Inf Syst Front (2015) 17:423–438
DOI 10.1007/s10796-013-9411-3

Security investment and information sharing under an alternative security breach probability function

Xing Gao · Weijun Zhong · Shue Mei

Published online: 23 February 2013

Abstract Nowadays, in order to protect information assets, many firms have gradually realized the importance of security investment and information sharing. It is worth pointing out that security breach probability functions play a vital role in firms' strategic choices. This paper investigates how to determine security investment and information sharing for two firms by employing an alternative well-accepted security breach probability function. In particular, assuming that both firms make their decisions individually, we analyze information sharing, aggregate attack, aggregate defense and the security breach probability at equilibrium. Then we compare these results with those in three (partially) centralized decision cases where a social planner regulates security investment, information sharing or both of them. Between the individual decision case and the partially centralized decision case with the social planner only controlling information sharing, and between the centralized decision case and the other partially centralized decision case, we demonstrate that, although aggregate attack, aggregate defense and the security breach probability remain unchanged, more intervention from the social planner would give rise to higher social welfare. Besides, it turns out that some well-known results of Hausken (Journal of Accounting and Public Policy, 26(6), 639–688, 2007) drastically change in our framework.

Keywords Security investment · Information sharing · Interdependence · Social planner · Security breach probability function

X. Gao (✉) · W. Zhong · S. Mei
School of Economics and Management, Southeast University, Nanjing, Jiangsu, China
e-mail: gxingstar@163.com

1 Introduction

Currently, computers and communication networks are particularly important for many organizations, without which commerce and entertainment as we know would cease to exist. In order to fulfill various requirements, firms' information systems in this electronically networked world have become more and more dynamic, distributed and complex, which facilitates hackers' misappropriation of data resources. As reported by Computer Emergency Response Team (CERT), the number of computer security incidents increased strikingly from 1988 to 2003, shown in Table 1. Even worse, the reported statistics are likely to underestimate the risk of information systems for at least two reasons (D'Arcy et al. 2009). First, many security incidents fail to be discovered due to technological limitations (Whitman 2003). Second, some firms seem very reluctant to disclose such information, since the disclosure will to a certain extent harm their reputation, stock prices (Campbell et al. 2003; Chai et al. 2011), consumer confidence (Gal-Or and Ghose 2005) and market shares (Cavusoglu et al. 2004). In order to reduce the likelihood of serious damages arising from security incidents, many firms usually focus on security technologies, such as firewalls and intrusion detection systems (IDS) (Ulvila and Gaffney 2004; Cavusoglu and Raghunathan 2004; Cavusoglu et al. 2005, 2009). Unfortunately, practitioners and academics gradually realize that it is excessively difficult to achieve an adequately secure environment simply through such technological tools (Hamill et al. 2005). Actually, Zhao et al. (2008) show that the Internet can be viewed as an economic system besides being a set of technology components, which implies that participants' incentives should be paid particular attention to. It is quite consistent with the observation of Anderson and Moore (2006) that security failure is caused at least as often by bad incentives as by bad design. Therefore, a large and growing literature

Table 1 The number of security incidents reported by CERT (http://www.cert.org/stats/cert_stats.html#incidents)

Year	1988	1989	1990	1991	1992	1993	1994	1995
Number	6	132	252	406	773	1,334	2,340	2,412
Year	1996	1997	1998	1999	2000	2001	2002	2003
Number	2,573	2,134	3,734	9,859	21,756	52,658	82,094	137,529

has emerged concerning the economics of information security (Dutta and Mccrohan 2002; Gordon and Loeb 2006; Galbreth and Shor 2010; Hausken 2012; Kshetri 2006, 2009; Kong et al. 2012; Leeson and Coyne 2006; Ryan and Ryan 2006; Young et al. 2007).

Our paper was mainly inspired by Hausken (2007), who provides a lot of crucial insights into security investment and information sharing between two firms by introducing a symmetric contest success function as a security breach probability function in a manner. The contest success function is first used in modeling tournaments, conflicts and rent-seeking, where each participant strives to improve the probability of winning a prize (Skaperdas 1996). Security breach probability functions characterize the likelihood that information sets would be breached, given that firms have made their decisions concerning security investment and information sharing while hackers have launched cyber attacks against these firms. These functions are extremely important in formulating strategic choices for firms and hackers, by which many novel findings have been advanced (Gordon and Loeb 2002; Hausken 2006b; Huang et al. 2008). In Hausken (2007), an underlying assumption is that the efforts between each firm and the hacker are symmetric, which may be insufficient to capture their actual behavior sometimes, since one of them is possibly at an advantage in affecting the security breach probability. Virtually, the asymmetry of participants' efforts in the contest success function has been discussed in the rent-seeking model (Leininger 1993; Clark and Riis 1998). Besides, the asymmetric effects on the security breach probability are also common in reality. For example, if there are many drawbacks in an information system, it can be breached more easily by hackers, implying that hackers' efforts are more effective. On the other hand, one firm's efforts will be more effective in protecting its information system from being breached when there are fewer drawbacks. In consideration of the asymmetry efforts, the purpose of our paper is to further investigate security investment and information sharing under an alternative widely-accepted security breach probability function introduced by Cavusoglu et al. (2008). Moreover, there are still two other distinctive features in our model. For one thing, the security breach probability under discussion takes into account each firm's inherent vulnerability explicitly, which is already widely studied theoretically and empirically as an important factor (Gordon and Loeb 2002; Kannan and Telang 2005; Telang and Wattal 2007; Tanaka et al. 2005; Arora et al. 2006). For another, our model allows the value associated with an information asset to differ between the hacker and the two firms.

This paper, together with Hausken (2007), focuses primarily on information sharing, which has been proved effective in achieving maximal benefit and improving social welfare with lower expenditure (Gordon et al. 2002, 2003a). The governments and many public organizations have fostered some movements toward information sharing between public and private sectors. For example, the U.S. federal government has ever encouraged the establishment of industry-based CERT, Information Sharing and Analysis Centers (ISACs), Electron Crimes Task Forces (ECTFs) and Chief Security Officers Round Tables (CSORTs). In particular, Financial Services-Information Sharing and Analysis Center (FS-ISAC) was founded in 1999 as an industry forum for sharing information about critical security threats facing financial service sectors. Using the shared reliable and timely information from financial services providers, commercial security firms, government agencies, law enforcement and other trusted resources, the FS-ISAC can quickly disseminate physical and cyber threat alerts to member firms to help protect their information systems as soon as possible. Moreover, industry experts analyze the threat to identify recommended solutions, which are also shared among member firms so that they can receive the latest tried-and-true procedures and best practices for guarding against known and emerging security threats. FS-ISAC membership grew from less than one thousand in 2005 to more than four thousand in 2011. However, there are some negative aspects for information sharing such as moral hazard of participating firms (Gal-Or and Ghose 2003), loss of consumer confidence and satisfaction (Gal-Or and Ghose 2005; Lee and Lee 2012), as well as possible reduction in social welfare (Kannan and Telang 2005).

As modern computers and communication networks develop rapidly, the interdependence between firms has been widely stressed (Kunreuther and Heal 2003; Hausken 2009; Heal and Kunreuther 2007; Hare and Goldstein 2010; Zhuang et al. 2007; Zhuang 2010). The interdependent risk, exemplified with baggage scanning between two conjoint airlines and fire precaution between two neighboring sites, strongly emphasizes the effect of contagion. In particular, the interdependence between firms can be illustrated clearly at two

different levels in networked supply chains (Bandyopadhyay et al. 2010). The first level is mutual interconnectivity implicitly through the Internet, by which a hacker could first breach one firm and then reach to other firms more easily. The second level of contagion risk occurs when one firm allocates its partial information asset to other firms. Furthermore, it has already been revealed that there exists positive or negative interdependence of cyber attacks even between countries (Kim et al. 2012; Png et al. 2008). Following such literature, the interdependence is incorporated in our model.

Our analysis points out that when two firms make their choices individually, information sharing is independent of the efficiency of security investment; aggregate attack and aggregate defense increase with the interdependence between the two firms; and aggregate attack decreases with the efficiency of security investment while aggregate defense increases with the efficiency of cyber attacks. It is demonstrated that the security breach probability increases with the related firm's inherent vulnerability, the interdependence, the efficiency of cyber attacks and the hacker's benefit, but decreases with the efficiency of security investment and the related firm's monetary loss. Furthermore, this paper investigates three (partially) centralized decision cases in which security investment, information sharing or both of them would be respectively regulated by a social planner. It turns out that each firm's aggregate attack, aggregate defense and its security breach probability remain unchanged between the individual decision case and the partially centralized decision case with the social planner only controlling information sharing, and between the centralized decision case and the other partially centralized decision case. We finally arrive at a conclusion that the social planner's intervention can always benefit the social welfare between such decision scenarios, whether security investment is chosen individually or centrally.

The remainder of this paper is organized as follows. We begin with a review of relevant literature in Section 2 before describing notations and the model in Section 3. Section 4 presents our main results when the two firms independently choose both security investment and information sharing and simultaneously the hacker chooses cyber attacks. Section 5 highlights changes of information sharing, aggregate defense, aggregate attack, the security breach probability and the social welfare in (partially) centralized decision cases. Section 6 briefly summarizes our findings and provides some future research directions. All proofs are relegated to Appendixes.

2 Literature review

There has been much literature concerning security investment and information sharing in information systems. By a simple decision-theoretic model incorporating inherent vulnerability of one information system and potential loss of one firm, Gordon and Loeb (2002) show that the firm may not necessarily shift its emphasis to such information set with the highest vulnerability. Besides, they demonstrate that the firm invests maximum 37 % of the expected loss from a security breach. Using alternative security breach probability functions, Hausken (2006b) finds that the results of Gordon and Loeb (2002) change. All these findings are confirmed by Anderson and Moore (2006), who suggest that many problems in information security lie in stakeholders' misaligned incentives. Bodin et al. (2005) adopt an analytic hierarchy process to illustrate how to spend limited information security budget most effectively and how to enhance the level of information security. In order to fully characterize relatively rare but extraordinarily critical security failures, Wang et al. (2008) introduce the concept of value-at-risk to quantitatively estimate the value at risk so that a decision-maker is able to make a proper investment choice based on its own risk preference. Besides, some real options techniques have been employed in investigating security investment (Gordon et al. 2003b; Herath and Harath 2009). Nevertheless, the game theory approach seems more appropriate to model the strategic interaction between firms and hackers. As pointed out by Cavusoglu et al. (2008), decision environments should not be treated as static, since firms always deal with strategic hackers seeking opportunities for cyber attacks, while hackers often target vulnerable and poorly-protected systems.

