Information sharing among firms and cyber attacks

Kjell Hausken

Abstract

As the Sarbanes-Oxley Act strengthens internal controls, and the government encourages information sharing, accounting gains significance through secure representation, storage, and transfer of information, and by laying the foundation for assessing costs and benefits. Information sharing and security investment for two firms are inverse U shaped in the aggregate attack, and interlinked through the interdependence and the firm's unit cost of security investment. Both increase in the interdependence (e.g. US telecommunications industry). With given security investment, social welfare is inverse U shaped in information sharing. Individual optimization implies free riding. A social planner is introduced controlling information sharing, security investment, or both, in simultaneous and two period games. Two period games where the social planner moves first are realistic when the social planner is highly respected. For the simultaneous game, a social planner controlling information sharing (security investment) imposes unreasonably high sharing (security investment). Firms free ride in the variable they control. The social planner imposes more moderate levels in the two period games. A social planner controlling both information sharing and security investment in a two period game where the social planner moves first is the most beneficial control scenario when the firms' defense efficiencies are high. If these are sufficiently high, the attack is deterred altogether.

Keywords: Cyber war; Conflict; Contest success function; Security investment; Information sharing; Security breaches; Interdependence; Social planner; Social welfare; Budget control

1. Introduction

Information sharing and security investment are essential in today's internet era. Firms naturally find incentives to invest in security technology, but incentives for information sharing are harder to furnish. Aside from some cases where confidentiality plays a role, information sharing is usually collectively beneficial. Gordon et al. (2006b) identify three categories of information disclosure. These are voluntary disclosure of proactive steps toward improving information security, voluntary disclosure of information security vulnerabilities, and voluntary disclosure of information security breaches. Two recent developments impact information disclosure. First, the US federal government encourages the establishment of Security Based Information Sharing Organizations (SB/ISOs) of various kinds, such as Information Sharing & Analysis Centers (ISACs), CERT, INFRAGARD, etc. Second, the 2002 Sarbanes-Oxley Act (SOX) places strict requirements on firms, such as (Sections 302 and 404) establishing and maintaining adequate internal controls for financial reporting, and assessing annually the effectiveness of those controls. These are steps in the right direction. There is a need to scrutinize the underlying logic by which firms decide whether or not to share information. When cases have been identified where information sharing does, should, or can indeed occur, which this article intends to accomplish, then infrastructure, laws, regulations, and cultures may be developed and designed to enhance information sharing.

Although SOX does not regulate changes in information security activities, Gordon et al. (2006b) find that voluntary disclosure in 2003–2004 increased 100% compared with 2000–2001, concomitant with enhanced awareness of the role of information security. Whether this trend will continue in the future is unclear since a double edged sword is involved when determining whether to disclose information security activities. A firm wants everyone to perceive that its information activities are secure. To build up that perception, outsiders need information. Two extreme strategies are as follows. The first is for a firm to state that we use the most recent and advanced technology and procedures, but you have to trust us since we release no information about these which can be exploited by agents with undesirable objectives. The second is for a firm to release all information about technology and procedures so that all agents know the exact manner in which the firm is well protected. The potential downside of this second strategy is that agents with undesirable objectives may be better suited to design an attack strategy since they know what they are up against. We often hear firms choosing intermediates between these two extremes by alluding to the presence of the most advanced information security technology and procedures, without being too specific about what these are.

Information sharing and security investment have linkages to accounting and public policy, as also observed by Gordon et al. (2003). First, accounting means representing information in certain formats and on chosen media, for subsequent release according to regulations. Second, accountants administer internal controls for generating and disseminating information which involves tradeoffs between availability, retrievability, authentication, efficient dissemination, security, and confidentiality. See Ghose (2007) for some of these tradeoffs. Third, accountants lay the foundation for assessing strategies about gaining competitive advantage, which encompasses assessing the expenditures, risks, benefits, and profits of various chosen levels of information sharing and security investment. Fourth, since SOX regulates internal controls for financial reporting, which is under the purview of accounting, information sharing and security investment get more intrinsically linked with accounting. The linkage to public policy follows since the security of an interlinked information system depends on the strategies about information sharing and security investment chosen by all actors, those that generate and maintain it, those that are players in it, those that run it or attempt to administer or regulate it, those that are affected by it and attempt to affect it in return, those that attempt to use it to their advantage, those that attempt to reshape it, and those that attempt to shut it down.

Information sharing is a recent occurrence in the cyber era, but has a certain history in the literature on oligopolies, cooperative relationships, joint ventures, and trade associations (Gal-Or, 1985; Kirby, 1988; Novshek and Sonnenschein, 1982; Shapiro, 1986; Vives, 1990; Ziv, 1993). In the cyber era information sharing has been analyzed by Gal-Or and Ghose (2003, 2005), Gordon et al. (2003) and Schechter and Smith (2003). Security breaches and vulnerabilities have been analyzed by Campbell et al. (2003), Cavusoglu et al. (2004), Gordon and Loeb (2001, 2002, 2003), Gordon et al. (2006a), Hausken (2006b), Schenk and Schenk (2002), Tanaka et al. (2005).

The literature on information sharing and information security typically considers the external threat as fixed and immutable. In contrast, this article considers an external agent which optimizes a costly attack just as the two firms subject to attack optimize a costly defense. Two firms may operate independently in different markets, they may share markets, they may be strong competitors, they may be interlinked through vertical integration upstream or downstream, outsourcing, or other cooperative arrangements, or they may be so strongly interconnected that an attack on one is tantamount, in varying degrees, to an attack on the other. The interdependence may also be negative. For example, one firm's increase in security investment can redirect the agent's attack to the other firm and therefore reduce the other firm's contest success. The various kinds of interaction between firms influence the cyber war and strategic choices of both firms and the external agent. Both the interdependence between firms and the capacity of the external agent to inflict cyber attacks, determined by the agent's attack efficiency, are essential when scrutinizing incentives for information sharing. This article assigns separate modeling features for information sharing and security investment. A contest success function models information sharing with relative effectiveness to security investment. By considering the information sharing between firms, the leakage cost function is also modeled differently from the security investment cost function.

The two firms and attacking agent maximize their profits individually. The article proceeds to assume an exogenously given level of information sharing. This makes an interesting case to model the operation of the information sharing organizations (e.g., US-CERT), which is the firms' most commonly used channel for sharing their security information. The article thereafter assumes an exogenously given level of security investment. A predetermined level of security investment provides another interesting case about the problems of limiting information security budgets within firms. A social planner is introduced under a variety of different control scenarios. Given the current emergence of SB/ISOs, combined with firms' ubiquitous needs to control budgets, this article intends to understand the quite different impacts when a social planner or budget controls information sharing only, security investment only, or both, in a simultaneous game, and two period game.

One main difference between security investments and information sharing is that the former requires costly funding, planning, sustained effort through time, involving buildup of infrastructure, culture, and competence, while the latter may be more or less costless aside from leakage costs as a consequence of sharing. If information about security breaches, and other kinds of information, are compiled and stored in an organized and secure manner within each firm, deciding to share it with another firm may not involve more than pushing a transfer button, or storing the information on a disk and delivering it. In other words, security investments are costly since all investments are costly, while information sharing is costly in the different sense of risk of information leakage.

Gordon et al. (2003) find that when firms share information, each firm has reduced incentives to invest in information security. In contrast, Gal-Or and Ghose (2005) find that "security technology investments and security information sharing act as 'strategic complements'". This article assumes substitutability between own security investment and information received by the other firm, but allows for complementarity when the interdependence is negative.

The work by Gordon et al. (2003) and Gal-Or and Ghose (2005), and also this article, assume information scaled along one dimension. Gordon et al. (2003, p. 469) refer to a portion, which is a number between zero and one, of a firm's computer security information that it may decide to share with the other firm. Similarly, Gal-Or and Ghose (2005, p. 189) "normalize the amount of security information being shared so that it always lies between 0 and 1".

Generally, information is multi-faceted, of different kinds, and with different degrees of importance for different purposes. A one-dimensional con-ception of information means that different kinds of information are given dif-ferent weights according to their relative importance.

ISACs were developed by industry professionals after Presidential Decision Directive 63 was issued in 1998. PDD 63 was designed to create a public and private sector partnership to protect the critical infrastructure of the United States. PDD 63 was replaced in 2003 with HSPD-7. One example is the Financial Services Sector Information Sharing and Analysis Center—FS/ISAC The FS/ISAC became operational in October 1999 and was restructured in 2003 to broaden its mission and serve all financial services sector participants. The membership and participants are made up of eligible members (more than 1500) of the Financial Services Sector: Banks, S& L, Credit Unions, Securities Firms, Insurance Companies, Credit Card Companies, Mortgage Banking Companies, Financial Services sector profits, Financial Services Service Bureaus, Appropriate Industry Associations. The FS/ISAC gathers threat, risks, and vulnerability information about cyber and physical risks faced by the financial services sector. Members have a platform for sharing information and working with professionals who face the same problems. The FS/ISAC has industry experts to analyze risks and deliver alerts to participants. Alerts may be Normal, Urgent, or Crisis. They identify the level of risk to the sector, provide detail on the alert, and provide any recommended solution to the risk.[1]

There are four differences between this article and Hausken's (2006a) analysis of the interdependence, income, and substitution effects. First, and most importantly, this article assumes that each firm has two strategic choice variables, information sharing and security investment, while Hausken (2006a) assumes one strategic choice variable, security investment. This allows analyzing sophisticated tradeoffs between information sharing and security investment, in interaction with an optimizing external agent. Second, Hausken (2006a) lets the agent's attack depend on a resource constraint and an attack efficiency. For the substitution effect, the agent optimizes the attacks across the two firms subject to the resource constraint. In contrast, this article lets the agent choose optimal attacks against both firms, with no resource con-straint, and dependent on an attack efficiency. This implicitly accounts for opti-mal substitution across the two firms.[2] Third, Hausken (2006a) considers the

[1] I am indebted to William Lucyshyn for the formulation about ISACs in this paragraph.

