mechanism to enhance the advantages offered by both functions. Huang, Behara, and Goo (2014) examine the investment made by an organisation in a Healthcare Information Exchange to prevent opportunistic attacks. Besides the economics of information security investments, attack types have also been examined from other information security perspectives. For example, He, Chen, Su, and Sun (2014) propose a scheme to protect users from identity theft attacks in online social networking sites. A commonality of these previous studies is that they focus on a single firm who faces different attack types. However, the security investment decisions may be very different when multiple firms are involved, because firms' interconnection through trusted networks and information sharing make it possible for a firm to suffer from indirect attacks due to other firms'

[1] The prisoner's dilemma is a classical phenomenon in economics games. It suggests that two purely rational individuals will not always cooperate, even if it appears that cooperation is in their best interests.

vulnerability. Thus, this paper complements the IT security literature by considering interconnectivity between firms under different types of attacks.

Protecting interconnected information systems from viruses or hackers can be considered as an interdependent security (IDS) problem. Many problems, such as fire protection, theft protection, vaccinations and airline security, are typical IDS problems. All IDS problems share a common characteristic: the network consisting of the interconnected agents has negative externality, i.e. the agents in the network will increasingly attempt to offload reliability duties onto other agents as the degree of interconnectivity increases. Kunreuther and Heal (2003) study the airline security interdependence problem and find that an airline has much fewer economic incentives to invest in a security system if it believes that other airlines will not make similar investments. Varian (2004) provides a simple model to explain the free rider problem with three prototypical interdependence cases.

In reality, network insecurity is somewhat like air pollution or traffic congestion, in which a firm that connects insecure machines to the Internet does not bear the full consequences of its actions (Anderson & Moore, 2006). In addition, each firm within a network can make its own decision on security investment, but a firm's security risks depend not only on its own security practices but also on the security practices of other firms (Zhao et al., 2013). Traditional economic models such as economic benefit maximisation and expected utility theory do not allow a firm's information security investment behaviour to influence another's. Yet, a model for analysing information security investments should capture the strategic interaction between interconnected firms (Cavusoglu, Raghunathan, & Yue, 2008). Game theory is appropriate to model such strategic interactions. The game players could be firms trying to protect their information systems and hackers trying to attack the information systems. Alternatively, players could be interconnected firms that try to individually or jointly fend off attacks. Cavusoglu, Mishra, and Raghunathan (2005) apply game theory to explain that a firm can obtain a positive value from an intrusion detection system if the detection rate is greater than a threshold and will obtain a non-negative value from an optimally configured intrusion detection system. Hui, Hui, and Yue (2012) use game theory to analyse how the system interdependency risks interact with a mandatory security requirement to affect the equilibrium behaviours of a managed security service provider and its clients.

Because of the negative externality of interdependent security, many studies apply economic incentives to solve the IDS problem. Gordon et al. (2003) use game theory to show that information sharing can increase the level of information security and propose some incentive mechanisms for sharing information. Zhao et al. (2013) examine two alternative risk management approaches (risk pooling arrangements and managed security services) to solve the interdependency risks. Fang, Parameswaran, Zhao, and Whinston (2014) use game theory to model the interdependent security risk of inter-organisational information systems and propose an incentive mechanism to solve this problem. Only a few studies investigate the interdependent security risk from economic consideration of information security investments. For example, Ogut, Menon, and Raghunathan (2005) use game theory to analyse the impact of interdependent risks in cyber insurance and IT security investment and find that the interdependence of cyber-risk reduces a firm's investment in security technologies and cyber insurance. Kolfal, Patterson, and Yeo (2013) analyse optimal security investment decisions based on customer response to adverse IT security events.

Our literature review shows that prior studies have focused on many aspects of information security with interdependent risks. However, little research reveals how interdependent risks affect firms' information security investments when facing different attack types, and how economic incentives should be actualised to solve the negative externality of information security investments. We intend to fill these research gaps by developing a game-theoretical model to consider the optimal information security investments and the optimal economic incentives when interconnected firms face different attack types.

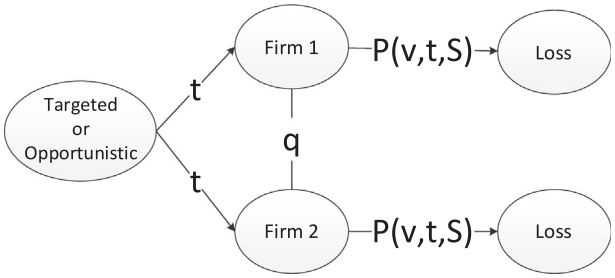

Fig. 1. The conceptual description of the model.

3. Model preliminaries

To model information security investments, we consider a single-event, single-period security breach,[2] with a probability p, of two risk-neutral[3] firms who face two attack types, targeted attack and opportunistic attack. The two firms' information systems are interconnected through trusted network or storing mutual information, as shown by Fig. 1. The case of three or more firms is similar and will be discussed in Section 6.

3.1. Information system features

When attackers successfully breach a firm's information system that stores confidential information, the firm may suffer a loss. We use L to denote the totality of loss this firm suffers. L includes not only direct losses such as those resulting from bank accounts stolen but also indirect losses such as the damage to a firm's reputation due to the security breach.

Because of the limitation of security technology and the complexity of security issues, perfect security is impossible for an information system (PWC, 2013; Zhang, Deng, Wei, & Deng, 2012). A firm could spend a certain amount of money to decrease the risk by reducing the breach probability. Many previous articles (e.g., Gordon & Loeb, 2002; Huang et al., 2008) show that the breach probability of a given information system can be characterised by three parameters: v, t and S. Let p be the breach probability, expressed as $p(v,t,S)$. The first parameter, v, denotes the information system's intrinsic vulnerability, i.e. without security protection, the success probability of an attack once launched. Note that the parameter v is intrinsic to the given information system and is only determined by the information system's configuration, i.e. v is fixed for a given information system and is not affected by the external environment, such as attack types. Because v is a probability, $0 < v < 1$.

The second parameter, t, represents the attack probability, or the probability for the information system to receive a certain type of attacks. We assume that a firm's security investment is

[2] In a single-event, one firm only suffers one (direct or indirect) breach. In a single-period economic model, all decisions and outcomes occur in a simultaneous instant.

[3] A risk-neutral firm is indifferent to investments that have the same expected value, even though the investments may have varying amounts of risk. For example, Investment #1 that generates either a net return of $200,000 or a net loss of $100,000 each with probability of 0.5, and Investment #2 that generates a net return of either $40,000 or $60,000 each with probability of 0.5. Notice that Investment #1 has more risk (i.e., larger standard deviation around the expected value) than investment #2. For a risk-neutral firm, the two investments are considered equal. But a risk-averse firm would require a higher expected value for an investment with a higher risk (Gordon & Loeb, 2002).

confidential to the attackers, thus the security investment does not affect the hackers' attack probability. In other words, t is exogenous to a firm's information system, and we fix the attack probability at $0 < t < 1$.

The third parameter, S, represents the information security investment. It can take many forms, such as purchasing firewall, installing intrusion detection systems or training users. Developing effective security investment strategies can prevent the damage from attackers (Andoh-Baidoo & Osei-Bryson, 2007). Thus the purpose of investing in information security is to decrease the breach probability. We formalise the above observations in the following assumption about the breach probability:

Assumption 1. We assume the law of diminishing return, which yields the following: $p' < 0$ and $p'' > 0$ where p' denotes the partial derivative of p with respect to S and p'' denotes the partial derivative of p' with respect to S.

3.2. Attack types

The difference between targeted attack and opportunistic attack in our model is shown in breach probability functions. We adopt the typical breach probability functions used in previous studies[4] (Gordon & Loeb, 2002; Huang & Behara, 2013; Huang et al., 2008):

$$p^I = \frac{vt^I}{kS^I + 1} \tag{1}$$

$$p^{II} = t^{II} v^{kS^{II}+1} \tag{2}$$

Formula (1) represents targeted attack, which is called *Class I* below. Formula (2) represents opportunistic attack, which is called *Class II* below. Compared to a targeted attack, an opportunistic attack may be more pervasive, massive, easier to address and tends to cause less damages to firms (Huang & Behara, 2013; Kim, Im, & Park, 2010). In contrast, firms may be less likely to encounter a targeted attack but tend to suffer from significant losses if a targeted attack is successful. As mentioned before, according to the CSI survey (Richardson, 2011), the respondents who suffer from malware infections (opportunistic attack) is four times as many as those who suffer from denial of service (targeted attack), and the loss from theft of information (targeted attack) is three times as much as that from virus (opportunistic attack). Thus, we formalize the above observations in the following assumption about attack types:

Assumption 2. We assume that the threat probability of an opportunistic attack is greater than that of a targeted attack and the loss caused by a targeted attack is greater than that caused by an opportunistic attack, i.e. $t^{II} = nt^I$, where $n > 1$ and $L^I = mL^{II}$ where $m > 1$.

The parameter k in the two formulas represents the security investment effectiveness. Because intrinsic vulnerability is not related to attack types and we assume that investment effectiveness for both attack types are equal, other parameters, such as S and t, have the superscript in both breach probability functions. Both of the two formulas satisfy the conditions of the breach probability function, $p(v, t, S)$, described above, which can be easily verified.

The two breach probability functions indicate that the breach probability and the threat probability is linear, given a reasonable assumption that threat probability is outside of the firms' control. However, the breach probability shows quite different characteristics with respect to the intrinsic vulnerability and the security investment. The breach probability is more convex in an opportunistic attack than in a targeted attack with respect to the intrinsic vulnerability. This relationship indicates that the breach probability of an opportunistic attack increases more slowly than that of a target attack when the intrinsic vulnerability is small, but once the intrinsic vulnerability crosses a certain threshold, the breach probability of an opportunistic attack increases more rapidly than that of a target attack. The breach probability is also more convex in an opportunistic attack than in a targeted attack with respect to the security investment. This relationship indicates that an initial investment more significantly affects opportunistic attacks. Furthermore, it also explains why opportunistic attacks can be more easily addressed than targeted attacks.

3.3. Network vulnerability

As shown in Fig. 1, attackers can successfully attack firm 1 (or firm 2) in two ways: direct or indirect. A direct breach of firm 1 occurs when attackers breach its information system directly, that is, the direct breach happens because of the firm's own security lapse. An indirect breach of firm 1 occurs when attackers breach the security of firm 2 firstly and the breach spreads to firm 1 through their trusted interdependence relationship. We assume that the probability that an indirect breach of firm 1 occurs is a constant, q, given that firm 2 has been breached. This parameter measures the extent of trust interdependence relationship between a firm and its partner, and does not change with self-security investment. q is high when the extent of system access authority is high. q is also high when firms share more information. Because q is a probability, $0 < q < 1$. Based on the description of network vulnerability, firm 1's investment can only reduce its own direct breach probability but cannot reduce its indirect breach probability. Firms can reduce indirect breach probability by redefining the trusted interdependence relationship with their partners (for instance, reducing the extent of system access authority or the extent of information sharing). We make the following assumptions about the total breach probability:

Assumption 3. The total breach probability of firm 1 depends on not only the probability of direct breaches but also the probability of indirect breaches which is equal to the direct breach probability of firm 2 multiplied by the network vulnerability, q.