Many investigations have been carried out to discuss security investment and information sharing within the framework of game theory in recent years. In particular, constructing an economically plausible security breach probability function based on Gordon and Loeb (2002), Cavusoglu et al. (2008) show an advantage of the game-theoretic approach over the traditional decision-theoretic approach. Hausken (2006a) studies how firms' security investment is influenced by their interdependence, attackers' income and ability to substitute their efforts between different targets. In consideration of agents' heterogeneous discount rates, Zhuang et al. (2007) develop a security game to reveal that the existence of myopic agents acts as a disincentive for non-myopic agents to invest in system security. Zhuang (2010) obtains that in an n-player game with errors, providing subsidies prone to an erroneous choice could increase the stability of a socially optimum equilibrium and decrease the total social costs. By examining the interaction between attackers and firms, Cremonini and Nizovtsev (2009) conclude that when attackers can substitute their efforts between targets, well-protected targets can use the signal of their superior protection level as a deterrence tool. Liu et al. (2011) find that firms would fully share their information when their information sets are complementary, but not share at all when their information sets are substitutive. Within a

Bertrand duopoly framework, some analytical results are derived by Gal-Or and Ghose (2005), who demonstrate that information sharing is more valuable in competitive industries. Interestingly enough, a differential game approach has already been employed to investigate security investment for competitive firms (Bandyopadhyay et al. 2012). Following these studies, this paper also uses a game-theoretic framework to discuss strategic decisions of security investment and information sharing.

3 The model

3.1 Notation

In this part, most of key elements which occur in our following discussion are collected for convenience.

Parameters:

v_i	the inherent vulnerability for firm i's information system, $0 \le v_i \le 1$, $i=1, 2$
γ	the efficiency of cyber attacks, $\gamma>0$
α	the efficiency of security investment, $\alpha>0$
β	a coefficient ensuring that security investment exhibits a diminishing marginal return, $\beta \ge 1$
ϕ	a coefficient ensuring that cyber attacks exhibit a diminishing marginal return, $0 \le \phi < 1$
η	the efficiency of information sharing, $0<\eta<1$
ρ	the interdependence between firms
L_i	firm i's monetary loss caused by a security breach, $L_i>0$
H_i	the hacker's benefit from firm i's security breach, $H_i>0$
$\kappa_1, \kappa_2, \kappa_3$	nonnegative coefficients of a leakage cost due to information sharing, $\kappa_1 \ge \kappa_2+\kappa_3$.

Decision variables:

z_i	firm i's security investment, $z_i>0$
s_i	firm i's information sharing with firm j, $s_i \ge 0$, $i, j=1, 2$, $i \ne j$
c_i	the hacker's cyber attack against firm i, $c_i>0$.

Functions:

S	the security breach probability function
z_i^a	firm i's aggregate defense
c_i^a	the hacker's aggregate attack against firm i
g_i	firm i's leakage cost due to information sharing
F_i	firm i's expected utility
H	the hacker's expected utility.

3.2 Assumptions

In order to protect its information system from being breached, firm i invests z_i for employing security experts and installing security devices such as firewalls, IDS, antivirus software, virtual private networks (VPN), content filters, access control systems, etc. Assume that firm i shares an amount s_i of information with firm j. The actual security investment firm i can acquire is thus $z_i+\eta s_j$, where $\eta \in (0, 1)$ measures the efficiency of information sharing. That is, η describes the similarity and the compatibility between the two firms' information technology environments (Liu et al. 2011). For example, η would be relatively large when both firms use Windows environments, but relatively small when one firm switches to a Linux operating system. The hacker spends c_i against firm i on a typical cyber attack process such as collecting information about the target's vulnerability, carrying out the attack and finally conducting post attack activity (Cavusoglu et al. 2008). That is, each cyber attack launched by the hacker consists of a learning phase and a standard attack phase. Following Cavusoglu et al. (2008), this paper considers targeted attacks by the hacker such as industrial espionage, denial of service (DoS) and intrusions, but not untargeted attacks such as worms and viruses. Given the contagion effect caused by the interdependence between these firms, firm i can finally get aggregate defense z_i^a and aggregate attack c_i^a

$$z_i^a = z_i + \eta s_j + \rho\left(z_j + \eta s_i\right) \text{ and } \mathrm{c_i^a} = \mathrm{c_i} + \rho \mathrm{c_j}, \mathrm{i}, \mathrm{j} = 1, 2, \mathrm{i} \ne \mathrm{j}. \quad (1)$$

The interdependence ρ can be positive or negative, whose magnitude should be restricted to ensure both z_i^a and c_i^a to be positive and further restricted if necessary. Under positive interdependence, each firm tends to cooperate to form more powerful aggregate defense, but inevitably suffers stronger aggregate attack, since the interdependence will facilitate the hacker's efforts as well. Opposite effects occur for negative interdependence (Hausken 2007).

There are three important elements to characterize firm i's information system, the inherent vulnerability v_i, the monetary loss caused by a security breach L_i, and the security breach probability function $s\left(v_i, z_i^a, c_i^a\right)$. The inherent vulnerability v_i represents the security breach probability without any aggregate defense and any aggregate attack. That is, v_i describes a scenario in which Internet resources are under no protection, thus readily available to the hacker. The information is completely invulnerable when $v_i=0$ and completely vulnerable when $v_i=1$. The monetary loss L_i can be tangible such as the loss of business and the maintenance cost of system failure, or intangible such as the loss in customer trust, reputation and competitiveness. This loss could be caused by a security breach associated with

confidentiality (including the strategic information becoming available to competitors or the fraudulent use of credit card information by the hacker), integrity (including faulty decisions based on data altered by an intruder), or availability (including missed sales from authorized users unallowable for legitimate access due to DoS attacks) (Gordon and Loeb 2002). Given the inherent vulnerability v_i, the security breach probability function $s(v_i, z_i^a, c_i^a)$ depends on aggregate defense z_i^a and aggregate attack c_i^a. More specially, this paper adopts a widely-accepted security breach probability function

$$s(v_i, z_i^a, c_i^a) = v_i(\gamma c_i^a + 1)^{\phi}(\alpha z_i^a + 1)^{-\beta}. \quad (2)$$

Noting that based on Gordon and Loeb (2002), function (2) is presented by Cavusoglu et al. (2008), therefore we refer to (2) as the G-C security breach probability function in our later discussion. Clearly, parameters γ and α measure efficiencies of cyber attacks and security investment respectively. It is necessary to assume that v_i is sufficiently small to ensure that $s(v_i, z_i^a, c_i^a)$ lies between 0 and 1 at equilibrium. Obviously, function (2) satisfies the following fundamental properties

(a) $s(v_i, 0, 0)=v_i$, which accords with the definition of v_i.
(b) $s(0, z_i^a, c_i^a) = 0$, that is, an information system with zero vulnerability is always completely protected for any aggregate defense and any aggregate attack.
(c) $\partial s(v_i, z_i^a, c_i^a)/\partial z_i^a < 0, \partial s(v_i, z_i^a, c_i^a)/\partial c_i^a > 0, \partial^2 s(v_i, z_i^a, c_i^a)/\partial(z_i^a)^2 > 0$ and $\partial^2 s(v_i, z_i^a, c_i^a)/\partial(c_i^a)^2 < 0$, implying that a higher level of aggregate defense (aggregate attack) decreases (increases) the security breach probability with a diminishing marginal return.

3.3 Expected utility

The expected monetary loss of firm i is the product $v_i L_i = s(v_i, 0, 0)L_i$ in the absence of security investment, information sharing and cyber attacks. With firm i's aggregate defense z_i^a, the intended reduction of the security breach probability is $s(v_i, 0, 0) - s(v_i, z_i^a, c_i^a) = v_i - s(v_i, z_i^a, c_i^a)$, which also depends on the hacker's aggregate attack c_i^a. Hence, the net benefit of firm i is given by $[v_i - s(v_i, z_i^a, c_i^a)]L_i - z_i$, where the term $[v_i - s(v_i, z_i^a, c_i^a)]L_i$ describes the intended reduction of firm i's monetary loss attributable to its aggregate defense (Gordon and Loeb 2002; Cavusoglu et al. 2008).

Although information sharing can contribute to the reduction of the security breach probability, it will incur a leakage cost $g_i(s_i, s_j)$ (Gal-Or and Ghose 2005; Pardo et al. 2006). Following Hausken (2007), assume that

$$g_i(s_i, s_j) = \kappa_1 s_i^2 - \kappa_2 s_j^2 - \kappa_3 s_i s_j \text{ with } \kappa_1 \geq \kappa_2 + \kappa_3, \mathrm{i}, \mathrm{j} = 1, 2, \mathrm{i} \neq \mathrm{j}, \quad (3)$$

where nonnegative κ_1, κ_2 and κ_3 respectively denote the inefficiency of firm i's leakage, the efficiency of firm j's leakage and the efficiency of joint leakage. Hence, the expected utility of firm i is given by

$$F_i = [v_i - s(v_i, z_i^a, c_i^a)]L_i - z_i - (\kappa_1 s_i^2 - \kappa_2 s_j^2 - \kappa_3 s_i s_j). \quad (4)$$

Generally speaking, the value attached to an information asset differs between firms and hackers. It is realized by firms through the utilization of the information asset in legal business processes, whereas it is acquired by hackers through the unauthorized use in an unlawful fashion. For example, for a firm storing credit card data of its customers, the value of its information asset is realized when the firm can facilitate its customers' payment process during purchase transactions. However, hackers obtain the value by fraudulent purchase and identity theft (Bandyopadhyay et al. 2012). Hence, it should be noted that firm i's monetary loss caused by a security breach L_i is usually not equal to the hacker's benefit H_i.