[2] A firm that decides to share information with another firm risks information leakage, and additionally causes a benefit for the other firm. This makes the first firm a more vulnerable target, and the external agent can be expected to substitute its attack from the other firm towards the first firm. Hence the substitution effect is not conducive to information sharing. The substitution effect is particularly interesting related to how two firms are different, and how the agent substitutes back and forth between the firms dependent on such differences.

income effect for n equivalent firms assuming an income reduction parameter which eliminates the attack (e.g. through freezing the agent's assets) if the firms' security investments are sufficiently large. This article confines attention to two firms and does not consider the income effect in this sense. However, the income effect is considered in the sense of depending on the agent's attack efficiency which is a parameter in the model. If the attack efficiency is reduced to zero, the agent's attack becomes infinitely costly, which effectively eliminates the agent's income. Fourth, this article considers the social planner's point of view which is especially important when assessing information sharing. Both Hausken (2006a) and this article consider interdependence between firms, which may be positive, zero, or negative.

Section 3 analyzes the model when each firm and the agent optimize individually. Section 4 assumes exogenously given information sharing. Section 5 assumes exogenously given security investment. Section 6 introduces a social planner who controls information sharing. Section 6.1 analyzes the two period game where the social planner moves first, while the firms and agent choose security investments and attacks in the second period. Section 6.2 considers the simultaneous game. Section 7 considers a social planner that controls security investment in a simultaneous game. Section 8 analyzes a social planner that controls both information sharing and security investment. Section 8.1 considers the simultaneous game. Section 8.2 considers the two period game where the social planner moves first. Section 9 assesses which games and control scenarios the agent and social planner prefer. Section 10 concludes.

2. The model

Consider two firms i and j with assets they value as r_i and r_j. An external agent launches a cyber security attack of magnitude T_i against firm i and T_j against firm j to appropriate as much as possible of the assets.[3] The cyber attack expenditure is F_i, where $\partial F_i/\partial T_i > 0$. We consider the simple case $F_i = CT_i$, where $1/C$ is the efficiency of cyber attack, and C is the inefficiency. This means that C is a unit transformation cost. The attack means attempting to break through the security defense of the firms in order to appropriate, get access to, or confiscate, something of value (e.g. bank accounts), or secure information which can be used to the firm's disadvantage, or to other firms' advantage, or to blackmail the firm, or to generate value in some other covert or not so covert manner.

[3] The author has analyzed the model when asset r_i is valued as r_i by firm i and R_i by the external agent, and analogously for r_j. The solution is more space consuming to write out, the results are intuitive, and the logic, results and policy recommendations are best conveyed confining attention to r_i and r_j.

Firm i invests t_i in information security technology to defend its asset, where t_i is the security investment cost, which we refer to as the investment. Firm i's investment consists in employing security experts, installing firewalls, encryption techniques, access control mechanisms, intrusion detection systems, etc. The security investment expenditure is f^i, where $\partial f^i/\partial t_i > 0$. We consider the simple case $f^i = c_i t_i$, where $1/c_i$ is the efficiency of security investment for firm i, so that c_i is the inefficiency, or a unit transformation cost. For simplicity, we assume risk neutral agents which does not change the nature of the argument. Both the expenditures $c_i t_i$ and CT_i can be capital and/or labor.

Firms are usually related to each other, e.g. through competitive relationships, or upstream and downstream networks. The relationship may consist in interconnection in goods and services (Kunreuther and Heal, 2003), or communication and information exchange via Electronic Data Interchanges (EDI). We introduce the parameter α to describe the two firms' relationship in resisting cyber attacks. The cyber contest between a firm and the agent for an asset takes the common ratio form (Skaperdas, 1996). Assuming relationship α between the firms, and no information sharing, we consider the four contest success functions

$$h^i = \frac{t_i + \alpha t_j}{t_i + T_i + \alpha(t_j + T_j)}, \quad h^j = \frac{t_j + \alpha t_i}{t_j + T_j + \alpha(t_i + T_i)}$$
$$H^i = 1 - h^i = \frac{T_i + \alpha T_j}{t_i + T_i + \alpha(t_j + T_j)}, \quad H^j = 1 - h^j = \frac{T_j + \alpha T_i}{t_j + T_j + \alpha(t_i + T_i)} \tag{1}$$

We require all numerators to be positive. h^i and h^j are the contest success of firms i and j. H^i and H^j are the contest success of the agent against firms i and j. Each firm benefits concavely from its own security investment, and suffers convexly from the agent's attack against itself. With positive interdependence, each firm benefits concavely from the other firm's security investment, and suffers convexly from the agent's attack against the other firm. With negative interdependence, each firm suffers concavely from the other firm's security investment, and benefits convexly from the agent's attack against the other firm. That is, for firm i, $\partial h^i/\partial t_i \geqslant 0, \partial^2 h^i/\partial t_i^2 \leqslant 0, \partial h^i/\partial t_j \geqslant 0$ when $\alpha > 0, \partial h^i/\partial t_j \leqslant 0$ when $\alpha < 0, \partial^2 h^i/\partial t_j^2 \leqslant 0, \partial h^i/\partial T_i \leqslant 0, \partial^2 h^i/\partial T_i^2 \geqslant 0, \partial h^i/\partial T_j \leqslant 0$ when $\alpha > 0, \partial h^i/\partial T_j \geqslant 0$ when $\alpha < 0, \partial^2 h^i/\partial T_j^2 \geqslant 0$. The expressions for the other three contest success functions are analogous.

When α is positive, the firms cooperate in defending themselves. Positive interdependence between firms also means that the agent's attack against one firm gets channeled further to a degree α to the other firm, exemplified with baggage transferred from one airline to the other (Kunreuther and Heal, 2003). Hence with positive interdependence, each firm gets a stronger defense, due to cooperation with the other firm, but is also subject to a stronger attack, due to channeling of the attack through the other firm. When $\alpha = 1$, the firms are 100% interdependent in the sense that firm i's choice of t_i has equal defense impact for firm i and firm j, and analogously for t_j. $\alpha > 1$ is theoretically pos-sible, but unlikely in praxis, and we exclude the possibility. It means that firm i's security investment t_i has larger defense impact for firm j than for firm i. When $\alpha = 0$, the firms are 100% independent and operate in isolation from each other. One firm's security investment then exclusively defends itself, with neither positive nor negative impact on the other firm.

When α is negative, which we refer to as negative interdependence, each firm's security investment is detrimental to the other firm, and merely strengthens one's own firm. Conversely to positive α, this also means that an attack on the other firm is beneficial for one's own firm. Hence with negative α, each firm gets a weaker defense, and is subject to a weaker attack. Although α can be arbitrarily negative, we do not allow negative contest success. Hence all numerators in (1) must be positive. For the special case that $t_i = t_j = T_i = T_j$, all the four contest success functions in (1) equal 1/2, independently of α. Fig. 1 illustrates the four contest success functions when firm i invests twice as much as firm i, and as the external agent invests against each of the firms, $t_i = 2$ and $t_j = T_i = T_j = 1$. When $\alpha = 1$, both firms cooperatively enjoy firm i's high investment, and their contest success is 0.6, while the agent earns 0.4 from each of the contests. As α decreases to $\alpha = 0$, the firms operate independently. This means that firm i and the agent earn contest success 2/3 and 1/3 respectively in their contest, while firm j and the agent both earn contest success 1/2 since their investments are equal. As α becomes negative, firm j starts to suffer, and the agent starts to suffer in the contest with firm i. Eq. (1) gives $h^j = 0$ when $\alpha = -0.5$, which means that the agent earns maximum contest success. Also, $\alpha = -0.5$ gives $h^i = 3/4$ and $H^i = 1/4$, to the benefit of firm i. Negative α causes

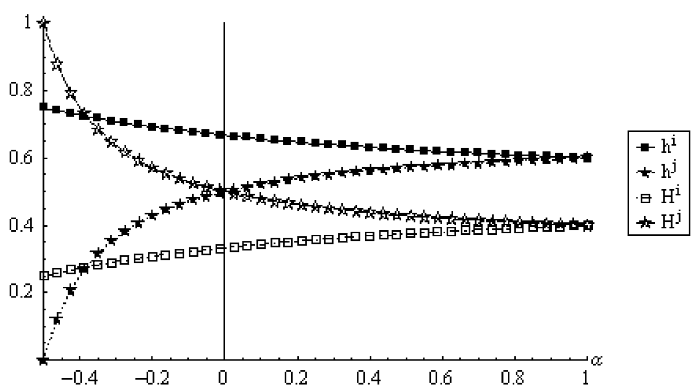

Fig. 1. Contest success as functions of the interdependence α when $t_i = 2$, $t_j = T_i = T_j = 1$, cf. Section 2.

a benefit for the firm that invests most, and larger discrepancies in the contest success. The interdependence α is a system characteristics and we assume the same α for both contests.