Thus the total probability of a successful breach for firm 1 can be expressed as follows:

$$P_1 = 1 - (1 - p_1)(1 - qp_2), \tag{3}$$

where p_1 is the direct breach probability of firm 1, qp_2 is the indirect breach probability of firm 1, and $(1 - p_1)(1 - qp_2)$ is the probability that firm 1 cannot be breached. We can define a similar breach probability for firm 2. Table 1 summarises the parameters and variables used in our model. The last four parameters will be introduced later.

4. Optimal security investments

We now examine the optimal information security investments for the two interconnected firms. We impose symmetric conditions on the two firms, i.e. $v_1 = v_2$, $t_1 = t_2$, $L_1 = L_2$ and $k_1 = k_2$. In the following sections, we omit the subscript when the two firms' variables are equal. Firm 1 aims to select a security investment level to maximise its expected net benefit, i.e. minimising the total expected cost. The total expected cost consists of the information security investment plus the expected loss, and the expected loss equals to the potential loss multiplied by its total breach

[4] Note that in the following sections, we use superscript *I* and *II* to represent the attack types, and used subscript 1 and 2 to represent the sequence of firms.

Table 1
Summary of notations.

Notation	Name	Condition
L	Potential loss	$L \geqslant 0$
v	Intrinsic vulnerability	$0 < v < 1$
t	Threat probability	$0 < t < 1$
S	Security investment	$S \geqslant 0$
k	Investment effectiveness	$k > 0$
p	Breach probability	$p(v, t, S)$
q	Network vulnerability	$0 < q < 1$
n	Ratio of threat probability	$n > 1$
m	Ratio of potential loss	$m > 1$
C	Total expected cost	$C \geqslant 0$
λ	Portion of liability	$0 < \lambda < 1$
θ	Portion of security information sharing	$0 < \theta < 1$
N	The number of firms	$N > 2$

probability. Thus, we can calculate firm 1's total expected cost as follows:

$$C = [1 - (1 - p_1)(1 - qp_2)]L + S_1 \tag{4}$$

After rearranging the first-order condition and the second-order condition, we obtain the following:

$$\frac{\partial C}{\partial S_1} = p_1'(1 - qp_2)L + 1 \tag{5}$$

$$\frac{\partial^2 C}{\partial S_1^2} = p_1''(1 - qp_2)L \tag{6}$$

Because (6) is greater than zero, the total expected cost function is convex and there exists an optimal security investment to minimise the total expected cost. When substituting the two breach probability functions (1) and (2) into (5), we can obtain the relationship between S_1 and S_2. For *Class I*, we obtain the following:

$$\frac{\partial C^I}{\partial S_1} = -\frac{kvt^I}{(kS_1^I + 1)^2}\left(1 - q\frac{vt^I}{kS_2^I + 1}\right)L^I + 1 \tag{7}$$

For *Class II*, we obtain the following:

$$\frac{\partial C^{II}}{\partial S_1} = k(\ln v)t^{II}v^{kS_1^{II}+1}(1 - qt^{II}v^{kS_2^{II}+1})L^{II} + 1 \tag{8}$$

Both firms simultaneously determine their investments, and the total expected cost is a multivariate continuous function. We can use the two reaction curve $S_2(S_1)$ and $S_1(S_2)$ to obtain each player's game strategy based on the other player's strategy. Solving the intersection of the two reaction curves and this intersection is our Nash equilibrium of the information security investment game. The Nash equilibrium is a solution concept of a non-cooperative game involving two or more players, in which each player is assumed to know the equilibrium strategies of the other players, and no player has anything to gain by changing only their own strategy. Since we assume that the two firms are identical, these factors such as potential loss and intrinsic vulnerability are common knowledge for both firms. Thus, both firms know the other's strategy based on common knowledge. The two firms will not unilaterally change their decision at the equilibrium state. More costs will be incurred if they choose other investment levels outside of the equilibrium strategy. Thus maintaining the Nash equilibrium is the best strategy for both firms.

By symmetry, the reaction curves of both firms are identical. Thus the Nash equilibrium of two firms are equal for both attack types, i.e. $S_1^{I^*} = S_2^{I^*}$ and $S_1^{II^*} = S_2^{II^*}$. To simplify, we use S^{I^*} and S^{II^*} to represent the optimal investment for both attack types. The slope of $S_2(S_1)$ should be higher than the slope of $S_1(S_2)$ to make the two reaction curves intersect to ensure the existence of the Nash equilibrium.

From (7), for *Class I*, we obtain the slope of two reaction curves in Nash equilibrium:

$$\left(\frac{\partial S_2^I}{\partial S_1^I} = \frac{2(kS^{I^*} + 1 - qvt^I)}{qvt^I}\right) > \left(\frac{\partial S_1^I}{\partial S_2^I} = \frac{qvt^I}{2(kS^{I^*} + 1 - qvt^I)}\right) \tag{9}$$

From (8), for *Class II*, we obtain the slope of two reaction curves in Nash equilibrium:

$$\left(\frac{\partial S_2^{II}}{\partial S_1^{II}} = \frac{1 - qt^{II}v^{kS^{II^*}+1}}{qt^{II}v^{kS^{II^*}+1}}\right) > \left(\frac{\partial S_1^{II}}{\partial S_2^{II}} = \frac{qt^{II}v^{kS^{II^*}+1}}{1 - qt^{II}v^{kS^{II^*}+1}}\right) \tag{10}$$

From (9), we obtain $3qvt^I < 2(kS^{I^*} + 1)$ for any S^{I^*}. Thus, we can obtain $qvt^I < \frac{2}{3}$ for *Class I*. From (10), we obtain $2qv^{kS^{II^*}+1}t^{II} < 1$ for any S^{II^*}. Thus, we obtain $qvt^{II} < \frac{1}{2}$ for *Class II*. We establish the boundary *for Class I* in a tighter condition to comparatively analyse both attack types at the same condition. In other words, we assume that both attack types satisfy the condition $qvt < \frac{1}{2}$, which is a sufficient but not necessary condition. Because our study focuses on the impact of the network vulnerability, we assume that the condition $vt < \frac{1}{2}$ holds to ensure that the problem always contains an optimal investment for all values of network vulnerability.

Setting (5) to zero can yield the optimal security investment of firm 1 for both attack types:

$$S = p'^{-1}\left(\frac{-1/L}{1 - qp(S^*)}\right) \tag{11}$$

Because closed-form solutions for optimal security investment are too complex, we adopt the implicit function analysis method. Thus, the optimal security investment of the targeted attack for firm 1 satisfies the following:

$$F^I = -\frac{kvt^I}{(kS^{I^*} + 1)^2}\left(1 - q\frac{vt^I}{kS^{I^*} + 1}\right)L^I + 1 = 0 \tag{12}$$

Furthermore, the optimal security investment of the opportunistic attack for firm 1 satisfies the following relationship:

$$F^{II} = k(\ln v)t^{II}v^{kS^{II^*}+1}(1 - qt^{II}v^{kS^{II^*}+1})L^{II} + 1 = 0 \tag{13}$$

By setting $y = S^{I^*}$ or $y = S^{II^*}$ and x as each parameter above, we can use $\frac{dy}{dx} = -\frac{\partial F/\partial x}{\partial F/\partial y}$ to examine the relationship between the optimal security investment and these parameters.

4.1. Optimal investment and potential loss

First, we examine the relationship between the optimal investment and the potential loss. Using implicit functions (11) and (12) for analysis, we obtain the following for *Class I*:

$$\frac{\partial S^{I^*}}{\partial L^I} = \frac{(kS^{I^*} + 1)(kS^{I^*} + 1 - qvt^I)}{kL^I(2kS^{I^*} + 2 - 3qvt^I)} \tag{14}$$

$$sign\left(\frac{\partial^2 S^{I^*}}{\partial L^{I2}}\right) = -sign\left(\left(kS^{I^*} + 1 - \frac{3}{2}qvt^I\right)^2 + \frac{3}{4}(qvt^I)^2\right) \tag{15}$$

For *Class II*, we obtain the following:

$$\frac{\partial S^{II^*}}{\partial L^{II}} = \frac{1 - qt^{II}v^{kS^{II^*}+1}}{k(\ln v)L^{II}(2qt^{II}v^{kS^{II^*}+1} - 1)} \tag{16}$$

$$sign\left(\frac{\partial^2 S^{II^*}}{\partial L^{II2}}\right) = -sign\left(\left(2qt^{II}v^{kS^{II^*}+1} - \frac{3}{4}\right)^2 + \frac{7}{16}\right) \tag{17}$$

We can easily identify that (14) and (16) are both greater than zero and (15) and (17) are both less than zero. Thus, we can conclude that the optimal security investment increases with the potential loss at a decreasing rate for both attack types.

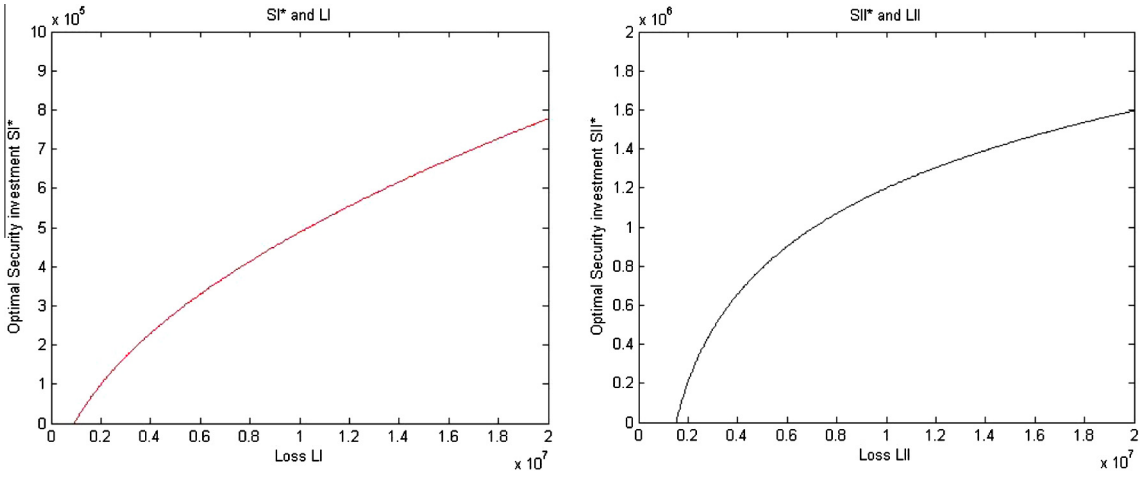

Fig. 2. Optimal investment with potential loss.