Following Cavusoglu et al. (2008), the hacker's benefit from attacking firm i is $[s(v_i, z_i^a, c_i^a) - v_i]H_i$, where $s(v_i, z_i^a, c_i^a) - v_i = s(v_i, z_i^a, c_i^a) - s(v_i, 0, 0)$ is the intended increase in the security breach probability because of the hacker's aggregate attack. Consequently, the expected utility of the hacker takes the form of

$$H = [s(v_1, z_1^a, c_1^a) - v_1]H_1 + [s(v_2, z_2^a, c_2^a) - v_2]H_2 - c_1 - c_2. \quad (5)$$

Obviously, if $s(v_i, z_i^a, c_i^a) < v_i, v_i - s(v_i, z_i^a, c_i^a)$ measures the decrease in the security probability due to aggregate defense. Thus, the hacker must launch a cyber attack to minimize $v_i - s(v_i, z_i^a, c_i^a)$, equivalently, to maximize $s(v_i, z_i^a, c_i^a) - v_i$. Otherwise, if $s(v_i, z_i^a, c_i^a) > v_i, s(v_i, z_i^a, c_i^a) - v_i$ measures the increase in the security probability caused by aggregate attack, which should be minimized by firm i's aggregate defense. In a word, the expected utilities describe the intended reduction in both firms' monetary loss and the intended increase in the hacker's benefit respectively. Therefore, the basic framework of expected utilities discussed above, introduced by Gordon and Loeb (2002) and developed by Cavusoglu et al. (2008), is economically plausible.

4 Equilibrium analysis

In this section, assume that both firms choose their security investment and information sharing while the hacker determines cyber attacks against both firms simultaneously and

independently. Appendix A derives the two firms' information sharing at equilibrium,

$$s_1 = s_2 = \rho\eta(2\kappa_1 - \kappa_3)^{-1}, \tag{6}$$

which are equal to zero for non-positive ρ.

Proposition 1. *Information sharing increases linearly in positive interdependence, and both firms share no information under negative interdependence. Furthermore, information sharing increases with its efficiency under positive interdependence, but never depends on the efficiency of security investment or each firm's inherent vulnerability.*

With an increase in positive interdependence, each rational firm has a stronger incentive to share its information in order to take an advantage for more robust aggregate defense against the external hacker. However, no firm has an incentive to share its information under negative interdependence. Besides, it is obvious that a high risk of leakage inhibits both firms from sharing their information. Hausken (2007) finds that information sharing decreases with the investment efficiency for each firm in his framework, namely the reciprocal of its unit cost. In contrast, we indicate that one firm's information sharing is independent of the investment efficiency. Actually, in the model of Hausken, the investment efficiency takes no influence on the contest-theoretic security breach probability but always benefits these firms. As the investment efficiency increases, i.e. the unit cost of security investment decreases accordingly, one firm reasonably shifts its emphasis from information sharing to security investment in order to maintain its aggregate defense with a low cost as possible. However, different from the contest success function, an increase in the investment efficiency makes each firm's information system more difficult to be breached under the G-C security breach probability function, and thus the hacker would launch a stronger cyber attack. Therefore, in order to protect their information systems, both firms may not necessarily share less information.

There have already been extensive studies concerning the relationship between security investment and the inherent vulnerability (Gordon and Loeb 2002; Tanaka et al. 2005). Nevertheless, to our knowledge it hasn't been discussed so far whether or not the inherent vulnerability affects firms' incentives to share their information. As a matter of fact, in credit markets, bank industry's average inherent vulnerability, arising from either inappropriate management mechanism or defective software design, may differ between developed and developing countries. However, in all these countries, bank industries usually seem willing to share their credit information (Büyükkarabacak and Valev 2012; Kallberg and Udell 2003; Hahm and Lee 2011; Zhang 2011), which accords with the result of proposition 1 that information sharing is independent of the inherent vulnerability.

Firm 1's aggregate attack and aggregate defense are given as follows by Appendix A,

$$c_1^a = \gamma^{-1}\left(v_1 L_1^{-\beta} H_1^{1+\beta}(\alpha\beta)^{-\beta}[\gamma\phi(1+\rho)]^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}} - \gamma^{-1}, \tag{7}$$

$$z_1^a = \alpha^{-1}\left(v_1 L_1^{1-\phi} H_1^{\phi}(\alpha\beta)^{1-\phi}[\gamma\phi(1+\rho)]^{\phi}\right)^{\frac{1}{1+\beta-\phi}} - \alpha^{-1}. \tag{8}$$

In what follows, without particular indications we only use firm 1's equilibrium to illustrate our main results, since firm 2's equilibrium can be obtained just by altering subscripts.

Proposition 2.

(i) *Both aggregate attack and aggregate defense increase with the interdependence.*
(ii) *Aggregate attack decreases with the efficiency of security investment, while aggregate defense increases with the efficiency of cyber attacks.*
(iii) *Aggregate attack increases with the hacker's benefit and decreases with the firm's monetary loss, while aggregate defense increases with both the hacker's benefit and the firm's monetary loss.*

Using the G-C security breach probability function, we obtain that an increase in the interdependence between both firms makes aggregate attack and aggregate defense much stronger. Intuitively, as the interdependence increases, the hacker realizes that a cyber attack launched against one firm will become much weaker due to this firm's stronger aggregate defense. Besides, a higher level of interdependence will enhance aggregate attack, thus the hacker would like to increase its cyber attack. These results are different from Hausken (2007), who shows that dependent on the investment efficiency, aggregate attack sometimes increases with the interdependence but sometimes decreases. The underlying reason is that the investment efficiency in this paper also characterizes the efficiency of aggregate defense.

At first glance, it seems difficult to understand that aggregate attack decreases with the investment efficiency while aggregate defense increases with the attack efficiency. As the investment efficiency increases, each firm will afford a higher level of investment to increase its aggregate defense. Thus, the hacker has to improve its cyber attack to achieve a competitive advantage, resulting in an increase in aggregate attack. On the other hand, as the attack efficiency increases, both firms become unwilling to make a higher level of security investment due to the consideration of an enormously high budget. This finding is consistent with the observation that technical requirements structurally favor attack over defense (Anderson 2001, 2002). This signifies the great reality that while firms must attempt to plug all

holes in vulnerable information assets, one hacker does well just by finding and exploiting one poorly-protected vulnerability. The technical bias in favor of attack is made even worse for a large number of low-probability bugs. By Anderson (2002), one firm's information system with 10^6 bugs each with a mean time before failure (MTBF) of 10^9h will have an MTBF of 1,000 h, which implies that the firm who spends even a million hours has very little chance to find that particular bug before a hacker exploits it. It follows from proposition 2 (iii) that each firm's monetary loss and the hacker's benefit have asymmetric influences on aggregate attack and aggregate defense. More particularly, as each firm's monetary loss increases, aggregate attack decreases and aggregate defense increases. But as the hacker's benefit increases, both aggregate attack and aggregate defense increase. That is, both firms care more about the hacker's strategic behavior and seem somewhat passive for their interaction with the hacker.

Substituting (7) and (8) into (2) yields

$$s\left(v_1, z_1^a, c_1^a\right) = \left(v_1 L_1^{-\beta} H_1^{\phi} (\alpha\beta)^{-\beta} [\gamma\phi(1+\rho)]^{\phi}\right)^{\frac{1}{1+\beta-\phi}}. \tag{9}$$

Proposition 3. *The G-C security breach probability function increases with the related firm's inherent vulnerability, the interdependence, the efficiency of cyber attacks and the hacker's benefit, but decreases with the efficiency of security investment and the firm's monetary loss.*

The hacker launches a stronger cyber attack as either the attack efficiency or its benefit increases, implying that the security breach probability increases. Similarly, an increase in the investment efficiency or the related firm's monetary loss leads to larger security investment and further higher aggregate defense, which yields a decrease in the security breach probability. Obviously, a higher inherent vulnerability gives rise to a higher probability of security breach since the hacker is able to gain access to each firm's information asset more easily. The G-C security breach probability increases with aggregate attack and decreases with aggregate defense, and both of them increase with the interdependence by proposition 2. Noticing that given efficiency parameters being equal the effect of aggregate attack is more remarkable than that of aggregate defense, we can conclude that the probability of security breach always increases with the interdependence as a result.

Policy advice 1. Both firms should share more security information with each other as the interdependence or the sharing efficiency increases, or sharing cost decreases. The interdependence is a double-edged sword, which serves as a positive factor for both aggregate defense and aggregate attack. Aggregate attack decreases with the investment efficiency and the related firm's monetary loss, and increases with the hacker's benefit. On the other hand, aggregate defense increases with the attack efficiency, the hacker's benefit and the related firm's monetary loss. The probability of security breach increases with the related firm's inherent vulnerability, the interdependence, the attack efficiency and the hacker's benefit, but decreases with the investment efficiency and the related firm's monetary loss.

5 The (partially) centralized decision cases

With the establishment of some organizations concerning information sharing such as ISACs, CERT and CSORTs, firms' decisions may be made in a (partially) centralized fashion. In this section, we analyze how these firms and the hacker interact when the social planner is able to regulate security investment, information sharing, or both of them respectively. Naturally, the purpose of the social planner is to maximize the overall expected utility,

$$\begin{aligned} F = &\left[v_1 - s\left(v_1, z_1^a, c_1^a\right)\right] L_1 + \left[v_2 - s\left(v_2, z_2^a, c_2^a\right)\right] L_2 \\ &- z_1 - z_2 - g_1(s_1, s_2) - g_2(s_2, s_1). \end{aligned} \tag{10}$$

5.1 Equilibrium comparisons

We mainly focus on each firm's information sharing, aggregate attack, aggregate defense as well as the security breach probability at equilibrium. Table 2 can be derived from Appendix B in which only security investment is controlled by the social planner.