Negative interdependence is more likely in competitive and conflictful environments where firms do not jointly benefit from their security investments, but benefit from investing more in security than the other firm. The higher investor may perceive the external agent as more threatening and may no longer accept the free ride of the lower investor, but instead prefer the agent to attack the other firm instead of one's own firm. Let us consider an example to illustrate negative interdependence, and assume $t_i > t_j = T_i = T_j$ since equal investments give contest success 1/2 independently of α. Assume that firm i spends part of its budget on attracting the other firm's Security Officer. We conceptualize this so that α decreases. The impact in (1) is that $t_j + \alpha t_i$ decreases so that the contest success of firm j decreases, and the agent succeeds more against firm j. Also $t_i + \alpha t_j$ in (1) decreases, but since $t_i > t_j$, the contest success of firm i increases as α decreases, and the agent succeeds less against firm i. The Security Officer of firm j brings more defending experience to firm i. This, combined with firm i's superior investment, cause higher contest success for firm i and for the agent against firm j, and conversely lower contest success for firm j and for the agent against firm i. There are also other cases where firms' security investments are detrimental to other firms, which causes negative α. If security investments are not confidential but publicly available, firms with low investments can experience high investments by other firms as detrimental to customer confidence. Further, security investments can be of defensive or offensive nature in various manners. For example, the defense of one firm may deter the agent from attacks on all firms, e.g. when the defense convinces the agent that other firms have similar defenses and that attack would be futile. Alternatively, the defense of one firm may implicitly redirect the agent to other firms, in extreme cases by suggesting that other firms are more easy targets. The profits v_i, v_j, and V of firm i, firm j, and the agent, respectively, are

$$\begin{aligned} v_i &= \frac{t_i + \alpha t_j}{t_i + T_i + \alpha(t_j + T_j)} r_i - c_i t_i, \quad v_j = \frac{t_j + \alpha t_i}{t_j + T_j + \alpha(t_i + T_i)} r_j - c_j t_j \\ V &= \frac{T_i + \alpha T_j}{t_i + T_i + \alpha(t_j + T_j)} r_i + \frac{T_j + \alpha T_i}{t_j + T_j + \alpha(t_i + T_i)} r_j - CT_i - CT_j \end{aligned} \tag{2}$$

Firm i invests t_i in security technology at an expenditure $c_i t_i$. The investments $t_i + \alpha t_j$ are contested by the agent's attack $T_i + \alpha T_j$. Firm i retains the fraction h^i of its asset r_i, and the agent appropriates the remaining fraction 1-h^i. Firm j retains the analogous fraction h^j through an expenditure $c_j t_j$. The agent thus gets two fractions and incurs expenditures $C(T_i + T_j)$.

Assume that firm i shares an amount s_i of information with firm j, which means that firm i delivers s_i to firm j, and that firm j shares an amount s_j of information with firm i. Gordon et al. (2003) find that when firms share information, each firm has reduced incentives to invest in information security. This means that an increase in s_j causes a decrease in t_i. Both s_j and t_i strengthen firm i's defense. These two kinds of defense act as strategic substitutes. We thus consider the more general contest success function

$$k^i = \frac{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}{t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)} \tag{3}$$

which satisfies the same conditions as h^i. A firm benefits concavely from information sharing from the other firm, regardless of their relationship, $\partial k^i/\partial s_j \geqslant 0, \partial^2 k^i/\partial s_j^2 \leqslant 0$. With positive interdependence, each firm also benefits concavely from its own information sharing, dependent on the size of $\alpha, \partial k^i/\partial s_i \geqslant 0, \partial^2 k^i/\partial s_i^2 \leqslant 0$. When $\alpha > 0$, t_i, s_i, t_j, s_j are substitutable weapons to defend the firms from cyber attacks. With negative interdependence, each firm suffers concavely from its own information sharing, $\partial k^i/\partial s_i \leqslant 0, \partial^2 k^i/\partial s_i^2 \leqslant 0$. When $\alpha < 0$,t_i and s_j remain substitutes, while t_i and t_j, and t_i and s_i, are complements in the sense that an increase in one is compensated with an increase of the other. With negative interdependence, if a firm increases its information sharing, or the other firm increases its security investment, the firm must increase its security investment to maintain its contest success. Strategic complementarity is also found by Gal-Or and Ghose (2005, p. 193) where firms also choose prices. The demand facing each product is linear in self and cross-price effects. They find that increased security investment by one firm leads to increased security investment and increased information sharing by its competitor. Comparing with Gordon et al. (2003), Gal-Or and Ghose (2005, p. 194) observe that "the main reason for the different result is the existence of the demand enhancing effects of information security sharing and technology investments in our model". Summing up, Eq. (3) accounts for substitutability between s_j and t_i under all circumstances, accounts for more extensive substitutability with positive interdependence, and also accounts for complementarity with negative interdependence.

Each firm succeeds better in the contest with the agent when it receives information from the other firm. The parameter γ scales how effective is information from the other firm relative to own security investment when it comes to contesting the agent's attack. With no interdependence, $\alpha = 0$, the numerator in (3) becomes $t_i + \gamma s_j$ which is firm i's competitive effort. With positive interdependence, the term $\alpha\gamma s_i$ in the numerator in (3) does not mean that firm i receives its same information s_i in return from firm j, but that s_i strengthens firm j's competitive effort $t_j + \gamma s_i$ which gets channeled back to firm i moderated by α. With negative interdependence, γs_i strengthens firm j's competitive effort $t_j + \gamma s_i$, which has negative impact on firm i just as t_j has negative impact when $\alpha < 0$.

Exchanging information is risky for both firms. Firms are usually open rather than closed systems, and transmission channels may be unreliable.

When two firms share information, some actors within or associated with the two firms may more easily find an incentive to transfer the information further onto criminal agents, or to agents with a conflict of interest with one or both firms, since it is more difficult to identify the perpetrator spreading the information, than when two firms do not share information. Also, the transfer channels and broader domain within which the information exists give hackers larger room for maneuver. Spreading information thus increases the risk of leakage. Gal-Or and Ghose (2005, pp. 190–191) designate leakage costs "that might be inflicted on firm i as a result of such sharing". They suggest the functional form $g^i = \phi_1 s_i^2 - \phi_2 s_j^2 - \phi_3 s_i s_j$, where $\phi_1 \geqslant \phi_2 + \phi_3$. We define ϕ_1 as the inefficiency (unit cost) of own leakage, ϕ_2 as the efficiency (unit benefit) of the other firm j's leakage (since firm i benefits from it), and ϕ_3 as the efficiency (unit benefit) of joint leakage. First, $\partial g^i/\partial s_i > 0$ and $\partial g^i/\partial s_j < 0$ since it is risky to share information and beneficial to receive it. Second, $\partial^2 g^i/\partial s_i^2 > 0$ and $\partial^2 g^i/\partial s_j^2 < 0$ due to "possible deleterious ripple effects" of security breaches. Third, $\partial^2 g^i/\partial s_i \partial s_j \leqslant 0$ since "intensified sharing by the competitor reduces the marginal leakage costs incurred by the firm". The profits u_i, u_j, and U of firm i, firm j, and the agent, respectively, are

$$\begin{aligned}
u_i &= \frac{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}{t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)} r_i - c_i t_i - (\phi_1 s_i^2 - \phi_2 s_j^2 - \phi_3 s_i s_j) \\
u_j &= \frac{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}{t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)} r_j - c_j t_j - (\phi_1 s_j^2 - \phi_2 s_i^2 - \phi_3 s_i s_j) \\
U &= \frac{T_i + \alpha T_j}{t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)} r_i + \frac{T_j + \alpha T_i}{t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)} r_j \\
&\quad - C(T_i + T_j)
\end{aligned} \tag{4}$$

That firms in a competitive relationship are less likely to engage in information sharing is modeled in (4) in the following ways. The first is to increase ϕ_1. The negative impact of information leakage from one firm can get magnified through negative advertisement by the other firm which is more likely with a competitive relationship. The second is to decrease ϕ_2. This means that a leakage from the other firm is less useful for one's own firm. The third is to decrease ϕ_3 which reduces the efficiency of joint leakage. The parameters γ and α also reflect competitiveness between firms, but more indirectly since these parameters have other purposes. When γ decreases, the firms share less information since it becomes less useful relative to security investment. When α decreases and becomes negative, sharing information is directly harmful to one's own profit.

Each firm's vulnerability is modeled in (4) in two ways, aside from the firm being vulnerable as determined by the information sharing parameters γ, ϕ_1, ϕ_2, ϕ_3. A firm's vulnerability is important when determining cumulative efforts in enhancing information security. First, a vulnerable firm has a higher unit cost c of security investment. If firm i is more vulnerable, it can thus afford a lower security investment, which causes lower contest success. Second, firm i's asset r_i can be reinterpreted as βr_i, $0 \leqslant \beta \leqslant 1$, where β is a usability parameter. As β decreases below 1, the vulnerable firm possesses a smaller asset. The firm assumes that a part of its asset is already lost through its vulnerability, and does its best to defend the remaining part of its asset.

We hereafter refer to the firms' aggregate defense and attack as

$$t_i^A = t_i + \gamma s_j + \alpha(t_j + \gamma s_i), \quad t_j^A = t_j + \gamma s_i + \alpha(t_i + \gamma s_j)$$
$$T_i^A = T_i + \alpha T_j, \quad T_j^A = T_j + \alpha T_i \tag{5}$$

The model has 10 parameters. These are four firm characteristics r_i, r_j, c_i, c_j, four information sharing parameters γ, ϕ_1, ϕ_2, ϕ_3, one agent characteristic C, and the interdependence α. These 10 parameters are common knowledge for all actors.