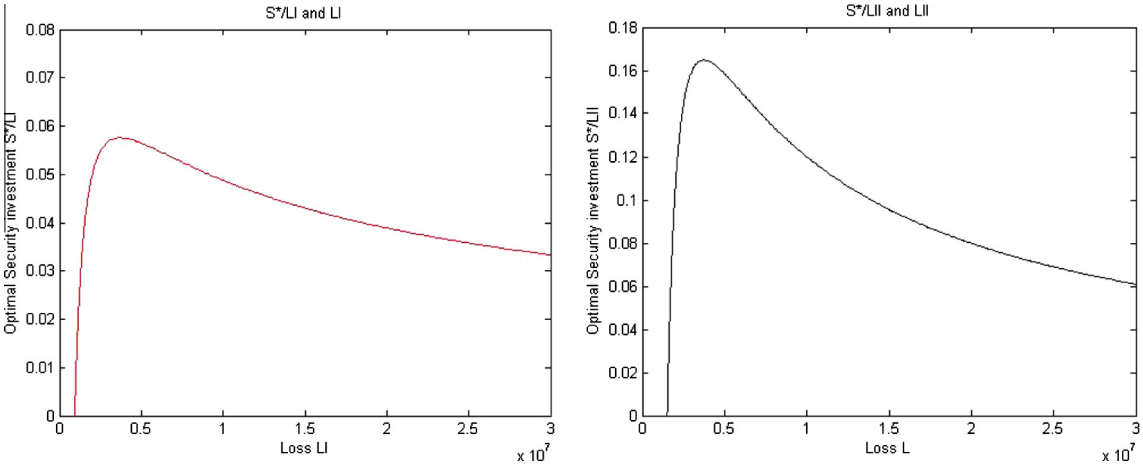

Fig. 3. Optimal investment with loss.

By using (12) and (13) and setting $S^{I^*} = 0$ and $S^{II^*} = 0$, we can obtain the minimum potential loss, below which firm 1's optimal security investment is zero. For *Class I*, we obtain $L_0^I = \frac{1}{kt^I v(1-qt^I v)}$ and for *Class II*, we obtain $L_0^{II} = \frac{1}{k(\ln v)t^{II} v(qt^{II} v-1)}$. Based on these two formulas we can deduce that $L_0^I < -n(\ln v)L_0^{II}$. Therefore, firms have a higher incentive to not invest in targeted attack when the potential loss caused by both attack types is so small that firms do not need to invest in security and v is greater than $e^{-\frac{1}{n}}$. In general, the minimum potential loss of targeted attacks is greater than that of opportunistic attacks. The condition above is tight; for instance, if $n = 2$, the minimum potential loss of opportunistic attack can be greater than that of targeted attack only when $v > 0.61$. If $n = 10$, the minimum potential loss of opportunistic attack can be greater than that of a targeted attack only when $v > 0.91$, but an information system with such a large intrinsic vulnerability is unlikely to be used.

The above analysis can be further illustrated with numerical examples. Fig. 2 shows the results of the numerical analysis when $v = 0.7, k = 0.000005, 2t^I = t^{II} = 0.7$ and $q = 0.5$. (The results are similar when we vary the values of v, k, t and q). The optimal information security investments of both attack types clearly increase with the potential loss at a decreasing rate. Furthermore, the two curves do not originate at zero. Therefore, both attack types feature a minimum potential loss as described above.

We also drew Fig. 3, in which the ordinate is the proportion of optimal investment and potential loss to find the change of the optimal investment when the potential loss increases. Fig. 3 shows that once $L > L_0$, both S^{I^*}/L and S^{II^*}/L increase rapidly to reach a peak and then decrease slowly to zero. Therefore, the optimal security investment increases with the potential loss but ultimately reaches a plateau as the potential loss increases for both attack types.

We now show the impact of potential loss on the optimal investments of firms.

Proposition 1. For both attack types, there exists a minimum potential loss, below which an interconnected firm does not need to invest in security and above which the firm's optimal investment increases with the potential loss at a decreasing rate, but ultimately reaches a plateau.

Several interesting implications emerge from this proposition. First, if the potential loss caused by an information security breach is sufficiently small, firms benefit from bearing the risk and not investing in security, even though firms simultaneously face direct and indirect attacks. In general, the minimum potential loss of targeted attacks below which firms have no incentive to invest in security is greater than that of opportunistic attacks. However, the minimum potential loss of opportunistic attacks can be greater than that of targeted attacks under some tight conditions. This

finding highlights the importance of adequate assessment of firms' potential loss and identifying the nature of attacks, because whether a firm would invest in security or not depends on the values of both potential loss and attack types.

Second, for both attack types, the optimal security investment increases with the potential loss at a decreasing rate, and finally reaches a plateau. This finding is in contrast to Huang et al. (2008), who reported that the optimal security investment of a single firm increases rapidly and then reaches a plateau as the potential loss increases for targeted attacks. For opportunistic attacks, they reported that the optimal security investment of a single firm increases rapidly and then becomes a percentage of potential loss as the potential loss increases. In other words, our analysis shows that a firm's optimal investment will ultimately reach a plateau irrespective of the attack types. Based on (14) and (16), both $\partial S^{I^*}/\partial L^I$ and $\partial S^{II^*}/\partial L^{II}$ are close to zero when L approaches infinity. Thus, the optimal investment in information security will finally reach a plateau for an interconnected firm when the potential loss increases, irrespective of the attack types. This relationship is understandable when we consider formula (4): the expected cost is equal to the total breach probability multiplied by the potential loss, but the total breach probability and the potential loss are independent of each other. Thus, the investment will lower the total breach probability and thereby lower the expected cost when the potential losses from both attack types are moderate or low. However, when the potential losses are high and result in catastrophic damages, investing in security to lower the total breach probability cannot reduce the expected cost to a range that firms could accept. In this situation, a better solution for firms is to adopt other measures, such as buying cyber insurance to compensate for the catastrophic loss. This finding also highlights the importance of adequate assessment of firms' potential loss, because firms should stop investing in security and adopt other measures when the potential loss is catastrophic.

4.2. Optimal investment and intrinsic vulnerability

Next, we examine the relationship between the optimal security investment and the intrinsic vulnerability. First, we discuss *Class I* with the help of (12) to obtain the following:

$$\frac{\partial S^{I^*}}{\partial v} = \frac{(kS^{I^*}+1)(kS^{I^*}+1-2qt^I v)}{kv(2kS^{I^*}+2-3qt^I v)} \tag{18}$$

$$sign\left(\frac{\partial^2 S^{I^*}}{\partial v^{I2}}\right) = -sign\left(\left(kS^{I^*}+1-\frac{3}{2}qvt^I\right)^2+\frac{3}{4}(qvt^I)^2\right) \tag{19}$$

Eq. (18) is greater than zero and (19) is less than zero, i.e. for the targeted attack, the optimal security investment increases with the intrinsic vulnerability at a decreasing rate.

Let $S^{I^*}=0$ in (12) to obtain $v_0(1-qt^I v_0)=\frac{1}{kt^I L^I}$. We then solve this formula to obtain $v_0=\frac{1-\sqrt{1-\frac{4q}{kL^I}}}{2qt^I}$ (we abandoned the other value because the intrinsic vulnerability is less than one), where v_0 is the minimum intrinsic vulnerability that makes S^{I^*} equal to zero and after v_0, S^{I^*} is greater than zero and increases with v. Fig. 4 shows the computational results of the above analysis, where $k=0.000005, 2t^I=t^{II}=0.5, q=0.5$ and $L^I=2L^{II}=\$4M$. (The results are similar when we varied the values of k,t,q and L). Fig. 4 shows that a minimum vulnerability, v_0, exists that sets the optimal security investment to zero. Beyond this minimum, the optimal security investment increases with the intrinsic vulnerability at a decreasing rate.

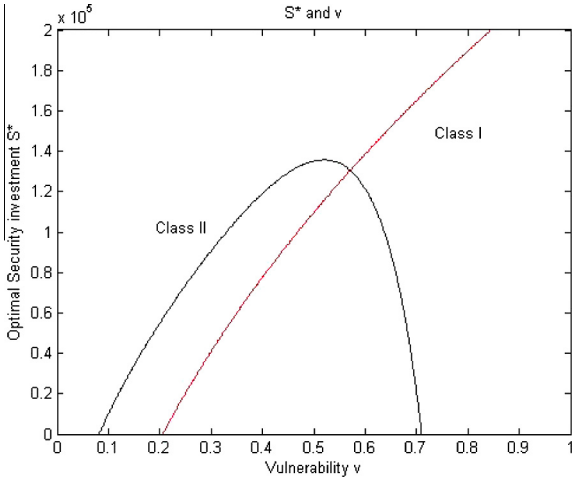

Fig. 4. Optimal investment with intrinsic vulnerability.

We then discussed *Class II* with the help of implicit function (13) to obtain the following:

$$\frac{\partial S^{II^*}}{\partial v} = -\left[\frac{kS^{II^*}+1}{kv(\ln v)}+\frac{1-qt^{II}v^{kS^{II^*}+1}}{kv(\ln v)^2(1-2qt^{II}v^{kS^{II^*}+1})}\right] \tag{20}$$

We examine two extreme cases of $v\to 0$ and $v\to 1$. With the help of L'Hôpital's Rule, we find $\left.\frac{\partial S^{II^*}}{\partial v}\right|_{v=0^+} = \lim_{v\to 0^+}\frac{1}{k}\frac{(kS^{II^*}+1)(\ln v)+1}{v(\ln v)^2} = \frac{1}{k}\lim_{v\to 0^+}\frac{(kS^{II^*}+1)/v}{(\ln v)^2+2(\ln v)} = \frac{1}{k}\lim_{v\to 0^+}\frac{kS^{II^*}+1}{2v} = +\infty$. Because $\lim_{v\to 1}\frac{kS^{II^*}+1}{kv(\ln v)} = +\infty$ and $\lim_{v\to 1}\frac{1-qt^{II}v^{kS^{II^*}+1}}{kv(\ln v)^2(1-2qt^{II}v^{kS^{II^*}+1})} = +\infty$, we obtain $\left.\frac{\partial S^{II^*}}{\partial v}\right|_{v=1} = -\infty$.