Proposition 4. *In the partially centralized decision case where just security investment is chosen by the social planner,*

(i) *each firm's information sharing is not higher than the individual optimum;*
(ii) *under positive (negative) interdependence, each firm's aggregate attack is smaller (larger) than the individual optimum, while aggregate defense is larger (smaller) than the individual optimum;*
(iii) *under positive (negative) interdependence, each firm's security breach probability is smaller (larger) than the individual optimum.*

In order to apprehend proposition 4 (i), note that

$$\begin{aligned} \frac{\partial F}{\partial z_1} &= \frac{\partial F_1}{\partial z_1} + \frac{\partial F_2}{\partial z_1} = \frac{\partial F_1}{\partial z_1} - \frac{\partial s\left(v_2, z_2^a, c_2^a\right)}{\partial z_1} L_2 \\ &= \frac{\partial F_1}{\partial z_1} - \frac{\partial s\left(v_2, z_2^a, c_2^a\right)}{\partial z_2^a} \rho L_2, \end{aligned} \tag{11}$$

Table 2 The social planner controls security investment

Information sharing	$s_1 = s_2 = \rho\eta[(1+\rho)(2\kappa_1 - \kappa_3)]^{-1}$
Aggregate attack	$c_1^a = \gamma^{-1}\left(v_1 L_1^{-\beta} H_1^{1+\beta}(1+\rho)(\alpha\beta)^{-\beta}(\gamma\phi)^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}} - \gamma^{-1}$
Aggregate defense	$z_1^a = \alpha^{-1}\left(v_1 L_1^{1-\phi} H_1^{\phi}(1+\rho)(\alpha\beta)^{1-\phi}(\gamma\phi)^{\phi}\right)^{\frac{1}{1+\beta-\phi}} - \alpha^{-1}$
The G-C security breach probability	$s(v_1, z_1^a, c_1^a) = \left(v_1 L_1^{-\beta} H_1^{\phi}(1+\rho)^{\phi-\beta}(\alpha\beta)^{-\beta}(\gamma\phi)^{\phi}\right)^{\frac{1}{1+\beta-\phi}}$

which implies that under positive interdependence, an increase in each firm's security investment always gives rise to a larger enhancement in the expected utility for the social planner. Therefore, the social planner would afford less information sharing than the individual optimum to maintain each firm's aggregate defense. Under positive interdependence, security investment chosen by the social planner becomes more effective. In this partially centralized decision case, aggregate defense, strongly dependent on security investment, is thus larger than the individual optimum under positive interdependence. The hacker, in a weaker position, would launch a smaller cyber attack than the individual optimum. Consequently, each firm's security breach probability declines under positive interdependence. Hausken (2007) neglects such comparisons due to the complexity. Since Eq. (11) is valid for all economically plausible security breach probability functions and leakage cost functions, our results seem somewhat robust.

One can easily obtain Table 3 from Appendix C when just information sharing is recommended by the social planner.

The following proposition is obvious.

Proposition 5. *In the partially centralized decision case where only information sharing is chosen by the social planner,*

(i) *each firm's information sharing is always higher than the partially centralized optimum with the social planner only controlling security investment, and higher than the individual optimum;*

(ii) *each firm's aggregate attack, aggregate defense and further its security breach probability are equal to the individual optimums.*

It can be easily validated that

$$\frac{\partial F}{\partial s_1} = \frac{\partial F_1}{\partial s_1} + \frac{\partial F_2}{\partial s_1} = \frac{\partial F_1}{\partial s_1} - \frac{\partial s(v_2, z_2^a, c_2^a)}{\partial z_2^a}\eta L_2 \qquad (12)$$

$$-\frac{\partial g_2(s_2, s_1)}{\partial s_1} > \frac{\partial F_1}{\partial s_1},$$

since $\partial g_2(s_2, s_1)/\partial s_1 < 0$ (a basic assumption for a leakage cost (Hausken 2007)). Information sharing is more effective in this partially centralized decision case than in two other decision cases described above. Therefore, the social planner would dictate higher information sharing, whether the interdependence is positive or negative. Even so, each firm's aggregate attack and aggregate defense remain unchanged between this partially centralized decision case and the individual decision case, since derivatives of the hacker's expected utility over cyber attacks and derivatives of the firm's expected utility over security investment would be the same for such decision cases. As a result, the security breach probability, dependent on each firm's aggregate attack and aggregate defense, remains unchanged. Proposition 5 shows that Hausken's related results are robust to a different security breach probability function. Equation (12) is always valid for all reasonable forms of the security breach probability and the leakage cost, which implies that proposition 5 would hold for more general models.

We are in a position to discuss the third case in which the social planner imposes both security investment and information sharing. The following Table 4 can be obtained from Appendix D.

Proposition 6. *In the centralized decision case where both security investment and information sharing are chosen by the social planner,*

(i) *each firm's information sharing is always higher than the partially centralized optimum with the social planner only controlling security investment, and always higher than the individual optimum, but higher than the other partially centralized optimum with the social planner simply controlling information sharing if and only if the interdependence is negative;*

(ii) *each firm's aggregate attack, aggregate defense and further its security breach probability are equal to the partially centralized optimums with the social planner only choosing security investment.*

Table 3 The social planner controls information sharing

Information sharing	$s_1 = s_2 = \eta(1+\rho)[2(\kappa_1 - \kappa_2 - \kappa_3)]^{-1}$
Aggregate attack	$c_1^a = \gamma^{-1}\left(v_1 L_1^{-\beta} H_1^{1+\beta}(\alpha\beta)^{-\beta}[\gamma\phi(1+\rho)]^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}} - \gamma^{-1}$
Aggregate defense	$z_1^a = \alpha^{-1}\left(v_1 L_1^{1-\phi} H_1^{\phi}(\alpha\beta)^{1-\phi}[\gamma\phi(1+\rho)]^{\phi}\right)^{\frac{1}{1+\beta-\phi}} - \alpha^{-1}$
The G-C security breach probability	$s(v_1, z_1^a, c_1^a) = \left(v_1 L_1^{-\beta} H_1^{\phi}(\alpha\beta)^{-\beta}[\gamma\phi(1+\rho)]^{\phi}\right)^{\frac{1}{1+\beta-\phi}}$

Table 4 The social planner controls both security investment and information sharing

Information sharing	$s_1 = s_2 = \eta[2(\kappa_1 - \kappa_2 - \kappa_3)]^{-1}$
Aggregate attack	$c_1^a = \gamma^{-1}\left(v_1 L_1^{-\beta} H_1^{1+\beta}(1+\rho)(\alpha\beta)^{-\beta}(\gamma\phi)^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}} - \gamma^{-1}$
Aggregate defense	$z_1^a = \alpha^{-1}\left(v_1 L_1^{1-\phi} H_1^{\phi}(1+\rho)(\alpha\beta)^{1-\phi}(\gamma\phi)^{\phi}\right)^{\frac{1}{1+\beta-\phi}} - \alpha^{-1}$
The G-C security breach probability	$s(v_1, z_1^a, c_1^a) = \left(v_1 L_1^{-\beta} H_1^{\phi}(1+\rho)^{\phi-\beta}(\alpha\beta)^{-\beta}(\gamma\phi)^{\phi}\right)^{\frac{1}{1+\beta-\phi}}$

It turns out that information sharing does not rely on the interdependence when both security investment and information sharing are specified by the social planner. The previous discussion can account for why information sharing in this centralized decision case is higher than in the individual decision case and in the partially decision centralized case with the social planner only controlling security investment. By Eq. (11), security investment is more effective for each firm in the partially centralized case with the social planner just choosing information sharing than in the centralized case provided that the interdependence between the two firms is negative. Therefore, both firms will invest more in this partially centralized decision case and further share less to maintain its aggregate defense under negative interdependence. It follows from proposition 6 (ii) that an additional control of information sharing makes no influence on aggregate defense and aggregate attack when the social planner enforces security investment. Actually, if security investment is controlled by the social planner, aggregate defense and aggregate attack can be obtained just by equating derivatives of the overall expected utility over security investment to zero and equating derivatives of the hacker's expected utility over cyber attacks to zero, both of which are independent of decision modes of information sharing. That is, aggregate defense and aggregate attack are determined as long as the fashion to choose security investment is given. Besides, although derived in our particular model, proposition 6 (ii) can be extended to other cases with general security breach probability functions and leakage cost functions.

Policy advice 2. Each firm should realize that aggregate attack, aggregate defense and further the security breach probability remain unchanged between the individual decision case and the partially centralized decision case with the social planner just controlling information sharing, and between the centralized decision case and the other partially centralized decision case.

5.2 Welfare analysis

In this subsection, assume that the inherent vulnerabilities, the potential monetary loss of the two firms and the benefits of the hacker are symmetric, i.e., $v_1=v_2=v$, $L_1=L_2=L$ and $H_1=H_2=H$. Hence, both firms share the same expected utility whether or not the social planner intervenes, which implies that the social welfare, described by (10), will be completely determined by each firm's expected utility. Hence, we use each firm's expected utility to measure the social welfare for simplicity. Removing variables' subscripts in this symmetric case, we can obtain each firm's expected utility

$$F_s = [v - s(v, z^a, c^a)]L - [z^a/(1+\rho) - \eta s] - (\kappa_1 - \kappa_2 - \kappa_3)s^2 \tag{13}$$

where $z=z^a/(1+\rho)-\eta s$ denotes the firm's security investment.