3. Analyzing the model: each firm and the agent optimize individually

Firm i's free choice variables are t_i and s_i, firm j's free choice variables are t_j and s_j, and the external agent's free choice variables are T_i and T_j. The two firms and one agent choose their free choice variables simultaneously and independently to maximize profits. Appendix 1 determines the six FOCs (first order conditions), the six choice variables, and the three profits. Information sharing in (A.6) is

$$s_i = \frac{\alpha\gamma(2\phi_1 c_i + \phi_3 c_j)}{(2\phi_1 - \phi_3)(2\phi_1 + \phi_3)} \tag{6}$$

Proposition 1. *Information sharing increases linearly in the interdependence, is zero with negative or no interdependence, and increases linearly more in one's own than in the other firm's unit cost of security investment. That is,* $\partial s_i/\partial\alpha > 0$ *when* $\alpha > 0$, $s_i = 0$ *when* $\alpha \leqslant 0, \partial s_i/\partial c_i > 0, \partial s_i/\partial c_j > 0, \partial^2 s_i/\partial\alpha^2 = \partial^2 s_i/\partial c_i^2 = \partial^2 s_i/\partial c_j^2 = 0.$

Proof. Follows from (6). $2\phi_1 > \phi_3$ since $\phi_1 \geqslant \phi_2 + \phi_3$. □

That information sharing increases in the interdependence between firms is exemplified by the US telecommunications industry which is highly interdependent and experiences substantial information sharing.[4] The high degree of competitiveness has been seen suggested as a tentative explanation of the need to

[4] I thank William Lucyshyn for making this observation about the US telecommunications industry.

share information, but interdependence seems to be a more plausible explanation. Firms realize that through their strong interdependence, sharing information with other firms flows back as a benefit to themselves. Allowing shared information to flow more freely throughout the industry gives each firm a competitive advantage, and gives the firms a more robust defense against external attackers. As the interdependence decreases to zero, information sharing vanishes, and remains absent for negative interdependence. When firms exist in isolation from each other, no firm has an incentive to share information, but would prefer to receive information. The classical free rider dilemma explains why information sharing does not occur, as also found by Gordon et al. (2003). The need to free ride becomes in principle even stronger for negative interdependence, since sharing information then gives a competitive advantage to the other firm which has direct negative impact on one's own defense. Since a negative amount of information cannot be shared, each firm refrains from information sharing in this case.

As the unit cost of security investment increases, a firm shifts its emphasis toward more information sharing to maintain its defense. With equal unit costs $c_i = c_j$ for the two firms, c_i is placed outside the bracket in the numerator in (6). The bracket is abbreviated with the corresponding bracket in the denominator, and the remaining numerator is $\alpha\gamma c_i$. The unit cost of security investment, the interdependence, and the effectiveness of information sharing relative to security investment then have equally strong and multiplicative proportional impact on boosting information sharing.

Information sharing of both firms increases regardless whose unit cost increases. But, as one firm's unit cost of security investment increases more than that of the other firm, the first firm shares substantially more information, and the other firm shares moderately more information. The firm with the highest unit cost is least inclined to free ride in information sharing. First, the higher unit cost implies a need to shift from security investment to information sharing. Second, the higher unit cost also causes the other firm to share information, which benefits the first firm. As an example, assume that the inefficiency of own information leakage is $\phi_1 = 2$, while the efficiency of joint leakage is $\phi_3 = 1$. This is a moderate example since ϕ_1 can be substantially larger than ϕ_3. With benchmark equal unit costs $c_i = c_j = 1$, the bracket in the numerator in (6) equals 5. Increasing own unit cost to $c_i = 2$, the bracket becomes 9. Alternatively, increasing the other firm's unit cost to $c_j = 2$, the bracket merely increases to 6. The increase in information sharing is 80% in the first case and only 20% in the second case.[5]

The aggregate attack and defense determined by (5), (A.3), (A.6), (A.7) and (A.8) are inverse U shaped in each other, i.e.

[5] Intuitively, s_i in (6) increases in γ and ϕ_3, and decreases in ϕ_1.

$$T_i^A = \sqrt{\frac{t_i^A(1+\alpha)r_i}{C}} - t_i^A, \quad T_i^A = \frac{c_i r_i (1+\alpha)^2}{[C + c_i(1+\alpha)]^2}$$
$$t_i^A = \frac{C r_i (1+\alpha)}{[C + c_i(1+\alpha)]^2}, \quad \frac{t_i^A}{T_i^A} = \frac{C}{c_i(1+\alpha)} \tag{7}$$

Proposition 2. *Information sharing and aggregate attack are interlinked through the interdependence and the firm's unit cost of security investment. Both increase in the interdependence,* $\partial s_i/\partial\alpha > 0$ *when* $\alpha > 0$, *and* $\partial T_i^A/\partial\alpha > 0$. *Information sharing increases in the unit cost,* $\partial s_i/\partial c_i > 0$. *The aggregate attack increases (decreases) in the firm's unit cost when it is low (high). That is,* $\partial T_i^A/\partial c_i > 0$ *when* $c_i < C/(1+\alpha)$, *and* $\partial T_i^A/\partial c_i < 0$ *otherwise.*

Proof. Follows from (6), (7) and Appendix 1. □

As the interdependence between firms increases, the agent realizes that an attack launched against one firm gets propelled further to the other firm. Hence the aggregate attack increases in the interdependence. Each firm responds by increasing its information sharing. Hence both aggregate attack and information sharing increase in the interdependence between firms. The results are mixed for the aggregate defense which consists of both security investment and information sharing. The aggregate defense increases in the interdependence when the unit cost of security investment is low, $\partial t_i^A/\partial\alpha > 0$ when $c_i < C/(1+\alpha)$, and decreases when it is high, $\partial t_i^A/\partial\alpha < 0$ when $c_i > C/(1+\alpha)$, (see (A.13)). When the unit cost is low, each firm can afford a large security investment, which takes care of a major part of the aggregate defense as the interdependence increases. Hence when c_i is low, aggregate attack, information sharing, and aggregate defense increase in α. When the unit cost is high, each firm cannot afford a large security investment. Instead it has to rely on information sharing taking care of part of the defense. Hence when c_i is high, aggregate attack and information sharing increase in α, while aggregate defense decreases in α.

As the firm's unit cost of security investment increases, its aggregate defense gets shifted from security investment to information sharing. The aggregate defense decreases, $\partial t_i^A/\partial c_i < 0$, and information sharing increases, $\partial s_i/\partial c_i > 0$. The agent responds to this in a mixed manner. When c_i is low, the aggregate defense is overwhelming, and the agent launches a small attack which increases in c_i and reaches a maximum. As c_i increases further, the aggregate defense weakens, and the agent can cash in on its attack by reducing it. Hence when c_i is low, aggregate attack and information sharing increase in c_i. When c_i is high, information sharing increases in c_i, while aggregate attack decreases in c_i. Aggregate defense always decrease in c_i, and aggregate attack decrease in C.

Assume that $c_i < C/(1+\alpha)$, which is a weak position for the agent. This means that the agent's unit cost of attack is high, the firm's unit cost is low, and the interdependence is low. In this case the agent's aggregate attack increases in the firm's unit cost. Although burdened with a high C, the agent earns a competitive advantage from a larger attack as the firm gets burdened with a higher c_i which causes a lower aggregate defense, $\partial t_i^A/\partial c_i < 0$. When $c_i > C/(1+\alpha)$, the results are opposite. The stronger agent's position causes it to cash in on its attack as c_i increases.

Proposition 3. *The aggregate attack is inverse U shaped in the aggregate defense and equals zero when* $t_i^A > r_i(1+\alpha)/C$. *Information sharing is independent of the agent's unit cost* C, *and also independent of* r_i, r_j, ϕ_2. *The aggregate attack and defense depend on the same parameters, and are independent of the information sharing parameters* γ, ϕ_1, ϕ_2, ϕ_3, *and also independent of the other firm's characteristics* r_j, c_j. *The aggregate defense increases (decreases) in the agent's unit cost when it is low (high). That is,* $\partial t_i^A/\partial C > 0$ *when* $c_i > C/(1+\alpha)$, *and* $\partial t_i^A/\partial C < 0$ *otherwise.*

Proof. Follows from (6), (7) and (A.14). □

When the defense is weak, the agent is successful even with a modest attack. As the defense increases, so does the attack toward a maximum, and it thereafter decreases. When the defense is sufficiently strong, the agent gives up and refrains from attacking. To understand the considerable independence between information sharing and attack with six free choice variables, first consider the firm's perspective. If C or r_i changes, both the aggregate attack and defense change. In this case the firm changes its aggregate defense by changing its security investment t_i, while keeping its information sharing s_i unchanged. The firm's security investment in (A.7) depends on all the 10 parameters except ϕ_2 which plays a role in the firm profits. Consequently the aggregate attack does not depend on γ, ϕ_1, ϕ_2, ϕ_3. In other words, the firm's security investment is driven by a broad set of concerns encompassing all parameters (except ϕ_2), while the firm's information sharing is driven by a narrower set of concerns encompassing information sharing parameters, but not encompassing the agent's unit cost, the two firms' values, and ϕ_2. Security investment and information sharing by both firms generate aggregate defense for each firm which encompasses all the parameters except the information sharing parameters and the other firm characteristics r_j, c_j.