We set (13) equal zero and obtain $v(-\ln v)(1-qt^{II}v)=\frac{1}{kt^{II}L^{II}}$. Note that $vt<\frac{1}{2}$, we can obtain $v(-\ln v)>\frac{2}{kt^{II}L^{II}}$ for $0<v<1$. Furthermore, $-vlnv$ takes on a maximum at $v=\frac{1}{e}$ and approaches 0 when v approaches either 0 or 1. Thus, for a given k, t^{II}, q and L^{II}, there exists a lower limit, v_0, and an upper limit, v_1, such that $S^{II^*}=0$ when $0<v<v_0$ or $v_1<v<1$ and $S^{II^*}>0$ when $v_0<v<v_1$. To determine if the v' that maximises S^{II^*} is unique, we set $\frac{\partial S^{II^*}}{\partial v}=0$, which yield $F=(kS^{II^*}+1)(\ln v)(1-2qt^{II}v^{kS^{II^*}+1})+1-qt^{II}v^{kS^{II^*}+1}=0$. We also obtain $\frac{\partial F}{\partial v}=-\frac{kS^{II^*}+1}{v}(2kS^{II^*}(\ln v)qt^{II}v^{kS^{II^*}+1}+2(\ln v)qt^{II}v^{kS^{II^*}+1}+3qt^{II}v^{kS^{II^*}+1}-1)$. Thus, as a sufficient but not necessary condition, when $vt<\frac{1}{3}$, $\frac{\partial F}{\partial v}>0$. Therefore, the value of v' that maximises S^{II^*} is unique in this situation.

In summary, we obtain that S^{II^*} increases from $-\infty$ when $v=0$ to zero when $v=v_0$. It increases to a positive maximum when $v=v'$ and then decreases to zero where $v=v_1$. It further decreases to $-\infty$ when v approaches 1. Although closed-form solutions for v_0, v_1 and v' could not be found, we can determine these values with numerical solutions. Fig. 4 shows the computational results of the above analysis, where $q=0.5, k=0.000005, 2t^I=t^{II}=0.5$ and $L^I=2L^{II}=\$4M$ (The results are similar when we vary the value of q, k, t and L). Fig. 4 shows that there exists a lower limit v_0 and an upper limit v_1 such that $S^{II^*}=0$ when $0<v<v_0$ or $v_1<v<1$ and $S^{II^*}>0$ when $v_0<v<v_1$. Furthermore, the v' that maximises S^{II^*} is unique. We now show the impact of intrinsic vulnerability on the optimal investments of firms.

Proposition 2. An interconnected firm that faces targeted attacks features a minimum intrinsic vulnerability, below which the optimal investment is zero and above which the optimal investment increases with the intrinsic vulnerability at a decreasing rate.

An interconnected firm that faces opportunistic attacks features a range of intrinsic vulnerability values, outside of which the optimal investment is zero and inside of which, the optimal investment is greater than zero and only one maximum exists.

Proposition 2 demonstrates that the impact of the intrinsic vulnerability on a firm's optimal security investment against targeted attacks is different from that against opportunistic attacks. We define a secure-configuration information system as one with which $v < v'$ and a dangerous-configuration information system as one with which $v > v'$.

In a secure-configuration, firms are willing to invest more in security as the intrinsic vulnerability increases, irrespective of attack types. In a dangerous-configuration, firms are still willing to invest more as the intrinsic vulnerability increases when they face targeted attacks, but are inclined to invest less as the intrinsic vulnerability increases when they face opportunistic attacks. Each firm strikes an appropriate balance between its risk exposure and the opportunity to mitigate the risk through investments in security (Cavusoglu et al., 2008). Thus firms face two risk types when they decide the security investment: risk of loss from security breach (security risk) and risk of over-spending in security (investment risk). In a secure-configuration, firms are more concerned with security risks, irrespective of the attack type. In a dangerous-configuration, firms are still more concerned with security risks when they face targeted attacks, but care more about investment risks when they face opportunistic attacks.

Thus, firms should identify which attack type they mainly face and the extent of intrinsic vulnerability before deciding on information security investments. When firms mainly face targeted attacks, they can ignore systems that have low intrinsic vulnerability and invest in systems that have a moderate or high intrinsic vulnerability. Because the security risk always outweighs the investment risk, firms should correspondingly increase investment, irrespective of the level of intrinsic vulnerability. This consequence is understandable because attackers are more likely to attack a system with a high intrinsic vulnerability if two systems are of same value to attackers. In addition, once a determined attacker decides to hack the targeted system, he/she is not easily stopped and will make every effort to complete the attack, and the loss caused by the targeted attack is usually catastrophic. Thus the security risk is always greater than the investment risk and firms should be more cautious and prevent breaches in their system as much as possible when they are under targeted attacks.

When a firm mainly faces opportunistic attacks, it can ignore systems that have an overly low or overly high intrinsic vulnerability and invest in systems that have a moderate intrinsic vulnerability. We can explain this conclusion by analysing the features of an opportunistic attack. As described above, opportunistic attacks are pervasive, frequent, easy to address and tend to cause less damage to firms, and an initial investment has a more significant effect against opportunistic attack. Thus, opportunistic attacks do not easily breach the system when the intrinsic vulnerability is sufficiently small. However, an opportunistic attack could easily breach the system when the intrinsic vulnerability is sufficiently high so that the system is in a dangerous configuration. Furthermore, opportunistic attacks are usually contagious because they are pervasive and frequent. In this situation, additional investment cannot prevent infections. Thus the investment risk outweighs the security risk and firms become more cautious about the investment risk. Ultimately, they are inclined to decrease the amount of investment. Because the intrinsic vulnerability is decided by the configuration of information system, firms should redefine system configuration that would reduce intrinsic vulnerability rather than invest against opportunistic attacks when the system is in a dangerous- configuration.

4.3. Optimal investment and network vulnerability

We now address the relationship between the optimal investment and network vulnerability. Network vulnerability, q, represents the extent of trusted interdependence relationship between two firms. Using (12) and (13) for analysis, we obtain the following for *Class I*:

$$\frac{\partial S^{I^*}}{\partial q} = -\frac{vt^I(kS^{I^*}+1)}{k(2kS^{I^*}+2-3qvt^I)} \tag{21}$$

$$sign\left(\frac{\partial^2 S^{I^*}}{\partial q^2}\right) = -sign(kS^{I^*}+1-qvt^I) \tag{22}$$

We obtain the following for *Class II*:

$$\frac{\partial S^{II^*}}{\partial q} = -\frac{t^{II}v^{kS^{II^*}+1}}{k(\ln v)(2qt^{II}v^{kS^{II^*}+1}-1)} \tag{23}$$

$$sign\left(\frac{\partial^2 S^{II^*}}{\partial q^2}\right) = -sign(3-4v^{kS^{II^*}+1}qt^{II}) \tag{24}$$

Eqs. (21) and (23) are both less than zero. Formula (22) and (24) are both less than zero, i.e. the optimal security investment decreases with the network vulnerability at a decreasing rate for both attack types. Therefore, information security systems indeed show interconnectivity with negative externality so that both firms are less willing to invest in security when their trusted interdependence relationship is tighter.

Next, we compare the impact of network vulnerability on both attack types. We substitute $t^{II} = nt^I$ into $\frac{\partial S^{II^*}}{\partial q}$ and obtained $\frac{\partial S^{II^*}}{\partial q} = -\frac{t^I v^{kS^{II^*}+1}}{k(\ln v)(2qt^I v^{kS^{II^*}+1}-1/n)}$. If $\frac{\partial S^{I^*}}{\partial q} < \frac{\partial S^{II^*}}{\partial q}$, then $2-\frac{3qvt}{kS^*+1} < (\ln v)(2qvt-\frac{1}{nv^{kS^*}})$ and $2 < (-\ln v)(1-2qvt^{II})$, which yields $v < e^{-2}$. Thus, as a sufficient but not necessary condition, when $v < e^{-2}$, $\frac{\partial S^{I^*}}{\partial q} < \frac{\partial S^{II^*}}{\partial q}$. Therefore, when the intrinsic vulnerability is less than e^{-2}, the network vulnerability has a stronger impact on a firm's investment when it faces targeted attack as opposed to an opportunistic attack.

Fig. 5 shows the optimal security investment levels S^{I^*} and S^{II^*} with respect to the network vulnerability, for $v = 0.4$, $k = 0.000005$, $2t^I = t^{II} = 0.8$ and $L^I = 2L^{II} = \$1M$.

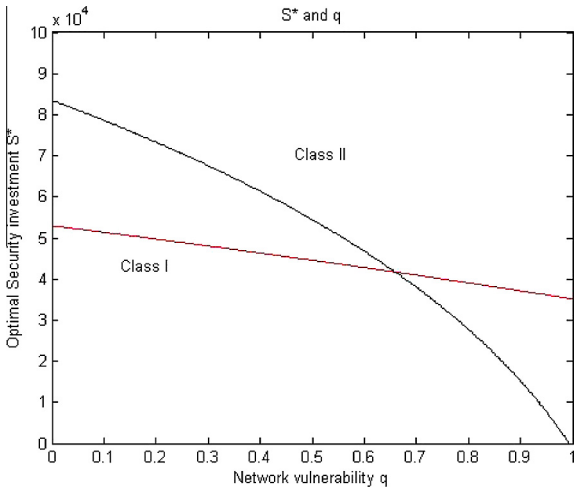

Fig. 5. Optimal investment with network vulnerability.

We now show the impact of network vulnerability on the optimal investments of firms.

Proposition 3. For both attack types, an interconnected firm's optimal investment decreases with the network vulnerability at a decreasing rate. When the network vulnerability is less than e^{-2}, the network vulnerability has a stronger impact on a firm's investment when firm faces a targeted attack than facing an opportunistic attack.

Proposition 3 demonstrates that the amount of investment will decrease more quickly when the network vulnerability increases. This conclusion seems counter-intuitive, because the network vulnerability increases a firm's total breach probability, firms expose more risks and thus should invest more in security. However, a firm's indirect breach probability increases when the network vulnerability increases. As we showed earlier, a firm's investment can only reduce its direct breach probability and cannot reduce its indirect breach probability. Thus, firms do not invest at the same level when they are interconnected because the inefficiency of investment reduces a firm's incentives to invest in security when its network vulnerability increases. We can use the IDS problem to explain this conclusion. Since the network consisting of the interconnected information systems shows negative externality, the firms in the network are more likely to attempt to offload reliability duties onto other firms when they become more interconnected. In order to solve the IDS problem, besides redefining the trusted interdependence relationship with their partners (for instance, reducing the extent of database access authority or the extent of information sharing) to reduce the network vulnerability, some economic incentives can be designed to internalize the negative externality of information security. We discuss two economic incentives in Section 5.

5. Economic incentives

In Section 4, we have shown that if economic incentives are lacking, an interconnected firm tends to invest less in security as the network vulnerability increases. It would be more attractive to a firm if there are some economic incentives that not only can improve the firm's security level but also can reduce its total expected cost. In this section, we discuss two such effective economic incentives: liability and security information sharing. As a benchmark, we start by characterising the socially optimal welfare. Then we show how to employ the two economic incentives to induce socially optimal welfare.