Denoting two different levels of information sharing by s_A and s_B, we can obtain

$$\eta s_A - (\kappa_1 - \kappa_2 - \kappa_3)s_A^2 - \left[\eta s_B - (\kappa_1 - \kappa_2 - \kappa_3)s_B^2\right] = (s_A - s_B)[\eta - (\kappa_1 - \kappa_2 - \kappa_3)(s_A + s_B)].$$

Since

$$\eta - (\kappa_1 - \kappa_2 - \kappa_3)\{\eta\rho/(2\kappa_1 - \kappa_3) + \eta(1+\rho)/[2(\kappa_1 - \kappa_2 - \kappa_3)]\} = \eta[(2\kappa_1 - \kappa_3) - (4\kappa_1 - 2\kappa_2 - 3\kappa_3)\rho]/[2(2\kappa_1 - \kappa_3)] > 0 \tag{14}$$

for some appropriate interdependence satisfying

$$\rho < (2\kappa_1 - \kappa_3)/(4\kappa_1 - 2\kappa_2 - 3\kappa_3)(> 0),$$

and

$$\eta - (\kappa_1 - \kappa_2 - \kappa_3)\{\rho\eta/[(1+\rho)(2\kappa_1 - \kappa_3)] + \eta/[2(\kappa_1 - \kappa_2 - \kappa_3)]\} = \eta[(2\kappa_1 - \kappa_3) + (2\kappa_2 + \kappa_3)\rho]/[2(1+\rho)(2\kappa_1 - \kappa_3)] > 0, \tag{15}$$

proposition 7 follows immediately for the symmetric case from proposition 5 and proposition 6.

Proposition 7.

(i) *If both firms choose their security investment, the social welfare when the social planner controls information sharing is higher than when both firms choose their information sharing.*

(ii) *If the social planner controls both firms' security investment, the social welfare when the social planner controls information sharing is higher than when both firms choose their information sharing.*

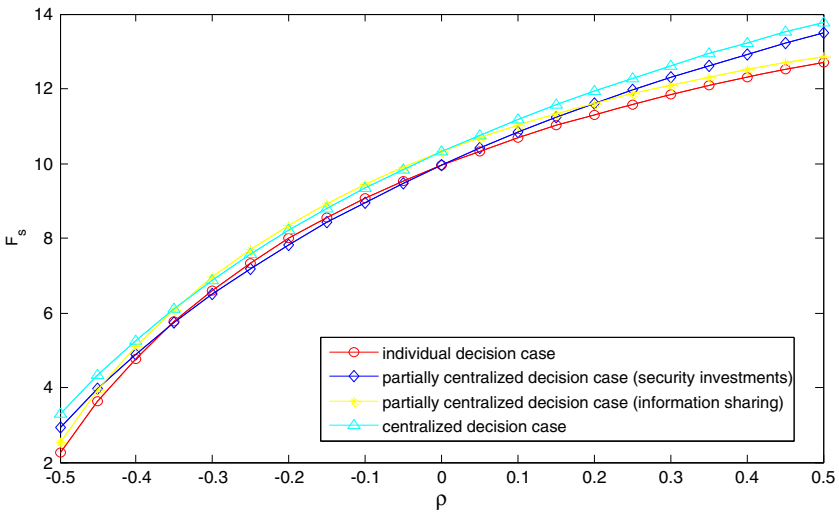

Fig. 1 Each firm's expected utilities with interdependence

When security investment is determined individually, aggregate defense, aggregate attack and further the security breach probability would remain unchanged no matter who chooses information sharing. Although the leakage cost when the social planner controls information sharing is larger than in the absence of the social planner, security investment in the former decision case, more heavily influencing the social welfare, is larger than in the latter. Consequently, each firm desires the social planner to control information sharing, which provides an advantage in its expected utility under appropriate interdependence. Also, a similar analysis shows that when the social planner controls security investment, each firm can get a larger expected utility if information sharing is chosen centrally, as described by proposition 7 (ii).

In order to compare social welfare in all four cases above, we must resort to a numerical example. Let v=0.6, γ=20, ϕ=0.2, α=0.2, β=1.5, L=50, H=20, η=0.95,

κ_1=2.1, κ_2=0.5, κ_3=1, and each firm's expected utility can be obtained in Fig. 1. It can be found that dependent on the interdependence, welfare comparisons between other cases seem very complex. Particularly speaking, although the centralized decision case can give rise to the largest social welfare in a wide range of interdependence, the partially centralized decision case with the social planner only controlling information sharing sometimes can also lead to the largest social welfare. Besides, it is possible that the social welfare in this partially centralized decision case is smaller than in the other partially centralized decision case with the social planner only choosing security investment.

Policy advice 3. Given that both firms determine their security investment, they are willing to choose information sharing centrally rather than individually. On the other hand, when the social planner regulates security investment, it is still better for the social planner to specify information sharing.

6 Conclusions

The security breach probability function is one of the most important factors to investigate the issue of information security. In this paper, employing an alternative widely-accepted security breach probability function (Cavusoglu et al. 2008), we further discuss security investment and information sharing for two firms which are suffering cyber attacks from one hacker. Different from Hausken (2007), our model incorporates each firm's inherent vulnerability, the potential monetary loss as well as the hacker's benefit from attacking. More importantly, efficiencies of security investment and cyber attacks are characterized by their asymmetric effects on the security breach probability, not by related unit costs.

When both firms choose security investment and information sharing individually, we demonstrate that information sharing is independent of the efficiency of security investment, while Hausken (2007) shows that information sharing decreases with this efficiency. Besides, we indicate that aggregate attack and aggregate defense increase with the interdependence between the two firms. Meanwhile, we find that aggregate attack decreases with the efficiency of security investment while aggregate defense increases with the efficiency of cyber attacks. Our results form a striking contrast to those by Hausken (2007), in which these relationships are ambiguous. In addition, we show that the security breach probability increases with the related firm's inherent vulnerability, the interdependence, the efficiency of cyber attacks and the hacker's benefit, but decreases with

the efficiency of security investment and the related firm's monetary loss.

We next discuss three situations where both firms' security investment and information sharing are determined in three (partially) centralized scenarios. Some novel results also follow. For example, with an alternative consideration that security investment is regulated by the social planner, Hausken (2007) shows that the change of information sharing relies upon a complex parameter setting including the efficiency of security investment, the leakage cost and the interdependence. In contrast, we argue that information sharing is not higher than the individual optimum. We reveal that each firm's aggregate attack, aggregate defense and its security breach probability remain unchanged between the individual decision case and the partially centralized decision case with the social planner only controlling information sharing, and between the centralized decision case and the other partially centralized decision case. We finally compare social welfare among these decision modes. It turns out that whether security investment is specified individually or centrally, the social planner's intervention always contributes to the social welfare between such decision cases.

In spite of these insights, there still exist some limitations in our study. First, unlike the work of Hausken (2007), due to the difference between security breach probability functions it is extremely complex to consider two-period games where the social planner moves before both firms and the hacker. Second, since the security breach probability function is foundational and important in modeling strategic interaction, it has remained unknown whether our results still hold for other particular functions. Third, we assume that both firms and the hacker are risk-neutral, but sometimes they may have different risk profiles (Huang et al. 2008). Fourth, an empirical investigation is necessary to validate our theoretic results.

Some interesting research directions are worth further investigation. For example, following Gal-Or and Ghose (2005), one can compare security investment and information sharing when both firms are engaged in price or quantity competition (Gao et al. 2012a). Besides, given a population of hackers, it is interesting to examine security investment when different types of hackers (value-seeking and opportunistic) switch according to some evolutionary dynamics (Bandyopadhyay et al. 2012; Gao et al. 2012b; Mookerjee et al. 2011).

Acknowledgments We wish to thank anonymous referees for constructive and informative comments that helped substantially improve the presentation of this manuscript. Financial supports from the National Natural Science Foundation of China (71071033) and the National Pillar Program of China (2012BAH29F01) are gratefully acknowledged.

Appendix A. Firms choose security investment and information sharing

The firm's and the hacker's expected utilities are respectively

$$F_1 = \left[v_1 - s\left(v_1, z_1^a, c_1^a\right)\right]L_1 - z_1 - \left(\kappa_1 s_1^2 - \kappa_2 s_2^2 - \kappa_3 s_1 s_2\right)$$
$$F_2 = \left[v_2 - s\left(v_2, z_2^a, c_2^a\right)\right]L_2 - z_2 - \left(\kappa_1 s_2^2 - \kappa_2 s_1^2 - \kappa_3 s_1 s_2\right)$$
$$H = \left[s\left(v_1, z_1^a, c_1^a\right) - v_1\right]H_1 + \left[s\left(v_2, z_2^a, c_2^a\right) - v_2\right]H_2 - c_1 - c_2$$

where $s\left(v_1, z_1^a, c_1^a\right) = v_1\left(\gamma c_1^a + 1\right)^{\phi}\left(\alpha z_1^a + 1\right)^{-\beta}$, $s\left(v_2, z_2^a, c_2^a\right) = v_2\left(\gamma c_2^a + 1\right)^{\phi}\left(\alpha z_2^a + 1\right)^{-\beta}$, ${c_1}^a = c_1 + \rho c_2$, $z_1^a = z_1 + \eta s_2 + \rho(z_2 + \eta s_1)$ and ${c_2}^a = c_2 + \rho c_1$, $z_2^a = z_2 + \eta s_1 + \rho(z_1 + \eta s_2)$.