For the symmetric case $r_i = r_j = r$, $c_i = c_j = c$, $t_i = t_j = t$, $s_i = s_j = s$, $u_i = u_j = u$, this gives

$$t = \frac{Cr}{[C + c(1+\alpha)]^2} - \frac{c\alpha\gamma^2}{2\phi_1 - \phi_3} \geqslant 0, \quad s = \frac{c\alpha\gamma}{2\phi_1 - \phi_3}$$

$$T = \frac{cr(1+\alpha)}{[C + c(1+\alpha)]^2}$$

$$
\begin{aligned}
t_i^A &= \frac{Cr(1+\alpha)}{[C+c(1+\alpha)]^2}, \quad T_i^A = \frac{cr(1+\alpha)^2}{[C+c(1+\alpha)]^2}, \quad \frac{t_i^A}{T_i^A} = \frac{C}{c(1+\alpha)} \\
u &= \frac{C}{[C+c(1+\alpha)]} r - ct - (\phi_1 - \phi_2 - \phi_3)s^2 \\
u &= \frac{Cr(C+c\alpha)}{[C+c(1+\alpha)]^2} + \frac{c^2\alpha\gamma^2[(2-\alpha)\phi_1 + \alpha\phi_2 - (1-\alpha)\phi_3]}{(2\phi_1 - \phi_3)^2} \\
U &= \frac{2c^2 r(1+\alpha)^2}{[C+c(1+\alpha)]^2}
\end{aligned} \tag{8}
$$

Information sharing increases, and security investment decreases, in the interdependence. The firms' profit increases in the interdependence when the unit cost c is large, see (A.15), in which case information sharing is beneficial. The agent's profit increases in the interdependence, see (A.16), since both firms then can be attacked more thoroughly. Information sharing is independent of the agent's unit cost of attack C. Both the aggregate defense and the security investment are inverse U shaped in the agent's unit cost of attack, with maximum when $C = c(1+\alpha)$, and equals zero when C is too low or too high as determined by $t = 0$ i n (8). When the attack is too low, there is no need for the firms to be much concerned and they can get away with low security investment. Conversely, when the attack is too large, the firms get overwhelmed, their defense doesn't matter much, and security investment gets reduced, eventually to zero. The security investment and aggregate defense are maximum when the attack is large enough to pose a threat, while at the same time the firms can limit that threat by designing a sufficient defense. As C decreases, the attack gets more and more overwhelming, and security investment decreases to zero. Section 5 analyzes the case with exogenously given security investment, which causes information sharing to depend on C. For very low C, even information sharing is not worth while against a formidable attacker.

Policy advice 1. *Each firm shifts some of its emphasis from security investment to information sharing as the interdependence, unit cost of security investment, effectiveness of information sharing, or efficiency of joint leakage increase, or the inefficiency of own leakage decreases. The agent's unit cost of attack affects the security investment and aggregate defense in an inverse U shaped manner, but does not affect information sharing except when security investment is exogenously given or zero.*

As we develop this article, we exemplify the symmetric solution for the parameter values $\alpha = c = C = 0.5$, $\gamma = \phi_2 = 1$, $r = \phi_1 = 2$, $\phi_3 = 0$. Line 2 in Table 1 shows the equilibrium solution. Observe the very low information sharing $s = 0.0625$ due to free riding.

Table 1
Security investment, information sharing, attack, social welfare, and attacker profit in symmetric game where $\alpha = c = C = 0.5$, $\gamma = \phi_2 = 1$, $r = \phi_1 = 2$, $\phi_3 = 0$

Section	Optimization	t	s	T	w	U
3	Individual firm and agent optimization	0.5775	0.0625	0.96	1.015	1.44
5	Exogenously given security investment	0.9	0.044	0.999	1.039	1.058
6.1	Social planner controls information sharing: Two period game	0.39	0.25	0.96	1.085	1.44
6.2	Social planner controls information sharing: Simultaneous game	0.265	0.375	0.96	1.054	1.44
7	Social planner controls security investment: Simultaneous game	0.9583	0.042	1	1.038	1
8.1 and 8.2	Social planner controls both information sharing and security investment	0.75	0.25	1	1.125	1

4. Exogenously given information sharing

Gordon et al. (2003, p. 478) show that if firms are allowed to select their levels of information sharing, they will have incentives not to share any security information in Nash equilibrium. Eq. (6) shows that this also holds for the current model if the interdependence between firms is zero or negative ($\alpha \leqslant 0$), if the unit costs of security investment are zero ($c_i = c_j = 0$, rendering information sharing useless since security investment comes for free), or if the unit cost of own leakage is infinite ($\phi_1 = \infty$). In some cases information sharing may not be possible or obtainable. The firms may lack the logistics for compiling or transferring information. Alternatively, hostility between the firms may be such that information is not shared even when such sharing is rational for each firm. Other hurdles against information sharing are pressures from owners, shareholders, employees, or customers, of each firm, or firms with which each firm has contracts.

It is of interest to determine the impact of specifying information sharing exogenously. Assume that the two firms agree to given levels s_i and s_j of information sharing. This may occur through trust building between the two firms, or backed by or facilitated by SB/ISOs. The agent's FOCs are given by (A.2), and the firms' FOCs are the first two equations in (A.1), where s_i and s_j are now constants. Hence the first two equations in (A.5) are valid. Inserting these into (A.3) and (A.4) and applying (5) gives

$$t_i^A = \frac{Cr_i(1+\alpha)}{[C + c_i(1+\alpha)]^2}, \quad T_i^A = \frac{c_i r_i (1+\alpha)^2}{[C + c_i(1+\alpha)]^2}$$
$$t_j^A = \frac{Cr_j(1+\alpha)}{[C + c_j(1+\alpha)]^2}, \quad T_j^A = \frac{c_j r_j (1+\alpha)^2}{[C + c_j(1+\alpha)]^2} \tag{9}$$

as in (7), written in terms of aggregate defense and attack. Solving (5) and (9) gives

$$
\begin{aligned}
t_i &= \frac{C}{1-\alpha}\left. \frac{r_i}{[C+c_i(1+\alpha)]^2} - \frac{\alpha r_j}{[C+c_j(1+\alpha)]^2} \right) - \gamma s_j \\
t_j &= \frac{C}{1-\alpha}\left. \frac{r_j}{[C+c_j(1+\alpha)]^2} - \frac{\alpha r_i}{[C+c_i(1+\alpha)]^2} \right) - \gamma s_i
\end{aligned} \tag{10}
$$

$$
\begin{aligned}
T_i &= \frac{(1+\alpha)}{(1-\alpha)}\left. \frac{c_i r_i}{[C+c_i(1+\alpha)]^2} - \frac{\alpha c_j r_j}{[C+c_j(1+\alpha)]^2} \right) \\
T_j &= \frac{(1+\alpha)}{(1-\alpha)}\left. \frac{c_j r_j}{[C+c_j(1+\alpha)]^2} - \frac{\alpha c_i r_i}{[C+c_i(1+\alpha)]^2} \right)
\end{aligned} \tag{11}
$$

and the profits are

$$
\begin{aligned}
u_i &= \frac{C}{C+c_i(1+\alpha)} r_i - c_i t_i - (\phi_1 s_i^2 - \phi_2 s_j^2 - \phi_3 s_i s_j) \\
u_j &= \frac{C}{C+c_j(1+\alpha)} r_j - c_j t_j - (\phi_1 s_j^2 - \phi_2 s_i^2 - \phi_3 s_i s_j) \\
U &= \frac{c_i(1+\alpha)}{C+c_i(1+\alpha)} r_i + \frac{c_j(1+\alpha)}{C+c_j(1+\alpha)} r_j - C(T_i + T_j)
\end{aligned} \tag{12}
$$

The agent's attacks and profit depend on the aggregate defense t_i^A and t_j^A, and not on how the firms allocate between security investment and information sharing. Hence T_i, T_j, U depend on parameters only, and not on s_i and s_j. In (10), $t_i + \gamma s_j$ and $t_j + \gamma s_i$ also depend on parameters only. One firm's security investment and the other firm's information sharing are strategic substitutes. Increasing one decreases the other and vice versa.

Policy advice 2. *By increasing its information sharing, one firm causes a decrease in the other firm's security investment. Conversely, by decreasing its information sharing, one firm causes an increase in the other firm's security investment. The aggregate defense and attack, and the agent's profit, remain unchanged as a consequence of altering information sharing exogenously.*

But the firms' profits depend on information sharing. To determine how, we determine the first and second derivatives of the profits for each firm, where s_i and s_j are now variables,

$$
\frac{\partial u_i}{\partial s_i} = -2\phi_1 s_i + \phi_3 s_j, \quad \frac{\partial^2 u_i}{\partial s_i^2} = -2\phi_1, \quad \frac{\partial u_j}{\partial s_j} = -2\phi_1 s_j + \phi_3 s_i, \quad \frac{\partial^2 u_j}{\partial s_j^2} = -2\phi_1 \tag{13}
$$

Setting the two FOCs in (13) equal to zero and solving gives $s_i = s_j = 0$. This can be interpreted as the solution of a two period game where the firms choose information sharing independently and simultaneously in the first period, while the firms and agent choose security investments and attacks independently and simultaneously in the second period. Such a game is solved with backward recursion, starting with the second period which gives the solution in (10) and (11), and proceeding with the first period which gives $s_i = s_j = 0$. This means that not even interdependence between firms can generate information sharing when the firms are requested to choose information sharing up front in the first period, postponing security investments and attacks to the second period.

Consider firm i and assume that information sharing by firm j is exogenously positive, $s_j > 0$. Eq. (13) shows that firm i's profit increases in s_i when $s_i = 0$, reaches a maximum when $s_i = \phi_3 s_j / 2\phi_1$, and decreases when $s_i > \phi_3 s_j / 2\phi_1$. That is, firm i's profit is inverse U shaped in its own information sharing. The problem is that firm i does not have any incentives to share information in the two period game described here. Hence we introduce a social planner.