5.1. Joint decision

To evaluate the investment efficiency, we compare the firms' investments of two economic incentives with the optimal investment level. The optimal investment level is defined as the security investment level when all the firms jointly minimise their total expected costs. We should note the total expected cost of joint decision is also the social whole expected cost in security investment. Thus, the optimal investment level of joint decision is also the optimal investment level of social welfare. The total expected cost of joint decisions is defined as follows[5]:

$$C_J = [p_1 + (1-p_1)qp_2]L + S_1 + [p_2 + (1-p_2)qp_1]L + S_2 \tag{25}$$

Solving this formula can obtain firm 1's optimal investment:

$$S_J^* = p'^{-1}\left(\frac{-1/L}{1+q-2qp(S_J^*)}\right) \tag{26}$$

We now compare the optimal investment of joint decisions with that of individual decisions. Because both attack types satisfy the condition $vt < \frac{1}{2}$, we obtain $\frac{-1/L}{1-qp(S_D^*)} < \frac{-1/L}{1+q-2qp(S_J^*)}$. Hence, we obtain that $S_D^* < S_J^*$, which means the optimal investment of joint decisions is higher than that of individual decisions. Hence the security level of joint decisions is higher than that of individual decisions.

Next we compare the total expected cost of joint decisions with that of individual decisions. Both expressions of total expected cost have the same form, and $\frac{\partial C_D^*}{\partial S_D^*} < 0$ when $L > L_0$, and $S_D^* < S_J^*$, thus we can obtain that $C_J^* < C_D^*$, which means the total expected cost of joint decisions is lower than that of individual decisions.

Next we seek to find whether joint decision can internalize the negative externality of interconnection. We differentiate S_J^* with respect to q to get $\frac{\partial S_J^*}{\partial q} = \frac{p_1'^{-1}(1-2p)}{L(1+q-2qp)^2} > 0$, which means the optimal security investment increases with the network vulnerability for both attack types when firms jointly decide their investments.

We now use a numerical analysis to illustrate the impacts of joint decision on different attack types. We set $v = 0.5, k = 0.000005, 2t^I = t^{II} = 0.5$ and $L^I = 2L^{II} = \$10M$. For *Class I*, the optimal investment of individual decision is \$0.3 **M** and the optimal investment of joint decision is \$0.4 **M**. The percentage of increase in investment relative to the loss is 1%. For *Class II*, the optimal investment of individual decision is \$0.4 **M** and the optimal investment of joint decision is \$1.2 **M**. The percentage of increase in investment relative to the loss is 16%. Thus, the impacts of joint decision on opportunistic attacks are more intensive compare to that on targeted attacks.

Therefore, we can conclude that the optimal investment of joint decision can increase the security level and decrease the total expected cost, as well as internalise the negative externality of network vulnerability. Moreover, firms have more incentives to jointly decide their investments when they mainly face opportunistic instead of targeted attacks.

5.2. Liability

Liability offered by the legal system is an effective way to internalize the negative externality of interconnection (Kunreuther & Heal, 2003). Breaches can be observable for a variety of legal and social reasons. Nowadays firms in the vast majority of the United States—46 states as of October 12, 2010—are legally required to disclose security breaches involving exposure of personal information. For breaches that lead to service disruptions to internal employees and external customers, social word-of-mouth can spread the breach information (Lee, Geng, & Raghunathan, 2013). Thus we assume that breaches can be observable and the legal system can identify whether a breach is direct or indirect. If a firm suffers an indirect breach, the other firm that provides access to attackers should bear the liability and compensate for the damage to the former. We used the parameter λ to denote the intensity of the legal system's punishment, i.e. the portion of liability. Therefore, if firm 1 suffers an indirect breach, firm 2 should compensate firm 1 for the damage of λL and vice versa. Firm 1 can suffer a breach in three ways. First, attackers directly breach firm 1 and then breach firm 2 indirectly via firm 1; this breach probability is given by $p_1q(1-p_2)$. In this scenario, firm 1 should take on both firms' losses; thus, firm 1's expected cost is $(1+\lambda)L \cdot p_1q(1-p_2)$. Second, attackers only breach firm 1 directly and do not breach firm 2 indirectly via firm 1; this breach probability is $p_1 - qp_1(1-p_2)$. In this scenario, firm 1 should only undertake its own loss; thus, firm 1's expected cost is $L \cdot [p_1 - qp_1(1-p_2)]$.

[5] Note that in the following sections, subscript *J* represents the scenario of joint decision. Later, *D*, *L* and *S* represent the scenario of individual decision, liability, and security information sharing, respectively.

Third, attackers breach firm 2 directly and then breach firm 1 indirectly via firm 2, this breach probability is $p_2q(1-p_1)$. In this scenario, firm 1 suffers a loss L and then obtain a compensation from firm 2; thus firm 1's expected cost is $(1-\lambda)L \cdot p_2q(1-p_1)$. Therefore, the total expected cost of firm 1 is

$$C_L = [p_1(1+\lambda q - p_2 q) + p_2 q(1-\lambda)]L + S_1 \tag{27}$$

Solving this formula can obtain firm 1's optimal investment of liability $S_L^* = p'^{-1}\left(\frac{-1/L}{1+(\lambda-p(S_L^*))q}\right)$. Comparing to the optimal investment of individual decisions, we can obtain that $S_D^* < S_L^*$, which means the optimal investment of liability is higher than that of individual decisions. Hence the security level of liability is higher than that of individual decisions.

Next we compare the total expected cost of liability with that of individual decisions. Because the information security investments of symmetric firms are equal, the total expected cost of liability can be expressed as $C_L^* = [p(S_L^*) + p(S_L^*)q - p^2(S_L^*)q]L + S_L^*$. Since $\frac{\partial C_L^*}{\partial S_L^*} < 0$ when $L > L_0$, we can obtain that $C_L^* < C_D^*$, which means the total expected cost of liability is lower than that of individual decisions. Therefore, we can conclude that liability is an effective economic incentive that not only can improve an interconnected firm's security level but also can reduce its total expected cost.

Next we seek to find whether liability can internalize the negative externality of interconnection. We differentiated S_L^* with respect to q to get $\frac{\partial S_L^*}{\partial q} = \frac{(\lambda-p)p_1''^{-1}}{L(1+(\lambda-p)q)^2}$, we obtain that $\frac{\partial S_L^*}{\partial q} > 0$ only when $\lambda > p(S_L^*)$. That is, when $\lambda > p(S_L^*)$, an interconnected firm's optimal security investment increases with the network vulnerability for both attack types. Therefore, the mechanism of liability can internalise the negative externality of interconnection in the information security investment only when the portion of liability is greater than the breach probability.

We now deduce the relationship between the optimal investments with the portion of liability. We note that $\frac{\partial S_L^*}{\partial \lambda} = \frac{qp_1''^{-1}}{L(1+(\lambda-p(S_L^*))q)^2} > 0$, thus the optimal investment of liability increases with the portion of liability. We also get that the firm will underinvest when $\lambda < 1 - 2p(S_J^*) + p(S_L^*)$ and overinvest when $\lambda > 1 - 2p(S_J^*) + p(S_L^*)$. Therefore, the mechanism of liability can make firms overinvest or underinvest in security if the intensity of the legal system's punishment is set improperly.

Proposition 4. For both attack types, liability is an effective economic incentive that not only can improve an interconnected firm's security level but also can reduce its total expected cost. An interconnected firm's optimal investment increases with the network vulnerability once the portion of liability is greater than the breach probability.

Proposition 4 demonstrates that the mechanism of liability is an effective mechanism that can improve the security level, reduce the total expected cost, and internalise the negative externality of network vulnerability. However, the mechanism of liability only internalises the negative externality of interconnection and encourages firms to invest more in security when the portion of liability is greater than the breach probability. In order to overcome the negative externality of interconnection, the legal system should ensure that the portion of liability is greater than the breach probability. But if the punishment intensity is excessive, firms might overinvest in security. As a result, the mechanism of liability will cause misallocation and waste of resources. An appropriate level of punishment intensity needs to be set to appropriately motivate firms and increase the level of social welfare.

After determining the punishment intensity, the next question is how to make the mechanism of liability work. The mechanism of liability is similar to the risk pooling arrangement (RPA). An RPA is a mutual form of insurance organisation in which the policyholders are also the owners (Zhao et al., 2013). Before breaches occur, both firms give the same amount of money to a mutual insurer, like the legal system. Because the breaches can be observable and the legal system can identify whether a breach is direct or indirect, legal system can use the mutual insurance to compensate firms who suffer indirect breaches. For example, both firms give $40,000 to the legal system. If firm 1 suffers a direct breach and firm 2 suffers an indirect breach because of firm 1, and both firms' losses are $30,000. According to the portion of liability (for example, $\lambda = \frac{1}{3}$), firm 1 should compensate firm 2 for $10,000 and the legal system should use the mutual insurance to compensate firm 2 for $20,000. As a result, both firms have remaining $30,000 in the mutual insurance, and firm 1 suffers a loss of $40,000 and firm 2 suffers a loss of $20,000. If firm 2 suffers an indirect breach from firm 1, but firm 1 does not suffer a direct breach, this scenario is a possible case of crime committed by firm 1, and how to solve such a case is outside the scope of this paper. Since identifying the nature of attacks, direct or indirect and assigning blame on the responsible party is difficult in the network environment, we analyse another effective economic incentive: security information sharing.

5.3. Security Information sharing

Sharing information related to computer security breaches and unsuccessful breach attempts is a desirable way of supplementing the technical solutions to security problems for firms (Gordon et al., 2003). Because sharing alliances yield greater benefits in more competitive industries (Gal-Or & Ghose, 2005), the US government has developed many security-based information sharing organisations, such as the CERT Coordination Centre, the Information Sharing Analysis Centres, the Secret Service Electron Crimes Task Force, etc. We discuss the benefit of security information sharing and provide insight into the impact of security information sharing on both attack types in this section.

We follow the formulation of Gordon et al. (2003) in defining security information sharing of information security investment. That is, if a firm shares security information with the other firm, a portion of the former's information security investment will benefit the latter without diminishing (or enhancing) the benefit to the former. Essentially, the intuition is that the disclosure of vulnerabilities in a particular type of security technology by one firm leads the other firm to invest less in that technology or procure a smaller amount of that product. A direct consequence of such security information sharing would be pre-emptive cost savings in technology investment (Gal-Or & Ghose, 2005). For simplify, we make the following assumptions about the security information sharing:

Assumption 4. we assume that if a firm obtain some others' security information that the firm cannot get it freely, the others' security investment will add to the firm's. We also assume that the two firms share security information to each other without the risk of leakage.