The first order conditions are given by

$$\begin{aligned}\partial F_1/\partial z_1 &= \alpha\beta v_1 L_1\left(\gamma c_1^a + 1\right)^{\phi}\left(\alpha z_1^a + 1\right)^{-\beta-1} - 1 = 0\\ \partial F_2/\partial z_2 &= \alpha\beta v_2 L_2\left(\gamma c_2^a + 1\right)^{\phi}\left(\alpha z_2^a + 1\right)^{-\beta-1} - 1 = 0\end{aligned} \tag{A1}$$

$$\begin{aligned}\partial F_1/\partial s_1 &= \alpha\beta v_1 L_1\rho\eta\left(\gamma c_1^a + 1\right)^{\phi}\left(\alpha z_1^a + 1\right)^{-\beta-1}\\ &\quad - 2\kappa_1 s_1 + \kappa_3 s_2 = 0\\ \partial F_2/\partial s_2 &= \alpha\beta v_2 L_2\rho\eta\left(\gamma c_2^a + 1\right)^{\phi}\left(\alpha z_2^a + 1\right)^{-\beta-1}\\ &\quad - 2\kappa_1 s_2 + \kappa_3 s_1 = 0\end{aligned} \tag{A2}$$

$$\begin{aligned}\partial H/\partial c_1 &= \gamma\phi v_1 H_1\left(\gamma c_1^a + 1\right)^{\phi-1}\left(\alpha z_1^a + 1\right)^{-\beta}\\ &\quad + \rho\gamma\phi v_2 H_2\left(\gamma c_2^a + 1\right)^{\phi-1}\left(\alpha z_2^a + 1\right)^{-\beta} - 1 = 0\\ \partial H/\partial c_2 &= \gamma\phi v_2 H_2\left(\gamma c_2^a + 1\right)^{\phi-1}\left(\alpha z_2^a + 1\right)^{-\beta}\\ &\quad + \rho\gamma\phi v_1 H_1\left(\gamma c_1^a + 1\right)^{\phi-1}\left(\alpha z_1^a + 1\right)^{-\beta} - 1 = 0\end{aligned} \tag{A3}$$

Substituting (A1) into (A2) yields

$$s_1 = s_2 = \rho\eta(2\kappa_1 - \kappa_3)^{-1}.$$

(A3) gives

$$\begin{aligned}&\gamma\phi v_1 H_1\left(\gamma c_1^a + 1\right)^{\phi-1}\left(\alpha z_1^a + 1\right)^{-\beta}\\ &= \gamma\phi v_2 H_2\left(\gamma c_2^a + 1\right)^{\phi-1}\left(\alpha z_2^a + 1\right)^{-\beta} = (1+\rho)^{-1}\end{aligned} \tag{A4}$$

which, together with (A1), implies

$$\begin{aligned}\gamma c_1^a+1&=\left(v_1L_1^{-\beta}H_1^{1+\beta}(\alpha\beta)^{-\beta}[\gamma\phi(1+\rho)]^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\\ \gamma c_2^a+1&=\left(v_2L_2^{-\beta}H_2^{1+\beta}(\alpha\beta)^{-\beta}[\gamma\phi(1+\rho)]^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\end{aligned}\tag{A5}$$

$$\begin{aligned}\alpha z_1^a+1&=\left(v_1L_1^{1-\phi}H_1^{\phi}(\alpha\beta)^{1-\phi}[\gamma\phi(1+\rho)]^{\phi}\right)^{\frac{1}{1+\beta-\phi}}\\ \alpha z_2^a+1&=\left(v_2L_2^{1-\phi}H_2^{\phi}(\alpha\beta)^{1-\phi}[\gamma\phi(1+\rho)]^{\phi}\right)^{\frac{1}{1+\beta-\phi}}\end{aligned}\tag{A6}$$

It follows from (A4) and (A5) that

$$\begin{aligned}c_1&=\left((\alpha\beta)^{-\beta}[\gamma\phi(1+\rho)]^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\left[\left(v_1L_1^{-\beta}H_1^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}-\rho\left(v_2L_2^{-\beta}H_2^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\right][\gamma(1-\rho^2)]^{-1}-[\gamma(1+\rho)]^{-1}\\ c_2&=\left((\alpha\beta)^{-\beta}[\gamma\phi(1+\rho)]^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\left[\left(v_2L_2^{-\beta}H_2^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}-\rho\left(v_1L_1^{-\beta}H_1^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\right][\gamma(1-\rho^2)]^{-1}-[\gamma(1+\rho)]^{-1}\end{aligned}\tag{A7}$$

$$\begin{aligned}z_1&=\left((\alpha\beta)^{1-\phi}[\gamma\phi(1+\rho)]^{\phi}\right)^{\frac{1}{1+\beta-\phi}}\left[\left(v_1L_1^{1-\phi}H_1^{\phi}\right)^{\frac{1}{1+\beta-\phi}}-\rho\left(v_2L_2^{1-\phi}H_2^{\phi}\right)^{\frac{1}{1+\beta-\phi}}\right][\alpha(1-\rho^2)]^{-1}-[\alpha(1+\rho)]^{-1}-\eta s_2\\ z_2&=\left((\alpha\beta)^{1-\phi}[\gamma\phi(1+\rho)]^{\phi}\right)^{\frac{1}{1+\beta-\phi}}\left[\left(v_2L_2^{1-\phi}H_2^{\phi}\right)^{\frac{1}{1+\beta-\phi}}-\rho\left(v_1L_1^{1-\phi}H_1^{\phi}\right)^{\frac{1}{1+\beta-\phi}}\right][\alpha(1-\rho^2)]^{-1}-[\alpha(1+\rho)]^{-1}-\eta s_1\end{aligned}\tag{A8}$$

We now validate the second order conditions of the equilibrium. Noting the first order conditions (A1) and (A2), one can easily get at equilibrium

$$\begin{aligned}&\partial^2F_1/\partial z_1^2=-\alpha(\beta+1)\left(\alpha z_1^a+1\right)^{-1}<0\\ &\partial^2F_1/\partial s_1^2=-\alpha\rho\eta(\beta+1)(2\kappa_1s_1-\kappa_3s_2)\left(\alpha z_1^a+1\right)^{-1}-2\kappa_1<0\\ &\partial^2F_1/\partial z_1\partial s_1=-\alpha\rho\eta(\beta+1)\left(\alpha z_1^a+1\right)^{-1}\end{aligned}$$

and further

$$\begin{aligned}&\left[\partial^2F_1/\partial z_1^2\right]\left[\partial^2F_1/\partial s_1^2\right]-\left[\partial^2F_1/\partial z_1\partial s_1\right]^2\\ &=\alpha^2(1+\beta)^2[\rho\eta(2\kappa_1s_1-\kappa_3s_2)-\rho^2\eta^2]\left(\alpha z_1^a+1\right)^{-2}\\ &\quad+2\kappa_1\alpha(1+\beta)\left(\alpha z_1^a+1\right)^{-1}>0\end{aligned}$$

for appropriate interdependence ρ. Therefore, the second order condition for F_1 is satisfied. Analogously, the second order condition for F_2 can be validated.

Noting the first order condition (A4), one can get

$$\begin{aligned}&\partial^2H/\partial c_1^2=\gamma(\phi-1)(1+\rho)^{-1}\left[\left(\gamma c_1^a+1\right)^{-1}+\rho^2\left(\gamma c_2^a+1\right)^{-1}\right]\le0\\ &\partial^2H/\partial c_2^2=\gamma(\phi-1)(1+\rho)^{-1}\left[\left(\gamma c_2^a+1\right)^{-1}+\rho^2\left(\gamma c_1^a+1\right)^{-1}\right]\le0\\ &\partial H^2/\partial c_1\partial c_2=\gamma\rho(\phi-1)(1+\rho)^{-1}\left[\left(\gamma c_1^a+1\right)^{-1}+\left(\gamma c_2^a+1\right)^{-1}\right]\end{aligned}$$

and further

$$\begin{aligned}&\left[\partial^2H/\partial c_1^2\right]\left[\partial^2H/\partial c_2^2\right]-\left[\partial H^2/\partial c_1\partial c_2\right]^2\\ &=\gamma^2(\phi-1)^2\left(\gamma c_1^a+1\right)^{-1}\left(\gamma c_2^a+1\right)^{-1}(1+\rho)^{-2}(1+\rho^4-2\rho^2)\ge0\end{aligned}$$

for appropriate interdependence ρ. Hence, the second order condition for H is satisfied as well.

Appendix B. The social planner only controls security investment

When only security investment is controlled by the social planner, (A2) and (A3) remain valid. (A1) becomes

$$\begin{aligned}\partial F/\partial z_1&=\alpha\beta v_1L_1\left(\gamma c_1^a+1\right)^{\phi}\left(\alpha z_1^a+1\right)^{-\beta-1}\\ &\quad+\rho\alpha\beta v_2L_2\left(\gamma c_2^a+1\right)^{\phi}\left(\alpha z_2^a+1\right)^{-\beta-1}-1=0\\ \partial F/\partial z_2&=\rho\alpha\beta v_1L_1\left(\gamma c_1^a+1\right)^{\phi}\left(\alpha z_1^a+1\right)^{-\beta-1}\\ &\quad+\alpha\beta v_2L_2\left(\gamma c_2^a+1\right)^{\phi}\left(\alpha z_2^a+1\right)^{-\beta-1}-1=0\end{aligned}$$

which implies

$$\begin{aligned}&\alpha\beta v_1L_1\left(\gamma c_1^a+1\right)^{\phi}\left(\alpha z_1^a+1\right)^{-\beta-1}\\ &\quad=\alpha\beta v_2L_2\left(\gamma c_2^a+1\right)^{\phi}\left(\alpha z_2^a+1\right)^{-\beta-1}=(1+\rho)^{-1}.\end{aligned}\tag{B1}$$

Substituting (B1) into (A2) results in

$$s_1=s_2=\rho\eta[(1+\rho)(2\kappa_1-\kappa_3)]^{-1}.$$

Combining (B1) with (A4) gives

$$\begin{aligned}\gamma c_1^a+1&=\left(v_1L_1^{-\beta}H_1^{1+\beta}(1+\rho)(\alpha\beta)^{-\beta}(\gamma\phi)^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\\ \gamma c_2^a+1&=\left(v_2L_2^{-\beta}H_2^{1+\beta}(1+\rho)(\alpha\beta)^{-\beta}(\gamma\phi)^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\end{aligned}\tag{B2}$$

$$\begin{aligned}\alpha z_1^a+1&=\left(v_1L_1^{1-\phi}H_1^{\phi}(1+\rho)(\alpha\beta)^{1-\phi}(\gamma\phi)^{\phi}\right)^{\frac{1}{1+\beta-\phi}}\\ \alpha z_2^a+1&=\left(v_2L_2^{1-\phi}H_2^{\phi}(1+\rho)(\alpha\beta)^{1-\phi}(\gamma\phi)^{\phi}\right)^{\frac{1}{1+\beta-\phi}}\end{aligned}\tag{B3}$$