5. Exogenously given security investment

As an alternative to given or imposed information sharing, assume fixed security investment. This may most commonly occur through budget constraints within firms, but may also be imposed by managerial decision, or an agreement between firms, or other kinds of agreements, policies, laws, procedures. For example, the Chief Financial Officer (CFO) may inform the Chief Information Security Officer (CISO) that this year's budget allows for a certain security investment. A firm experiencing liquidity problems or other kinds of hardship may very well decide that security investment has to be pushed downwards, possibly toward zero, in a given year. Conversely, the CFO may in a given year decide that security investment is especially important, e.g. as a signal to customers, competitors, or others, and may inform the CISO that security investment is going to be especially high this year, without regard for what is optimal with respect to profit maximization. Faced with such a constraint, the CISO has to resort to his second free choice variable, information sharing, to maximize profits. We consider the symmetric case to ensure tractability. The two last equations in (A.1) are the FOCs for information sharing when security investment is exogenously given. Solving these together with the two equations in (A.2) when $r_i = r_j = r$, $t_i = t_j = t$, $s_i = s_j = s$, $T_i = T_j = T$ gives

$$t = \frac{Cr\alpha^2\gamma^2}{[C\alpha\gamma + s(1+\alpha)(2\phi_1 - \phi_3)]^2} - \gamma s, \quad T = \frac{rs\alpha\gamma(1+\alpha)(2\phi_1 - \phi_3)}{[C\alpha\gamma + s(1+\alpha)(2\phi_1 - \phi_3)]^2} \tag{14}$$

We express t as a function of s rather than vice versa to avoid the third order equation in s. In the other sections in this article, the aggregate defense and the security investment depend on the attacker's unit cost of attack C, while information sharing does not. However, with exogenously given security investment, the only way to make the aggregate defense depend on C is to let information sharing depend on C. Differentiating (14) gives

$$\begin{aligned}
&\frac{\partial t}{\partial s} = -\gamma\left(1 + \frac{2Cr\alpha^2\gamma(1+\alpha)(2\phi_1-\phi_3)}{[C\alpha\gamma + s(1+\alpha)(2\phi_1-\phi_3)]^3}\right) < 0 \Rightarrow \frac{\partial s}{\partial t} < 0 \\
&\frac{\partial^2 t}{\partial s^2} = \frac{6Cr\alpha^2\gamma^2(1+\alpha)^2(2\phi_1-\phi_3)^2}{[C\alpha\gamma + s(1+\alpha)(2\phi_1-\phi_3)]^4} > 0 \Rightarrow \frac{\partial^2 s}{\partial t^2} > 0 \\
&\frac{\partial T}{\partial s} = \frac{r\alpha\gamma(1+\alpha)(2\phi_1-\phi_3)[C\alpha\gamma - s(1+\alpha)(2\phi_1-\phi_3)]}{[C\alpha\gamma + s(1+\alpha)(2\phi_1-\phi_3)]^3} > 0 \\
&\quad \text{when } s < \frac{C\alpha\gamma}{(1+\alpha)(2\phi_1-\phi_3)} \\
&\frac{\partial^2 T}{\partial s^2} = -\frac{2r\alpha\gamma(1+\alpha)^2(2\phi_1-\phi_3)^2[2C\alpha\gamma - s(1+\alpha)(2\phi_1-\phi_3)]}{[C\alpha\gamma + s(1+\alpha)(2\phi_1-\phi_3)]^4} < 0 \\
&\quad \text{when } s < \frac{2C\alpha\gamma}{(1+\alpha)(2\phi_1-\phi_3)}
\end{aligned} \tag{15}$$

which shows that the attack is inverse U shaped in information sharing. Eq. (14) reduces to (8) when t has the equilibrium value in (8). Since t and s are strategic substitutes, decreasing (increasing) t below (above) this equilibrium value, causes s to increase (decrease). Line 3 in Table 1 shows the equilibrium solution with high exogenously given security investment $t = 0.9$. The firms free ride on information sharing, $s = 0.044$, but welfare increases to $w = 1.039$. Fig. 2 illus-

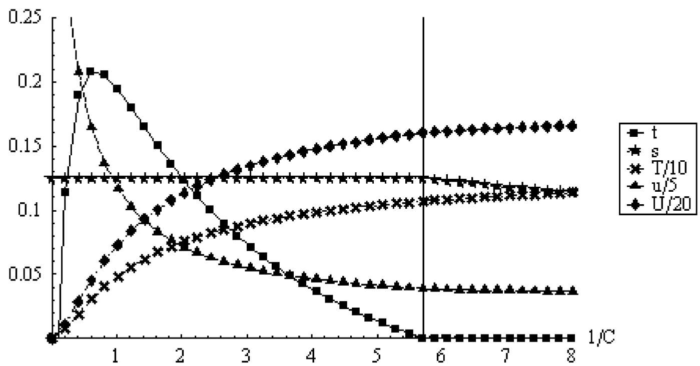

Fig. 2. t, s, T, u, U as functions of the agent's attack efficiency $1/C$, cf. Section 5.

trates with the same parameters as in Table 1 except that $c = 1$ which is disadvantageous for the firms by reducing t quickly to zero when $1/C > 5.70$. Security investment is inverse U formed in $1/C$, consistently with Section 3. Observe how information sharing when $1/C < 5.70$ is constant at $s = 0.125$ independent of $1/C$, consistently with (8), and decreases when $1/C > 5.70$, consistently with this section and the inverse U form for the aggregate defense.

6. Social planner controls information sharing

6.1. Two period game

For the issues regarding information sharing, especially in economic analysis, we care about the implication for public policy. Today's governments are concerned about the operation of information sharing organizations. Welfare analysis is needed to show how regulation in the level of sharing affects the social welfare. Since the model allows cyber attacks to be variable, the regulation about sharing depends upon the level of attacks. A social planner maximizes the joint profit $w = u_i + u_j$ of the two firms. This section assumes that the social planner controls the information sharing variables s_i and s_j, but not the security investment variables t_i and t_j, which are still controlled by the firms. There are thus four strategic actors who choose their free choice variables optimally given the other actors' choices. The external agent's free choice variable are as before, T_i and T_j. Essential in welfare analysis is a comparison of the social optimal and each individual firm's optimal levels of information sharing to see whether the social planner's regulation is more socially beneficial than each individual firm's free decisions. That is, will each firm's self-regulation result in an under-provided level of information sharing?

This section assumes that the social planner chooses information sharing simultaneously for both firms in the first period, while the firms and agent choose security investments and attacks independently and simultaneously in the second period. This two period game is realistic when a credible social planner, such as a SB/ISO, can commit the two firms in advance to the specified information sharing levels. The commitment would operate especially well if it could be implemented in enforceable laws and procedures backed with sanctions and punishment for noncompliance. This usually requires a social planner who has built up a reputation over a long term perspective, is well respected, and whose recommendations are taken seriously. If such a commitment is sufficiently strong, the levels of information sharing specified by the social planner in the first period are taken as given, carved in stone of you like, by the firms and agent when they choose their free choice variables in the second period. Defenses are usually built up over time and it is usually realistic that the social planner moves first and the agent second.[6]

Solving with backward recursion, the second period solution is given by (10) and (11). For the first period, inserting (12) into $w = u_i + u_j$ and differentiating gives

$$\frac{\partial w}{\partial s_i} = \gamma c_j - 2[(\phi_1 - \phi_2)s_i - \phi_3 s_j] = 0, \quad \frac{\partial w}{\partial s_j} = \gamma c_i - 2[(\phi_1 - \phi_2)s_j - \phi_3 s_i] = 0 \tag{16}$$

which are solved to yield

$$\tilde{s}_i = \frac{\gamma[(\phi_1 - \phi_2)c_j + \phi_3 c_i]}{2(\phi_1 - \phi_2 - \phi_3)(\phi_1 - \phi_2 + \phi_3)}, \quad \tilde{s}_j = \frac{\gamma[(\phi_1 - \phi_2)c_i + \phi_3 c_j]}{2(\phi_1 - \phi_2 - \phi_3)(\phi_1 - \phi_2 + \phi_3)} \tag{17}$$

which is independent of α, where a curved line above a variable expresses welfare analysis when the social planner controls information sharing in a two period game.

Proposition 4. (*i*) *With equal unit costs $c_i = c_j$ of security investment, social optimal information sharing in a two period game is $\tilde{s}_i = c_i\gamma/[2(\phi_1 - \phi_2 - \phi_3)]$, which is more than $1/\alpha$ times higher than the individual optimum.* (*ii*) *When $c_i = c_j$, the social welfare loss from free riding in information sharing is*

$$\widetilde{L} = \tilde{w} - w = \frac{c_i^2\gamma^2[2\phi_1 - 2\alpha(\phi_1 - \phi_2 - \phi_3) - \phi_3]^2}{2(\phi_1 - \phi_2 - \phi_3)(2\phi_1 - \phi_3)^2} \tag{18}$$

which is always positive, where $\partial\widetilde{L}/\partial\alpha < 0, \partial\widetilde{L}/\partial c_i > 0, \partial\widetilde{L}/\partial\gamma > 0$. (*iii*) *With unit cost $c_j = 0$ of security investment for the other firm j, and $\phi_2 = \phi_3 = 0$, the social optimum for firm i is $\tilde{s}_i = 0$ and $\tilde{s}_j = c_i\gamma/2\phi_1$, and the individual optimum is $s_i = c_i\alpha\gamma/2\phi_1$ and $s_j = 0$.*

Proof. See Appendix 2. □

Individually chosen information sharing depends crucially on the interdependence between firms. It equals zero with no interdependence, and increases proportionally. In contrast, social optimal information sharing in a two period game

[6] This paper does not analyze the case that the agent moves first, although that case is also possible, e.g. when a hacker announces up front that a new attack will occur at some point in the future (or simply commits resources to such an attack). In some such cases the social planner may have to operate in an emergency response mode.

is independent of the interdependence. This explains that the social optimum is more than $1/\alpha$ times higher than the individual optimum when $c_i = c_j$, which is high for low interdependence and equals infinity with no interdependence.