We use θ_i to denote the portion of security information that firm i shares with the other firm. In other words, security information sharing by firm i will shift firm j's information security investment by $\theta_i S_i$. Thus, we can rewrite firm 1's total expected cost in this scenario as follows:

$$C_S = [p_1(S_1 + \theta S_2) + (1 - p_1(S_1 + \theta S_2))qp_2(S_2 + \theta S_1)]L + S_1 \tag{28}$$

Solving this formula can obtain firm 1's optimal investment of security information sharing $S_S^* = p'^{-1}(\frac{-1/L}{1+q\theta-(1+\theta)qp(S_S^*)})$. Comparing to the optimal investment of security information sharing and that of individual decisions, we can obtain that $S_D^* < S_S^*$, which means

the optimal investment of security information sharing is higher than that of individual decisions. Hence the security level of security information sharing is higher than that of individual decisions.

Next we compare the total expected cost of security information sharing with that of individual decisions. With $\frac{\partial C_S^*}{\partial \theta} < 0$, $C_S^* = [p_1(S_S^*) + (1 - p_1(S_S^*))qp_2(S_S^*)]L + S_S^*$ is the maximum total expected cost of security information sharing. Given that $\frac{\partial C_D^*}{\partial S_D^*} < 0$ when $L > L_0$, and $S_D^* < S_S^*$, we can obtain that $C_S^* < C_D^*$, which means the total expected cost of security information sharing is lower than that of individual decisions. Therefore, we can conclude that security information sharing is an effective economic incentive that not only can improve an interconnected firm's security level but also can reduce its total expected cost.

Next we seek to find whether security information sharing can internalize the negative externality of interconnection. We differentiate S_S^* with respect to q to get $\frac{\partial S_S^*}{\partial q} = \frac{(\theta(1-p)-p)p_1''^{-1}}{L(1+q\theta-(1+\theta)qp)^2}$. We obtain that $\frac{\partial S_S^*}{\partial q} > 0$ only when $\theta > \frac{p(S_S^*)}{1-p(S_S^*)}$. We define an "effective value" of security information sharing as one in which $\theta_0 = \frac{p(S_S^*)}{1-p(S_S^*)}$, given an information system and its environment. That is, when $\theta > \theta_0$, an interconnected firm's optimal security investment increases with the network vulnerability for both attack types. Therefore, the mechanism of security information sharing can internalise the negative externality of interconnection in the information security investment only when the portion of security information sharing is greater than the "effective value".

We now deduce the relationship between the optimal investments with the portion of security information sharing. We note that $\frac{\partial S_S^*}{\partial \theta} = \frac{(q-qp)p_1''^{-1}}{L(1+q\theta-(1+\theta)qp)^2} > 0$, and $S_S^* = S_D^*$ when $\theta = 0$, and $S_S^* = S_J^*$ when $\theta = 1$. Therefore, the optimal investment increases with the portion of security information sharing, and the optimal investment of security information sharing is equal to the optimal investment of individual decisions if firms do not share security information. If firms share security information completely, the optimal investment of security information sharing is equal to the social optimal investment level.

Proposition 5. For both attack types, security information sharing is an effective economic incentive that not only can improve an interconnected firm's security level but also can reduce its total expected cost. An interconnected firm's optimal investment increases with the network vulnerability only when the portion of security information sharing is greater than an "effective value".

This proposition provides an interconnected firm with inspiration to adopt the mechanism of security information sharing. First, sharing security information is always beneficial and can improve the level of information security as well as reduce the total expected cost. Second, sharing information internalises the negative externality of interconnection and encourages firms to invest more in security only when the portion of security information sharing is greater than the "effective value". Thus, in order to overcome the negative externality of interconnection, some associations like CERT Coordination Centre can play a coordinating role by stipulating that any member has to follow the rule that each member's portion of security information sharing should be greater than the "effective value".

5.4. Numerical analysis

In this section, we conduct a numerical analysis to demonstrate these propositions. Because the numerical analysis of total expected cost is similar to that of the optimal security investment, we only show the latter's numerical analysis. Specifically, we use the following parameters for the numerical analysis (The results are similar when we varied these values):

$v = 0.5, \quad k = 0.000005, \quad 2t^I = t^{II} = 0.8, \quad L^I = 2L^{II} = \$4M,$
$q = \{0.2, 0.4, 0.6, 0.8\}, \quad \lambda = \{0, 0.1, 0.2, \ldots, 1\}, \quad$ and
$\theta = \{0, 0.1, 0.2, \ldots, 1\}.$

Table 2 shows the results for all 40 scenarios. It should be noted that the optimal investment of joint decisions is equal to the optimal investment of individual decisions when the network vulnerability equals zero. Based on the numerical results, the optimal investment of joint decisions is always greater than that of individual decisions, irrespective of attack types, and the optimal security investment of joint decisions increases with the network vulnerability.

We analyse the results via two plots. Because the plots for *Class I* and *II* are similar, we only provide pictures for the former. First, we plot the network vulnerability against the intensity of liability and the optimal investment to compare the mechanisms of joint decision and liability.

Fig. 6 shows that (1) the optimal investment of liability increases with the portion of liability; (2) the optimal investment of liability decreases with the network vulnerability when $\lambda < 0.1$ and increases with the network vulnerability when $\lambda > 0.1$; and (3) the optimal investment of liability is always less than the optimal investment of joint decision when $\lambda < 0.8$ but greater than the optimal investment of joint decision when $\lambda > 0.8$. These three findings verify proposition 4. In this situation, the minimum portion of the liability is 0.1 and the maximum portion of the liability is 0.8 within which the legal system will not cause a waste of resource.

Second we plot the network vulnerability against the portion of security information sharing and the optimal investment to compare the mechanisms of joint decision and security information sharing:

Fig. 7 shows that (1) the optimal investment of security information sharing increases with the portion of security information sharing; (2) the optimal investment of security information sharing decreases with the network vulnerability when $\theta < 0.2$ and increases with the network vulnerability when $\theta > 0.2$; and (3) the lower bound of the optimal investment of security information sharing is the optimal investment of individual decision, and the upper bound of the optimal investment of security information sharing is the optimal investment of joint decisions. These three findings verify proposition 5. In this situation, the "effective value" of security information sharing is equal to 0.2. The negative externality of interconnection can be internalised only when $\theta > 0.2$. Thus associations of security information sharing should stipulate the rule that each member's portion of security information sharing should be greater than 0.2.

6. Extension to three or more firms

In this section we extend the model from two firms to any finite number, N, of firms, where $N > 2$. Consider N symmetric fully interconnected firms, i.e., all firms are directly connected to each other. We use subscript N to denote this extension. For simplicity, we make the following assumption about the case of N firms:

Assumption 5. we only consider the first-order indirect attacks. That is, if more than two indirect attacks occur through firm 1, firm 1 only take the responsible for the first firm that is attacked indirectly. This assumption is reasonable when q is small. More than one sever security breach in a day is not likely to be very common, thus we also assume the loss is unchanged irrespective of the number of breaches. That is, the loss of another indirect attack can be ignored if the firm has already suffered an indirect attack.

Table 2

q	Individual decisions		Joint decisions		Liability		Information sharing	
	T	O	T	O	T	O	T	O
$\lambda = 0\ \theta = 0$								
0.2	1.959	2.855	2.314	3.345	1.959	2.855	1.959	2.855
0.4	1.917	2.759	2.614	3.726	1.917	2.759	1.917	2.759
0.6	1.874	2.652	2.902	4.080	1.874	2.652	1.874	2.652
0.8	1.829	2.530	3.179	4.407	1.829	2.530	1.829	2.530
$\lambda = 0.1\ \theta = 0.1$								
0.2	1.959	2.855	2.314	3.345	2.000	2.916	1.996	2.907
0.4	1.917	2.759	2.614	3.726	2.000	2.888	1.992	2.869
0.6	1.874	2.652	2.902	4.080	2.000	2.857	1.988	2.827
0.8	1.829	2.530	3.179	4.407	2.000	2.824	1.983	2.782
$\lambda = 0.2\ \theta = 0.2$								
0.2	1.959	2.855	2.314	3.345	2.040	2.975	2.032	2.959
0.4	1.917	2.759	2.614	3.726	2.081	3.010	2.065	2.976
0.6	1.874	2.652	2.902	4.080	2.122	3.050	2.098	2.994
0.8	1.829	2.530	3.179	4.407	2.163	3.083	2.132	3.013
$\lambda = 0.3\ \theta = 0.3$								
0.2	1.959	2.855	2.314	3.345	2.080	3.033	2.068	3.009
0.4	1.917	2.759	2.614	3.726	2.160	3.126	2.137	3.080
0.6	1.874	2.652	2.902	4.080	2.240	3.221	2.206	3.152
0.8	1.829	2.530	3.179	4.407	2.319	3.317	2.276	3.228
$\lambda = 0.4\ \theta = 0.4$								
0.2	1.959	2.855	2.314	3.345	2.120	3.090	2.104	3.059
0.4	1.917	2.759	2.614	3.726	2.237	3.238	2.208	3.179
0.6	1.874	2.652	2.902	4.080	2.354	3.385	2.312	3.303
0.8	1.829	2.530	3.179	4.407	2.469	3.530	2.415	3.429
$\lambda = 0.5\ \theta = 0.5$								
0.2	1.959	2.855	2.314	3.345	2.158	3.146	2.140	3.108
0.4	1.917	2.759	2.614	3.726	2.314	3.345	2.278	3.277
0.6	1.874	2.652	2.902	4.080	2.465	3.539	2.415	3.447
0.8	1.829	2.530	3.179	4.407	2.614	3.726	2.551	3.616
$\lambda = 0.6\ \theta = 0.6$								
0.2	1.959	2.855	2.314	3.345	2.197	3.201	2.175	3.157
0.4	1.917	2.759	2.614	3.726	2.388	3.448	2.347	3.372
0.6	1.874	2.652	2.902	4.080	2.574	3.684	2.517	3.584
0.8	1.829	2.530	3.179	4.407	2.754	3.908	2.683	3.792
$\lambda = 0.7\ \theta = 0.7$								
0.2	1.959	2.855	2.314	3.345	2.235	3.254	2.210	3.205
0.4	1.917	2.759	2.614	3.726	2.462	3.547	2.415	3.464
0.6	1.874	2.652	2.902	4.080	2.680	3.822	2.616	3.716
0.8	1.829	2.530	3.179	4.407	2.890	4.078	2.812	3.958
$\lambda = 0.8\ \theta = 0.8$								
0.2	1.959	2.855	2.314	3.345	2.273	3.307	2.245	3.252
0.4	1.917	2.759	2.614	3.726	2.533	3.643	2.482	3.554
0.6	1.874	2.652	2.902	4.080	2.783	3.952	2.713	3.842
0.8	1.829	2.530	3.179	4.407	3.022	4.237	2.937	4.116
$\lambda = 0.9\ \theta = 0.9$								
0.2	1.959	2.855	2.314	3.345	2.311	3.358	2.279	3.300
0.4	1.917	2.759	2.614	3.726	2.605	3.735	2.549	3.641
0.6	1.874	2.652	2.902	4.080	2.884	4.077	2.809	3.963
0.8	1.829	2.530	3.179	4.407	3.150	4.387	3.059	4.265
$\lambda = 1\ \theta = 1$								
0.2	1.959	2.855	2.314	3.345	2.348	3.408	2.314	3.345
0.4	1.917	2.759	2.614	3.726	2.675	3.824	2.614	3.726
0.6	1.874	2.652	2.902	4.080	2.983	4.196	2.902	4.080
0.8	1.829	2.530	3.179	4.407	3.275	4.530	3.179	4.407

In Table 2, all the level of investment should multiply 0.1 M. "T" represents targeted attack, and "O" represents opportunistic attack.