It follows from (B2) and (B3) that

$$\begin{aligned}c_1&=\left((1+\rho)(\alpha\beta)^{-\beta}(\gamma\phi)^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\left[\left(v_1L_1^{-\beta}H_1^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}-\rho\left(v_2L_2^{-\beta}H_2^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\right][\gamma(1-\rho^2)]^{-1}-[\gamma(1+\rho)]^{-1}\\ c_2&=\left((1+\rho)(\alpha\beta)^{-\beta}(\gamma\phi)^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\left[\left(v_2L_2^{-\beta}H_2^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}-\rho\left(v_1L_1^{-\beta}H_1^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\right][\gamma(1-\rho^2)]^{-1}-[\gamma(1+\rho)]^{-1}\end{aligned}\tag{B4}$$

$$\begin{aligned}z_1&=\left((1+\rho)(\alpha\beta)^{-\beta}(\gamma\phi)^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\left[\left(v_1L_1^{1-\phi}H_1^{\phi}\right)^{\frac{1}{1+\beta-\phi}}-\rho\left(v_2L_2^{1-\phi}H_2^{\phi}\right)^{\frac{1}{1+\beta-\phi}}\right][\alpha(1-\rho^2)]^{-1}-[\alpha(1+\rho)]^{-1}-\eta s_2\\ z_2&=\left((1+\rho)(\alpha\beta)^{-\beta}(\gamma\phi)^{1+\beta}\right)^{\frac{1}{1+\beta-\phi}}\left[\left(v_2L_2^{1-\phi}H_2^{\phi}\right)^{\frac{1}{1+\beta-\phi}}-\rho\left(v_1L_1^{1-\phi}H_1^{\phi}\right)^{\frac{1}{1+\beta-\phi}}\right][\alpha(1-\rho^2)]^{-1}-[\alpha(1+\rho)]^{-1}-\eta s_1\end{aligned}\tag{B5}$$

Now, consider the second order conditions at equilibrium. In a similar way, we can obtain $\partial^2F_1/\partial s_1^2<0$ and $\partial^2 F_2/\partial s_2^2<0$.

Given (B1), it is easy to derive that

$$\begin{aligned}\partial^2F/\partial z_1^2&=-\alpha(1+\beta)(1+\rho)^{-1}\left[\left(\alpha z_1^a+1\right)^{-1}+\rho^2\left(\alpha z_2^a+1\right)^{-1}\right]<0\\ \partial^2F/\partial z_2^2&=-\alpha(1+\beta)(1+\rho)^{-1}\left[\left(\alpha z_2^a+1\right)^{-1}+\rho^2\left(\alpha z_1^a+1\right)^{-1}\right]<0\\ \partial^2F/\partial z_1\partial z_2&=-\alpha\rho(1+\beta)(1+\rho)^{-1}\left[\left(\alpha z_1^a+1\right)^{-1}+\left(\alpha z_2^a+1\right)^{-1}\right]\end{aligned}$$

and

$$\begin{aligned}&\left[\partial^2F/\partial z_1^2\right]\left[\partial^2F/\partial z_2^2\right]-\left[\partial^2F/\partial z_1\partial z_2\right]^2\\ &=\alpha^2(1+\beta)^2\left(\alpha z_1^a+1\right)^{-1}\left(\alpha z_2^a+1\right)^{-1}(1+\rho)^{-2}(1+\rho^4-2\rho^2)>0\end{aligned}.$$

Analogously, the second order condition for H can be validated.

Appendix C. The social planner just controls information sharing

When only information sharing is controlled by the social planner, (A1) and (A3) remain valid. (A2) becomes

$$\begin{aligned}\partial F/\partial s_1&=\rho\alpha\beta v_1L_1\eta\left(\gamma c_1^a+1\right)^{\phi}\left(\alpha z_1^a+1\right)^{-\beta-1}+\alpha\beta v_2L_2\eta\left(\gamma c_2^a+1\right)^{\phi}\left(\alpha z_2^a+1\right)^{-\beta-1}\\ &\quad-2(\kappa_1-\kappa_2)s_1+2\kappa_3s_2=0\\ \partial F/\partial s_2&=\alpha\beta v_1L_1\eta\left(\gamma c_1^a+1\right)^{\phi}\left(\alpha z_1^a+1\right)^{-\beta-1}+\rho\alpha\beta v_2L_2\eta\left(\gamma c_2^a+1\right)^{\phi}\left(\alpha z_2^a+1\right)^{-\beta-1}\\ &\quad-2(\kappa_1-\kappa_2)s_2+2\kappa_3s_1=0\end{aligned}\tag{C1}$$

Substituting (A1) into (C1) gives

$$s_1=s_2=\eta(1+\rho)[2(\kappa_1-\kappa_2-\kappa_3)]^{-1}.$$

Aggregate defense and aggregate attack are derived from (A1) and (A3), both of which remain unchanged. Hence, security investment and cyber attacks are given by (A7) and (A8) respectively after substituting s_1 and s_2.

Noting (A1), we have

$$\partial^2 F/\partial s_1^2 = -\alpha\eta^2(1+\beta)\left[\rho^2\left(\alpha z_1^a+1\right)^{-1}+\left(\alpha z_2^a+1\right)^{-1}\right]-2(\kappa_1-\kappa_2)<0$$
$$\partial^2 F/\partial s_2^2 = -\alpha\eta^2(1+\beta)\left[\left(\alpha z_1^a+1\right)^{-1}+\rho^2\left(\alpha z_2^a+1\right)^{-1}\right]-2(\kappa_1-\kappa_2)<0$$
$$\partial^2 F/\partial s_1\partial s_2 = -\alpha\rho\eta^2(1+\beta)\left[\left(\alpha z_1^a+1\right)^{-1}+\left(\alpha z_2^a+1\right)^{-1}\right]+2\kappa_3$$

and

$$\begin{aligned}&\left[\partial^2 F/\partial s_1^2\right]\left[\partial^2 F/\partial s_2^2\right]-\left[\partial^2 F/\partial s_1\partial s_2\right]^2\\&=2\alpha\eta^2(1+\beta)[(\kappa_1-\kappa_2)(1+\rho^2)+2\kappa_3\rho)]\left[\left(\alpha z_1^a+1\right)^{-1}+\left(\alpha z_2^a+1\right)^{-1}\right]\\&+\alpha^2\eta^4(1+\beta)^2(1-\rho^2)^2\left(\alpha z_1^a+1\right)^{-1}\left(\alpha z_2^a+1\right)^{-1}+4\left[(\kappa_1-\kappa_2)^2-\kappa_3^2\right]>0\end{aligned}$$

for appropriate interdependence ρ since $\kappa_1 \geq \kappa_2+\kappa_3$. It is obvious that $\partial^2 F_1/\partial z_1^2 < 0$ and $\partial^2 F_2/\partial z_2^2 < 0$. As above, the second order condition for H can be validated in the same way.

Appendix D. The social planner controls both security investment and information sharing

When the social planner controls security investment and information sharing, (B1), (C1) as well as (A4) are valid. Substituting (B1) into (C1) yields

$$s_1 = s_2 = \eta[2(\kappa_1-\kappa_2-\kappa_3)]^{-1}.$$

Aggregate defense and aggregate attack in this case are equal to those when the social planner just controlling security investment, which are determined by (B1) and (A4). The security investment and cyber attacks can be obtained similarly, shown in (B4) and (B5) where s_1 and s_2 are replaced. The second order condition for the social planner is satisfied if the following symmetric matrix is negative definite,

$$J(\rho)=\begin{pmatrix}\partial^2 F/\partial z_1^2 & \partial^2 F/\partial z_1\partial z_2 & \partial^2 F/\partial z_1\partial s_1 & \partial^2 F/\partial z_1\partial s_2\\ \partial^2 F/\partial z_2\partial z_1 & \partial^2 F/\partial z_2^2 & \partial^2 F/\partial z_2\partial s_1 & \partial^2 F/\partial z_2\partial s_2\\ \partial^2 F/\partial s_1\partial z_1 & \partial^2 F/\partial s_1\partial z_2 & \partial^2 F/\partial s_1^2 & \partial^2 F/\partial s_1\partial s_2\\ \partial^2 F/\partial s_2\partial z_1 & \partial^2 F/\partial s_2\partial z_2 & \partial^2 F/\partial s_2\partial s_1 & \partial^2 F/\partial s_2^2\end{pmatrix}$$

where

$$\partial^2 F/\partial z_1\partial s_1 = -\alpha\rho\eta(1+\beta)(1+\rho)^{-1}\left[\left(\alpha z_1^a+1\right)^{-1}+\left(\alpha z_2^a+1\right)^{-1}\right]$$
$$\partial^2 F/\partial z_1\partial s_2 = -\alpha\eta(1+\beta)(1+\rho)^{-1}\left[\left(\alpha z_1^a+1\right)^{-1}+\rho^2\left(\alpha z_2^a+1\right)^{-1}\right]$$
$$\partial^2 F/\partial z_2\partial s_1 = -\alpha\eta(1+\beta)(1+\rho)^{-1}\left[\rho^2\left(\alpha z_1^a+1\right)^{-1}+\left(\alpha z_2^a+1\right)^{-1}\right]$$
$$\partial^2 F/\partial z_2\partial s_2 = -\rho\alpha\eta(1+\beta)\left[\left(\alpha z_1^a+1\right)^{-1}+\left(\alpha z_2^a+1\right)^{-1}\right]$$

and other partial derivatives are equal to the preceding after substituting aggregate defense and aggregate attack here. Exchanging the second and the fourth rows and simultaneously exchanging the second and the fourth columns of $J(0)$ yield

$$\widehat{J}(0)=\begin{pmatrix}A & O_{2\times 2}\\ O_{2\times 2} & B\end{pmatrix},$$

where $O_{2\times 2}$ is zero matrix,

$$A=\alpha(1+\beta)\left(\alpha z_1^a+1\right)^{-1}\begin{pmatrix}-1 & -\eta\\ -\eta & -1\end{pmatrix}$$

and

$$B=\begin{pmatrix}-\alpha\eta^2(1+\beta)(\alpha z_2^a+1)^{-1}-2(\kappa_1-\kappa_2) & 2\kappa_3\\ 2\kappa_3 & -\alpha\eta^2(1+\beta)\left(\alpha z_1^a+1\right)^{-1}-2(\kappa_1-\kappa_2)\end{pmatrix}.$$

Obviously, A has two negative eigenvalues. Since $\det B = \left[\alpha\eta^2(1+\beta)\left(\alpha z_2^a+1\right)^{-1}+2(\kappa_1-\kappa_2)\right]\left[\alpha\eta^2(1+\beta)\left(\alpha z_1^a+1\right)^{-1}+2(\kappa_1-\kappa_2)\right]-4\kappa_3^2 > 4\left[(\kappa_1-\kappa_2)^2-\kappa_3^2\right]\geq 0$, and $tr(B)<0$, symmetric matrix B also has two negative eigenvalues. Therefore, all eigenvalues of $\widehat{J}(0)$ are negative, which implies that $J(0)$ is negative definite since $J(0)$ and $\widehat{J}(0)$ have the same eigenvalues. By the continuity of $J(\rho)$

with respect to ρ, $J(\rho)$ is negative definite for ρ with a small magnitude (for any non-zero vector X, $X^T J(0)X<0 \Rightarrow X^T J(\rho)X<0$ as long as the magnitude of ρ is small). The second order condition for the hacker can be validated similarly.