The social welfare loss from free riding in information sharing is always positive when $c_i = c_j$. Naturally, the loss decreases in the interdependence which increases the individual optimum. Both optima increase in c_i and γ which cause relative advantage to information sharing over security investment. But, a social planner is better equipped to benefit from this relative advantage, so the welfare loss increases in c_i and γ.

Proposition 4(iii) illustrates that a social planner does not always recommend more information sharing. Consider the special case where the other firm has zero unit cost of security investment, $c_j = 0$. The other firm then does not share information, $s_j = 0$, and firm i prefers individually to share at $s_i = c_i\alpha\gamma/2\phi_1$, see Section 3. The social planner imposes information sharing $\tilde{s}_i = 0$ and $\tilde{s}_j = c_i\gamma/2\phi_1$ when $\phi_2 = \phi_3 = 0$. Contrary to Section 3, the social planner imposes no information sharing on firm i (recall that $\phi_2 = \phi_3 = 0$ is a special case), which is far less than the individual optimum, and substantial information sharing on firm j. The social planner does not tolerate the free riding of firm j caused by $c_j = 0$. The sum of information sharing for the two firms is nevertheless higher with than without a social planner also for this case, but only when $\alpha < 1$. Although $c_j = 0$ is a special case, it illustrates that when the unit cost of security investment is substantially less for the other firm, so that it would like to free ride, then the first firm prefers to share more information individually than what a social planner recommends, while the reverse is the case for the other firm since the social planner does not tolerate free riding.

For the symmetric case $r_i = r_j = r$, $c_i = c_j = c$, the solution is

$$t = \frac{Cr}{[C + c(1+\alpha)]^2} - \frac{c\gamma^2}{2(\phi_1 - \phi_2 - \phi_3)} \geqslant 0$$
$$s = \frac{c\gamma}{2(\phi_1 - \phi_2 - \phi_3)}, \quad T = \frac{cr(1+\alpha)}{[C + c(1+\alpha)]^2}$$
$$t_i^A = \frac{Cr(1+\alpha)}{[C + c(1+\alpha)]^2}, \quad T_i^A = \frac{cr(1+\alpha)^2}{[C + c(1+\alpha)]^2}, \quad \frac{t_i^A}{T_i^A} = \frac{C}{c(1+\alpha)}$$
$$u = \frac{Cr(C + \alpha c)}{[C + c(1+\alpha)]^2} + \frac{c^2\gamma^2}{4(\phi_1 - \phi_2 - \phi_3)}, \quad w = 2u, \quad U = \frac{2c^2r(1+\alpha)^2}{[C + c(1+\alpha)]^2} \tag{19}$$

Line 4 in Table 1 shows the equilibrium solution. Information sharing increases four times to $s = 0.25$ as enforced by the social planner. However, the firms respond by free riding on security investment, which decreases from $t = 0.5775$ to $t = 0.39$. The aggregate attack and defense remain unchanged, so the attacker's profit remains unchanged. However, the social welfare, and thus the profit for each firm, increases to $w = 1.085$, in accordance with Proposition 4. Removing free riding on information sharing causes increased information leakage costs, but these are lower than the gains from reduced security investment.

The concern of the social planner is how to regulate the level of sharing in responding to certain level of attacks, in order to maximize the social welfare. Assuming that the firms retain their equilibrium security investment $t = 0.39$ determined by (19), Fig. 3 illustrates how the social welfare $w = 2u$ depends on information sharing s and attack T, determined by inserting the equilibrium value of t into Eq. (4) for the symmetric case allowing s and T to be free variables. The welfare of course increases as the attack decreases. But, as the attack decreases, note that the inverse U shape as a function of information sharing broadens. Too low information sharing is dysfunctional since a firm can boost its aggregate defense through information sharing. Too high information sharing is also dysfunctional since the information sharing leakage costs become unbearable. Of course, when $T = 0$, w decreases throughout in s since information sharing is not necessary and only causes costs when there is no attack. Fig. 3 assumes $\alpha = 0.5$, but visual inspection of Fig. 3 for other values of α suggests that it is qualitatively similar also for other values of the interdependence.

6.2. Simultaneous game

Many of today's SB/ISOs are in a buildup phase. Their influence is increasing and they may become successful in the future. Whether their recommendations get the strength of law backed by sanctions remains to be seen. It is thus

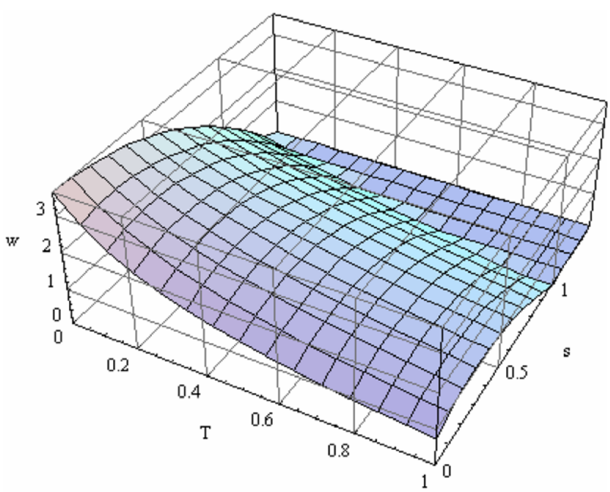

Fig. 3. The social welfare w as a function of information sharing s and attack T, cf. Section 6.1.

of interest to analyze the case where the SB/ISO, the two firms, and the attacking agent operate simultaneously. No actor is a first mover. Nothing can be taken as given ahead of anything else. The actors have a short term perspective, or more specifically a static time perspective where they adapt to each other at a specific point in time. Appendix 3 determines the six FOCs, the six choice variables, and the profits. Information sharing in (A.21) is

$$\hat{s}_i = \frac{\gamma[(\phi_1 - \phi_2)(c_j + \alpha c_i) + \phi_3(c_i + \alpha c_j)]}{2(\phi_1 - \phi_2 - \phi_3)(\phi_1 - \phi_2 + \phi_3)} \tag{20}$$

where a hat above a variable expresses welfare analysis when the social planner controls information sharing in a simultaneous game.

Proposition 5. (*i*) *Social optimal information sharing in a simultaneous game is always higher than the social optimum in a two period game,* $\hat{s}_i \geqslant \tilde{s}_i$, *and always higher than the individual optimum.* (*ii*) *With equal unit costs* $c_i = c_j$ *of security investment, social optimal information sharing is* $\hat{s}_i = c_i(1+\alpha)\gamma/[2(\phi_1 - \phi_2 - \phi_3)]$, *which is* $1 + \alpha$ *times higher than* $\tilde{s}_i$, *and more than* $(1 + \alpha)/\alpha$ *times higher than the individual optimum.* (*iii*) *The social welfare in a two period game minus the social welfare in a simultaneous game is*

$$\widehat{L} = \tilde{w} - \hat{w} = \frac{\alpha^2\gamma^2[(c_i^2 + c_j^2)(\phi_1 - \phi_2) + 2c_ic_j\phi_3]}{4(\phi_1 - \phi_2 - \phi_3)(\phi_1 - \phi_2 + \phi_3)} \tag{21}$$

which is always positive. (*iv*) *When* c_i c_j *and* $\phi_2 = \phi_3 = 0$, *the social welfare in a simultaneous game minus the social welfare in the absence of a social planner is* $\hat{w} - w = c_i^2\gamma^2(1 - 2\alpha)/2\phi_1$, *which is positive when* $\alpha < 1/2$. (*v*) *When* $c_j = 0$ *for firm j, and* $\phi_2 = \phi_3 = 0$, *the social and individual optima coincide at* $s_i = \alpha\gamma c_i/2\phi_1$. (*vi*) *The aggregate defense is the same for individual optimization and when a social planner controls information sharing in a two period or simultaneous game, though profits change.*

Proof. (i)–(v) See Appendix 3. (vi) Follows from comparing (A.7), (10) and (A.22). □

Proposition 5 shows that it is collectively beneficial if the social planner can dictate information sharing in advance in a two period game, rather than operating simultaneously with the firms and the agent in a simultaneous game. In the simultaneous game the social planner dictates information sharing that is higher than in the two period game, which causes the firms to free ride more in their security investment. Since the aggregate defense and attack are the same in the simultaneous and two period game, the firms compensate for the required high information sharing in the simultaneous game by reducing security investment so that t_i^A and t_j^A remain unchanged. Hence a simultaneous game can be quite dysfunctional. The social planner knows that it can dictate information sharing, but it cannot do so in advance. It compensates for this by recommending an unreasonably high level of information sharing, and more unreasonable when the interdependence is high, causing the firms to free ride. Interestingly, without interdependence between firms, $\alpha = 0$, the simultaneous and two period game recommend the same levels of information sharing, $\hat{s}_i = \tilde{s}_i$, which is higher than $s_i = 0$ for the individual optimum.