First we discuss the situation of individual decision. The firm 1's total expected cost of individual decision now is:

$$C_{DN} = [1 - (1 - p_1)\prod_{i=2}^{N}(1 - qp_i)]L + S_1 \tag{29}$$

We can yield the optimal security investment of firm 1:

$$S_{DN} = p'^{-1}\left(\frac{-1/L}{(1-qp)^{N-1}}\right) \tag{30}$$

According to the first-order condition w.r.t. L, we get $\frac{\partial S^*_{DN}}{\partial L} = \frac{p_1''^{-1}}{L^2(1-qp)^{N-1}} > 0$, which means in the situation of individual decision, the optimal security investment increases with the potential loss for both attack types when there are N firms.

According to the first-order condition w.r.t. q, we get $\frac{\partial S^*_{DN}}{\partial q} = \frac{-p_1''^{-1}NP}{L(1-qp)^N} < 0$, which means in the situation of individual decision, the optimal security investment decreases with the network vulnerability for both attack types when there are N firms.

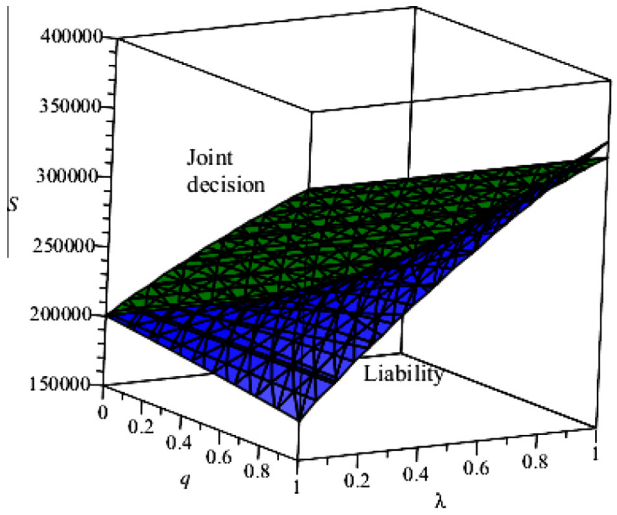

Fig. 6. Comparison between joint decision and liability.

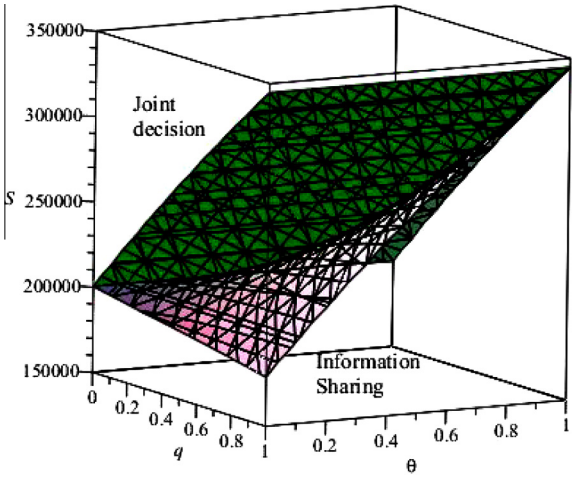

Fig. 7. Comparison between joint decision and security information sharing.

According to the first-order condition w.r.t. N, we get $\frac{\partial S^*_{DN}}{\partial N} = \frac{p_1'^{-1}\ln(1-qp)}{L(1-qp)^{N-1}} < 0$, which means in the situation of individual decision, the optimal security investment decreases with the number of firms for both attack types when there are N firms.

Second we discuss the situation of joint decision. The firm 1's total expected cost of joint decision now is:

$$C_{JN} = \sum_{i=1}^{N}\left[1 - \prod_{j=1}^{N}(1-\eta p_j)\right]L + S_i] \tag{31}$$

where $\eta = \begin{cases} q & i \neq j \\ 1 & i = j \end{cases}$

We can yield the optimal security investment of firm 1:

$$S_{JN} = p'^{-1}\left(\frac{-1/L}{(1-qp)^{N-2}(1+Nq-Npq-q)}\right) \tag{32}$$

According to the first-order condition w.r.t q, we get $\frac{\partial S^*_{JN}}{\partial q} = \frac{p_1'^{-1}}{L}\frac{(N-1)(pq(Np+1-q)+1-2p)}{(1-pq)^{N-1}(Nq(p-1)+q-1)^2} > 0$, which means in the situation of joint decision, the optimal security investment increases with the network vulnerability for both attack types when there are N firms.

According to the first-order condition w.r.t. N, we get $\frac{\partial S^*_{JN}}{\partial N} = \frac{p_1'^{-1}[\ln(1-qp)\bullet(Nq(p-1)+q-1)+qp-q]}{-L(1-qp)^{N-2}(Npq-Nq+q-1)^2}$, $\frac{\partial S^*_{JN}}{\partial N} > 0$ only when $N < \frac{(1-q)\ln(1-qp)+q(1-p)}{\ln(1-qp)\bullet q(p-1)}$, which means in the situation of joint decision, the optimal security investment increases with the number of firms for both attack types only when the number of firms is not too large.

Next we consider the scenario of liability. Similar to the situation of liability with two firms, firm 1 can suffer a breach in three ways. First, attackers directly breach firm 1 and then breach one or $N-1$ firms, firm 1 should take on all breached firms' losses; thus, firm 1's expected cost is $\sum_{i=1}^{N-1}(1+i\lambda)Lp_1q^i(1-p)^i$. Second, attackers only breach firm 1 directly and do not breach any other firms indirectly via firm 1, firm 1 should only undertake its own loss; thus, firm 1's expected cost is $[p_1 - \sum_{i=1}^{N-1}p_1q^i(1-p)^i]L$. Third, attackers breach firm i directly and then breach firm 1 indirectly via firm i, firm 1 suffers a loss L and then obtain a compensation from firm i; because another indirect attack on firm 1 and an indirect attack from an indirect attack can be ignored, firm 1's expected cost is $(1-\lambda)L\cdot p_iq(1-p_1)$. Therefore, the firm 1's total expected cost of liability now is:

$$C_{LN} = \left[\sum_{i=1}^{N-1}[i\lambda p_1q^i(1-p)^i] + p_1 + (1-\lambda)pq(1-p_1)\right]L + S_1 \tag{33}$$

We can yield the optimal security investment of firm 1:

$$S^*_{LN} = p'^{-1}\left(\frac{-1/L}{\sum_{i=1}^{N-1}[i\lambda q^i(1-p)^i] + (\lambda-1)pq + 1}\right) \tag{34}$$

According to the first-order condition w.r.t q, we get $\frac{\partial S^*_{LN}}{\partial q} = \frac{p_1'^{-1}\left[\sum_{i=1}^{N-1}[i^2\lambda q^{i-1}(1-p)^i]+(\lambda-1)p\right]}{L\left[\sum_{i=1}^{N-1}[i\lambda q^i(1-p)^i]+(\lambda-1)pq+1\right]^2}$, we obtain that $\frac{\partial S^*_{LN}}{\partial q} > 0$ only when $\lambda > \frac{p}{\sum_{i=1}^{N-1}[i^2q^{i-1}(1-p)^i]+p}$. That is, in the situation of liability, an interconnected firm's optimal security investment increases with the network vulnerability for both attack types only when the portion of liability is large enough. Therefore, similar to the situation of liability with two firms, when there are N firms, the mechanism of liability can internalise the negative externality of interconnection in the information security investment only when the portion of liability is large enough.

According to the first-order condition w.r.t λ, we get $\frac{\partial S^*_{LN}}{\partial \lambda} = \frac{p_1'^{-1}[\sum_{i=1}^{N-1}[iq^i(1-p)^i]+pq]}{L\left[\sum_{i=1}^{N-1}[i\lambda q^i(1-p)^i]+(\lambda-1)pq+1\right]^2} > 0$, which means in the situation of liability, the optimal security investment increases with the portion of liability for both attack types when there are N firms.

From(34), we can easy find that $\frac{\partial S^*_{LN}}{\partial N} > 0$, which means in the situation of liability, the optimal security investment increases with the number of firms for both attack types.

In the end we discuss the scenario of security information sharing. The firm 1's total expected cost of security information sharing now is:

$$C_{SN} = \left[1 - \prod_{i=1}^{N}\left[1 - \eta p\left(\sum_{j=1}^{N}\omega S_j\right)\right]\right]L + S_1 \tag{35}$$

where $\eta = \begin{cases} q & i \neq 1 \\ 1 & i = 1 \end{cases}$ and $\omega = \begin{cases} \theta & i \neq j \\ 1 & i = j \end{cases}$

We can yield the optimal security investment of firm 1:

$$S^*_{SN} = p'^{-1}\left(\frac{-1/L}{(1-pq)^{N-1} + (N-1)(1-p)q\theta}\right) \tag{36}$$

According to the first-order condition w.r.t q, we get $\frac{\partial S^*_{SN}}{\partial q} = \frac{p_1'^{-1}(1-N)}{L}\frac{p(1-pq)^{N-2} - (1-p)\theta}{[(1-pq)^{N-1} + (N-1)(1-p)q\theta]^2}$, we obtain that $\frac{\partial S^*_{SN}}{\partial q} > 0$ only when

$\theta > \frac{p(1-pq)^{N-2}}{1-p}$. That is, in the situation of security information sharing, an interconnected firm's optimal security investment increases with the network vulnerability for both attack types only when the portion of security information sharing is large enough. Therefore, similar to the situation of security information sharing with two firms, when there are N firms, the mechanism of security information sharing can internalise the negative externality of interconnection in information security investment only when the portion of security information sharing is large enough.