References

Anderson, R. (2001). Why information security is hard: an economic perspective. *Proceedings of the Seventeenth Computer Security Applications Conference, IEEE Computer Society Press*, 358–365.

Anderson, R. (2002). *Security in open versus closed systems-the dance of Boltzmann, Coase and Moore*. Technical report, Cambridge University, England.

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

Arora, A., Nandkumar, A., & Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure?-an empirical analysis. *Information Systems Frontiers, 8*(5), 350–362.

Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010). Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. *Information Technology and Management, 11*(1), 7–23.

Bandyopadhyay, T., Liu, D., Mookerjee, V. S., Wilhite, A. W. (2012). Dynamic competition in IT security: a differential games approach. *Information Systems Frontiers*, in press, doi:10.1007/s10796-012-9373-x.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM, 48*(2), 78–83.

Büyükkarabacak, B., & Valev, N. (2012). Credit information sharing and banking crises: an empirical investigation. *Journal of Macroeconomics, 34*(3), 788–800.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448.

Cavusoglu, H., & Raghunathan, S. (2004). Configuration of detection software: a comparison of decision and game theory approaches. *Decision Analysis, 1*(3), 131–148.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: capital market reaction for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9*(1), 69–105.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*(1), 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*(2), 281–304.

Cavusoglu, H., Raghunathan, S., & Cavusoglu, H. (2009). Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems. *Information Systems Research, 20*(2), 198–217.

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: stock market evidence of investors' behavior. *Decision Support Systems, 50*(4), 651–661.

Clark, D. J., & Riis, C. (1998). Contest success functions: an extension. *Economic Theory, 11*(1), 201–204.

Cremonini, M., & Nizovtsev, D. (2009). Risks and benefits of signaling information system characteristics to strategic attackers. *Journal of Management Information Systems, 26*(3), 241–274.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79–98.

Dutta, A., & Mccrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67–87.

Galbreth, M. R., & Shor, M. (2010). The impact of malicious agents on the enterprise software industry. *MIS Quarterly, 34*(3), 595–612.

Gal-Or, E., & Ghose, A. (2003). *The economic consequences of sharing security information*. Proceedings of the Second Workshop on Economics and Information Security, University of Maryland.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research, 16*(2), 186–208.

Gao, X., Zhong, W., & Mei, S. (2012a). On local stability of Cournot models with simultaneous and sequential decisions. *Mathematical Social Sciences, 63*(3), 207–212.

Gao, X., Zhong, W., Mei, S. (2012b). Stochastic evolutionary game dynamics and their selection mechanisms. *Computational Economics, 41*(2), 233–247.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457.

Gordon, L. A., & Loeb, M. P. (2006). Economic aspects of information security: an emerging field of research. *Information Systems Frontiers, 8*(5), 335–337.

Gordon, L. A., Alumni, E. Y., Loeb, M. P., Lucyshyn, W. (2002). *An economics perspective on the sharing of information related to security breaches: Concepts and empirical evidence*. Workshop on Economics and Information Security, University of California, Berkeley.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003a). Sharing information on computer systems security: an economic analysis. *Journal of Accounting and Public Policy, 22*(6), 461–485.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003b). Information security expenditures and real options: a wait-and-see approach. *Computer Security Journal, 19*(2), 1–7.

Hahm, J. H., & Lee, S. (2011). Economic effects of positive credit information sharing: the case of Korea. *Applied Economics, 43*(30), 4879–4890.

Hamill, J. T., Deckro, R. F., & Kloeber, J. M., Jr. (2005). Evaluating information assurance strategies. *Decision Support Systems, 39*(3), 463–484.

Hare, F., & Goldstein, J. (2010). The interdependent security problem in the defense industrial base: an agent-based model on a social network. *International Journal of Critical Infrastructure Protection, 3*(3–4), 128–139.

Hausken, K. (2006a). Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy, 25*(6), 629–665.

Hausken, K. (2006b). Returns to information security investment: the effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers, 8*(5), 338–349.

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy, 26*(6), 639–688.

Hausken, K. (2009). Strategic defense and attack of complex networks. *International Journal of Performability Engineering, 5*(1), 13–30.

Hausken, K. (2012). The economics of terrorism against two targets. *Applied Economics Letters, 19*(12), 1135–1138.

Heal, G., & Kunreuther, H. (2007). Modeling interdependent risks. *Risk Analysis, 27*(3), 621–634.

Herath, H., & Harath, T. (2009). Investments in information security: a real options perspective with Bayesian postaudit. *Journal of Management Information Systems, 25*(3), 337–375.

Huang, D., Qing, H., & Ravi, B. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics, 114*(2), 793–804.

Kallberg, J. G., & Udell, G. F. (2003). The value of private sector business credit information sharing: the US case. *Journal of Banking & Finance, 27*(3), 449–469.

Kannan, K., & Telang, R. (2005). Market for software vulnerabilities? think again. *Management Science, 51*(5), 726–740.

Kim, S. H., Wang, Q., & Ulrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM, 55*(3), 66–73.

Kong, H. K., Kim, T. S., & Kim, J. (2012). An analysis on effects of information security investments: a BSC perspective. *Journal of Intelligent Manufacturing, 23*(4), 941–953.

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy, 4*(1), 33–39.

Kshetri, N. (2009). Positive externality, increasing returns and the rise in cybercrimes. *Communications of the ACM, 52*(12), 141–144.

Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty, 26*(2–3), 231–249.

Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: a study on a large-scale hacking incident on the Internet. *Information Systems Frontiers, 14*(2), 375–393.

Leeson, P., & Coyne, C. J. (2006). The economics of computer hacking. *Journal of Law, Economics and Policy, 1*(2), 511–532.

Leininger, W. (1993). More efficient rent-seeking: a Münchhausen solution. *Public Choice, 75*(1), 43–62.

Liu, D., Ji, Y., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems, 52*(1), 95–107.

Mookerjee, V., Mookerjee, R., Bensoussan, A., & Yue, W. T. (2011). When hackers talk: managing information security under variable attack rates and knowledge dissemination. *Information Systems Research, 22*(3), 606–623.

Pardo, T. A., Cresswell, A. M., Thompson, F., & Zhang, J. (2006). Knowledge sharing in cross-boundary information system development in the public sector. *Information Technology and Management, 7*(4), 293–313.

Png, I. P. L., Wang, C. Y., & Wang, Q. H. (2008). The deterrent and displacement effects of information security enforcement: international evidence. *Journal of Management Information Systems, 25*(2), 125–144.

Ryan, J. C. H., & Ryan, D. J. (2006). Expected benefits of information security investments. *Computers & Security, 25*(8), 579–588.

Skaperdas, S. (1996). Contest success functions. *Economic Theory, 7*(2), 283–290.

Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: an empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy, 24*(1), 37–59.

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering, 33*(8), 544–557.

Ulvila, J. W., & Gaffney, J. E. (2004). A decision analysis method for evaluating computer intrusion detection systems. *Decision Analysis, 1*(1), 35–50.

Wang, J., Chaudhury, A., & Rao, H. R. (2008). A value-at-risk approach to information security investment. *Information Systems Research, 19*(1), 2008.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM, 46*(8), 91–95.

Young, R., Zhang, L., & Prybutoka, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management, 24*(4), 281–287.

Zhang, R. (2011). The role of information sharing in trade credit distribution: evidence from Thailand. *Asian-Pacific Economic Literature, 25*(1), 133–149.

Zhao, X., Fang, F., & Whinston, A. B. (2008). An economic mechanism for better Internet security. *Decision Support Systems, 45*(4), 811–821.

Zhuang, J. (2010). Impacts of subsidized security on stability and total social costs of equilibrium solutions in an n-player game with errors. *The Engineering Economist, 55*(2), 131–149.

Zhuang, J., Bier, V. M., & Gupta, A. (2007). Subsidies in interdependent security with heterogeneous discount rates. *The Engineering Economist, 52*(1), 1–19.

Xing Gao is a Ph.D. student receiving a Ph.D. degree soon at Southeast University in China. His research interests include information security economics, game theory as well as the theory of industry origination. He has published research articles in journals such as Mathematical Social Sciences and Computational Economics.

Weijun Zhong is a Professor at Southeast University in China, whose current research interests include information security economics, management information systems, management of technology and innovation. Prof. Zhong has published research articles in various academic journals including Journal of Management Information Systems, International Journal of Production Economics, Technological Forecasting and Social Change, Marketing Letters and Operations Research Letters.

Shue Mei is a Professor at Southeast University in China and focuses on the economics of information security, management information systems, electronic commerce, management of technology and innovation. Prof. Mei has published research articles in many journals including Technological Forecasting and Social Change, Marketing Letters, Operations Research Letters and Computational Economics.