According to the first-order condition w.r.t. θ, we get $\frac{\partial S^*_{SN}}{\partial \theta} = \frac{p_1''^{-1}}{L} \frac{(N-1)(1-p)q}{[(1-pq)^{N-1}+(N-1)(1-p)q\theta]^2}$, we obtain that $\frac{\partial S^*_{SN}}{\partial \theta} > 0$, which means in the situation of security information sharing, the optimal security investment increases with the portion of security information sharing for both attack types when there are N firms.

According to the first-order condition w.r.t N, we get $\frac{\partial S^*_{SN}}{\partial N} = \frac{p_1''^{-1}}{L} \frac{(1-pq)^{N-1}\ln(1-pq)+(1-p)q\theta}{[(1-pq)^{N-1}+(N-1)(1-p)q\theta]^2}$, we obtain that $\frac{\partial S^*_{SN}}{\partial N} > 0$ only when $N > \frac{\ln\frac{(p-1)q\theta}{\ln(1-pq)}}{\ln(1-pq)} + 1$, which means in the situation of security information sharing, the optimal security investment increases with the number of firms for both attack types only when the number of firms is large enough.

Proposition 6. Given three or more firms, for both attack types, both economic incentives are effective to internalize the negative externality of interconnection if their rules are set properly. With increasing number of firms, the optimal investment of liability always increases but the optimal investment of security information sharing increases only when the number of firms is large enough.

Proposition 6 shows that both economic incentives are effective to internalize the negative externality of interconnection if their rules are set properly in the case of three or more firms. That is, the optimal investments of both economic incentives increase with the network vulnerability only when the portion of liability (or the portion of security information sharing) is large enough. In addition, the optimal investments of both economic incentives always increase with the portion of liability (or the portion of security information sharing), regardless of the number of firms. Compared to the case of two firms in Proposition 4 and Proposition 5, Proposition 6 offers some new insights. First, with increasing number of firms, the optimal security investment of individual decision always decreases, the optimal security investment of liability always increases, the optimal security investment of joint decision increases only when the number of firms is not too large, and the optimal security investment of security information sharing increase only when the number of firms is large enough. Second, the portion of liability (or the portion of security information sharing) that can enable both economic incentives to internalize the negative externality of interconnection is decided not only by the breach probability, but also by the number of firms. These findings highlight the importance of adequate assessment of the number of firms' partners, especially for those associations of security information sharing.

7. Conclusions

Although research into the information security has received some attention, economics considerations related to information security investment are rare. The current understanding of the optimal information security investment and the optimal economic incentives for interconnected firms is limited. In this paper, we employ game theory to model the relationship between the optimal information security investment and the characteristics of firms' security environment, and propose two economic incentives to solve the interdependent risk problem. In summary, we have made the following contributions to research. First, we model the optimal information security investments of firms by taking into account the reality that firms face different attack types. We follow prior studies by identifying targeted and opportunistic attacks as two attack types that firms face and provide insights into firms' characteristics to better understand of their behaviours under different scenarios. Second, our model considers the information systems of interconnected firms, which is a more realistic assumption than the individual systems assumed by prior studies. Lastly, our study extends prior studies by discussing two effective economic incentives that not only can internalise the negative externality and improve a firm's security level but also can reduce its total expected cost.

Our results offer some insights into information security management practices.

(1) Not all information security risks are worth fighting against. As the potential loss increases, it is unadvisable to increase the security investment proportionately. A firm is better off not investing in security until the potential loss reaches a certain value for a given attack type. Firms should stop investing in security and adopt other measures when the potential loss is catastrophic. These findings emphasise the importance of adequate assessment of firms' potential loss and identifying the nature of attacks.
(2) A firm should correspondingly increase investment with intrinsic vulnerability when facing targeted attacks while focus on those systems that fall into the midrange of intrinsic vulnerability when facing opportunistic attacks. Since intrinsic vulnerability is decided by the configuration of information system, firms should redefine system configuration that would reduce intrinsic vulnerability rather than invest against opportunistic attacks when the system is in a dangerous- configuration.
(3) Firms are unwilling to invest in security and often offloading reliability problems on others when the trusted interdependence relationship becomes tighter in the absence of economic incentives. When the network vulnerability is less than e^{-2}, the network vulnerability has a stronger impact on a firm's investment when firm faces targeted attacks than facing opportunistic attacks.
(4) The optimal investment of joint decision can increase the security level, decrease the total expected cost, and internalise the negative externality of network vulnerability. Firms have more incentives to jointly decide their investments when they mainly face opportunistic instead of targeted attacks.
(5) In order to solve the prisoner's dilemma in the information security investment game, besides redefining the trusted interdependence relationship with their partners to reduce the network vulnerability, liability and security information sharing, two economic incentives, can be used to internalize the negative externality of information security. We find that if the rules are set properly, both of them can effectively internalise the negative externality, improve a firm's security level, and reduce the total expected cost. For liability, the legal system should enact rules to specify the appropriate portion of liability. The negative externality of interconnection will not be overcome if the portion of liability is too low but overinvestment in security could result if the portion of liability is too high. For security information sharing, associations of security information sharing should stipulate the rule that each member's portion of security information sharing should be greater than an "effective value" in order to overcome the negative externality of interconnection.

(6) Both economic incentives are effective in the case of three or more firms. With more firms, the optimal investment of liability always increases but the optimal investment of security information sharing increases only when the number of firms is large enough. In the case of three or more firms, the effective portion of liability (or the effective portion of security information sharing) is decided not only by the breach probability, but also by the number of firms. These insights draw attention to the many trade-offs firms often face and the importance of accurate assessment of firms' security environment, including potential loss, the nature of attacks, intrinsic vulnerability, network vulnerability and the number of partners. Firms can evaluate these factors by using many methods like the expert grading method and decision tree. For example, Huang, Lin, Lin, and Sun (2013) formulate an analysis model to express the security grades of software vulnerability. Andoh-Baidoo and Osei-Bryson (2007) use decision tree to analyse the observed cumulative abnormal stock market return, which is one measure of the loss of the breached firms.

As with all analytical models, this study has limitations. First, the information security investment game has two participants: firms and hackers. In our analysis, we ignore the behaviour of hackers and only consider the firms' behaviours. Second, we use two breach probability functions to represent targeted and opportunistic attacks, assuming that they are independent of each other. However, targeted and opportunistic attacks may occur simultaneously in the real world, which we do not consider in this study. Our study points to several future directions for research. For instance, this work could be extended by modelling the behaviours between firms and hackers when firms are interconnected and hackers share information. Another interesting research is to design the incentive mechanisms that could encourage firms to decide jointly and share security information, and guide the legal system to stipulate rules to enforce compliance of firms. In addition, information security investments will be different in the situation of multiple breaches, and our work can be extended to include this situation. Lastly, the managerial implications of our findings can be examined with empirical data in a future study.

Acknowledgements

The research presented in this paper is supported by the National Natural Science Foundation Project of China (71390331 & 71390333), the Program for New Century Excellent Talents in University (NCET-13-0460), the National Soft Science Project of China (2014GXS4D151), the Soft Science Project of Shaanxi province (2014KRZ04), and the Fundamental Research Funds for the Central Universities.

References

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*, 610–613.

Andoh-Baidoo, F. K., & Osei-Bryson, K. M. (2007). Exploring the characteristics of Internet security breaches that impact the market value of breached firms. *Expert Systems with Applications, 32*, 703–725.

Casey, E. (2003). Determining intent—opportunistic vs targeted attacks. *Computer Fraud & Security, 2003*, 8–11.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*, 28–46.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems, 25*, 281–304.

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2014). Outsourcing information security: Contracting issues and security implications. *Management Science, 60*, 638–657.

Collins, M. P., Gates, C., & Kataria, G. (2006). A model for opportunistic network exploits: The case of P2P worms. In: *fifth workshop on economic of information security*, Cambridge, England.

Fang, F., Parameswaran, M., Zhao, X., & Whinston, A. B. (2014). An economic mechanism to manage operational security risks for inter-organizational information systems. *Information Systems Frontiers, 16*, 399–416.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research, 16*, 186–208.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*, 438–457.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy, 22*, 461–485.

He, B. Z., Chen, C. M., Su, Y. P., & Sun, H. M. (2014). A defence scheme against Identity Theft Attack based on multiple social networks. *Expert Systems with Applications, 41*, 2345–2352.

Huang, C. D., & Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics, 141*, 255–268.

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a healthcare information exchange: An economic analysis. *Decision Support Systems, 61*, 1–11.

Huang, C. D., Hu, Q., & Behara, R. S. (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.

Huang, C. C., Lin, F. Y., Lin, F. Y. S., & Sun, Y. S. (2013). A novel approach to evaluate software vulnerability prioritization. *Journal of Systems and Software, 86*, 2822–2840.

Hui, K. L., Hui, W., & Yue, W. T. (2012). Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems, 29*, 117–155.

Kim, H. K., Im, K. H., & Park, S. C. (2010). DSS for computer security incident response applying CBR and collaborative response. *Expert Systems with Applications, 37*, 852–870.

Kolfal, B., Patterson, R. A., & Yeo, M. L. (2013). Market impact on IT security spending. *Decision Sciences, 44*, 517–556.

Krebs, B. (2014). Email Attack on vendor set up breach at target. In Krebs on security <http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/#more-24313>.

Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty, 26*, 231–249.

Lee, C. H., Geng, X. J., & Raghunathan, S. (2013). Contracting information security in the presence of double moral hazard. *Information Systems Research, 24*, 295–311.

Ogut, H., Menon, N., & Raghunathan, S. (2005). Cyber insurance and IT security investment: impact of interdependence risk. In: *Fourth workshop on the economics of information security*, Harvard University.

Parker, D. B. (1997). The strategic values of information security in business. *Computers & Security, 16*, 572–582.

Ponemon, I. (2013). 2013 Cost of data breach study: Global Analysis. In: *PGP Corporation*.

PWC (2013). Key findings from the Global State of Information Security Survey 2013.

Richardson, R. (2011). CSI 15th annual computer crime and security survey. *Computer Security Institute (CSI)*.

Straub, D. W. Jr., (1990). Effective IS security: An empirical study. *Information Systems Research, 1*, 255–276.

Straub, D., Goodman, S., & Baskerville, R. (2008). Framing of information security policies and practices. *Information Security Policies, Processes, and Practices*, 5–12.

Varian, H. (2004). System reliability and free riding. In *Economics of information security* (pp. 1–15). Springer.

Wang, J., Chaudhury, A., & Rao, H. R. (2008). A value-at-risk approach to information security investment. *Information Systems Research, 19*, 106–120.

Zhang, Y. J., Deng, X. Y., Wei, D. J., & Deng, Y. (2012). Assessment of E-commerce security using AHP and evidential reasoning. *Expert Systems with Applications, 39*, 3611–3623.

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems, 30*, 123–152.