With equal unit costs $c_i = c_j$ of security investment, the social planner in a simultaneous game imposes at least twice as much information sharing as the firms would individually choose with interdependence $\alpha = 1$, at least three times as much when $\alpha = 1/2$, and substantially more with low interdependence and as ϕ_2 increases, see (20). Recall that ϕ_2 is the efficiency of the other firm's leakage, which the social planner knows how to benefit from.

A special case emerges when the other firm has zero unit cost of security investment, $c_j = 0$. The other firm then does not need to share information, $s_j = 0$, and firm i prefers to share at $s_i = c_i\alpha\gamma/2\phi_1$, when given individual choices and $\phi_3 = 0$, see (6). The social planner imposes information sharing $\hat{s}_i = c_i\alpha\gamma/2\phi_1$ and $\hat{s}_j = c_i\gamma/2\phi_1$ when $\phi_2 = \phi_3 = 0$. Hence the only case when the social planner imposes information sharing down toward that level chosen individually by a firm, is when the other firm has very low unit cost of security investment.

We know from Section 6.1 that the firms always prefer a social planner in a two period game. Proposition 5 specifies that they do not always prefer a social planner in a simultaneous game. The question is whether each firm prefers a social planner which causes increased leakage costs due to high information sharing but also reduced cost of security investment due to free riding. Using (A.9) and (A.24), the social welfare with a social planner minus the social welfare without a social planner when $c_i = c_j$ is

$$\begin{aligned}\hat{w} - w = {} & [c_i^2\gamma^2(4(1-2\alpha)\phi_1^2 + \phi_3^2 - 4\alpha\phi_3(\phi_2 + \phi_3) \\ & + \alpha^2(4\phi_2^2 + 8\phi_2\phi_3 + 3\phi_3^2) - 4\phi_1(\phi_3 + \alpha^2(2\phi_2 + \phi_3) \\ & - \alpha(2\phi_2 + 3\phi_3)))]/[2(\phi_1 - \phi_2 - \phi_3)(2\phi_1 - \phi_3)^2] \end{aligned} \tag{22}$$

which is positive when

$$\hat{w} - w > 0 \quad \text{when } \alpha < \frac{2\phi_1 - \phi_3}{4\phi_1 - 2\phi_2 - 3\phi_3} = \alpha_T \tag{23}$$

where $\alpha_T \geqslant 1/2$. This means that the firms prefer a social planner controlling information sharing only when the interdependence is lower than α_T. When the interdependence is higher than α_T, the unreasonably high degree of information sharing imposed by the social planner operating simultaneously causes too much leakage costs. The firms respond by free riding substantially on security investment, lowering the cost of security investment. However, the information sharing leakage costs are already unbearable for the firms when α is high. Hence we propose the following policy advice.

Policy advice 3. *A social planner that controls information sharing in a simultaneous game is advised to assess the interdependence* α *between the firms in relation to the information leakage parameters* ϕ_1, ϕ_2, ϕ_3 *as determined by* (23). *When the interdependence is high,* $\alpha > \alpha_T$, *the firms are collectively better off if they are allowed to regulate their information sharing themselves without external interference, or if a social planner can be generated which operates in advance in a two period game. When the interdependence is low,* $\alpha < \alpha_T$, *and especially for firms that operate in isolation from each other without interdependence, a social planner regulating information sharing is collectively beneficial.*

Line 5 in Table 1 shows the equilibrium solution. Information sharing increases 50% to $s = 0.375$. Preventing the social planner to behave in advance causes it to impose a suboptimally high level of information sharing. The firms respond by free riding even more on security investment, which decreases to $t = 0.265$. The social welfare decreases to $w = 1.054$.

7. Social planner controls security investment: simultaneous game

The 2002 Sarbanes-Oxley Act places strict requirements on firms, such as establishing and maintaining adequate internal controls for financial reporting, and assessing annually the effectiveness of those controls. SB/ISOs encourage firms to share information. The future will likely show attempts to work incentives, inducements, and possibly requirements to share information, into laws and regulations. Given the plethora of requirements for firms, a possible further development is to induce or require firms to invest in security in certain manners. One example is requirements that certain security installations and procedures have to be in place, analogous to airlines being required to meet certain minimum standards. Another example is requirements to invest a certain percentage of profit into security, analogous to taxation, or to invest certain amounts determined by the size, type, nature, or other characteristics of the firm. Security investment may alternatively be controlled by a budget imposed or dictated by someone else than the decision makers within the firm who usually make optimizing decisions. For example, the budget may be determined by the CEO overruling the CISO who may usually make security decisions, or determined in some manner within the firm influenced by historic events or future goals or external conditions, or determined by shareholders, or determined by laws and regulations designed to reach societal or other goals. We refer to these examples as the case when the social planner determines security investment. This case constitutes an interesting and clear benchmark. More specifically, this section assumes that the social planner controls security investment, the firms control information sharing, and the attacker controls the attack. Appendix 4 determines the solution.

The symmetric solution is

$$
\begin{aligned}
&t = \frac{Cr}{(C+c)^2} - \frac{c\alpha\gamma^2}{(1+\alpha)(2\phi_1 - \phi_3)} \geqslant 0 \\
&s = \frac{c\alpha\gamma}{(1+\alpha)(2\phi_1 - \phi_3)}, \quad T = \frac{cr}{[C+c]^2} \\
&t_i^A = \frac{Cr(1+\alpha)}{[C+c]^2}, \quad T_i^A = \frac{cr(1+\alpha)}{[C+c]^2}, \quad \frac{t_i^A}{T_i^A} = \frac{C}{c} \\
&u = \frac{C^2 r}{(C+c)^2} + \frac{c^2\alpha\gamma^2[(2+\alpha)\phi_1 + \alpha\phi_2 - \phi_3]}{(1+\alpha)^2(2\phi_1 - \phi_3)^2}, \quad w = 2u, \quad U = \frac{2c^2 r}{[C+c]^2}
\end{aligned}
\tag{24}
$$

Proposition 6. (*i*) *Firm i's individually optimal information sharing in a simultaneous game when the social planner controls security investment, but not information sharing, is lower than in the individual optimization case without the social planner's control when* $c_i < c_j(2\phi_1 - \alpha\,\phi_3)/(2\alpha\phi_1 - \phi_3)$, *which is satisfied in the symmetric case when* $\alpha < 1$. (*ii*) *The social planner dictates more security investment than when the firms optimize individually.*

Proof. (i) Follows from comparing (A.27) and (6). (ii) The first positive term in the expression for t in (24) is larger than the corresponding first term in (8). The second negative term in the expression for t in (24) has smaller absolute value than the corresponding second term in (8). □

Note that $(2\phi_1 - \alpha\phi_3)/(2\alpha\phi_1 - \phi_3) \geqslant 1$. This proposition shows that unless one's own unit cost of security investment is sufficiently higher than in the other firm, a firm free rides even more on information sharing when security investment is dictated by a social planner. Line 6 in Table 1 shows how the social planner increases security investment to the extremely high level $t = 0.958$. This is reminiscent of Section 6.1 where the social planner chooses extremely high information sharing. That is, the social planner imposes a high value for the variable it controls, and the firms respond by free riding and choosing a low value for the variable they control. As the social planner chooses high t, the firms choose very low information sharing $s = 0.042$. The social welfare is $w = 1.038$, slightly lower than when t is given at $t = 0.9$.

Policy advice 4. *A social planner or budget controlling only security investment should be aware that dictating high security investment causes the firms to free ride more on information sharing than if the firms control both security investment and information sharing.*

The third order equation for s in (14) implies that a two period game where the social planner controls security investment is analytically cumbersome, and is not analyzed.

8. Social planner controls both information sharing and security investment

The results in the previous sections raise the issue of whether a social planner should be allowed to control both information sharing and security investment. The firms can then free ride neither on information sharing nor on security investment. This leaves the firms without free choice variables, while the social planner has four free choice variables t_i, s_i, t_j, s_j, and maximizes the joint profit $w = u_i + u_j$ of the two firms. The external agent's free choice variable are as before, T_i and T_j.

8.1. Simultaneous game

We first consider the simultaneous game. Appendix 5 determines the six FOCs, the six choice variables, and the three profits. Information sharing in (A.33) is

$$\bar{s}_i = \frac{\gamma[(\phi_1 - \phi_2)c_j + \phi_3 c_i]}{2(\phi_1 - \phi_2 - \phi_3)(\phi_1 - \phi_2 + \phi_3)} = \tilde{s}_i \tag{25}$$

which happens to be equivalent to the information sharing in the two period game in (17) in Section 6.1 where the social planner controls information sharing in a two period game. A bar above a variable expresses welfare analysis when the social planner controls both information sharing and security investment.

Proposition 7. (*i*) *Social optimal information sharing when the social planner controls both information sharing and security investment in a simultaneous game is equal to the social optimum in a two period game where the social planner controls only information sharing,* $\bar{s}_i = \tilde{s}_i$. (*ii*) *In the symmetric case* $r_i = r_j = r$, $c_i = c_j = c$, *the social welfare when the social planner controls both information sharing and security investment minus the social welfare in a two period game where the social planner controls only information sharing is*

$$\bar{w} - \tilde{w} = \frac{2\alpha c C r[C^2 - c^2 + \alpha c C]}{[C + c]^2[C + c(1+\alpha)]^2} > 0 \quad \text{when } c < \frac{C\left(\alpha + \sqrt{\alpha^2 + 4}\right)}{2} \tag{26}$$

Proof. (i) Follows from comparing (25) and (17). (ii) Follows from inserting (10), (11), (17) into (12) and applying $\tilde{w} = \tilde{u}_i + \tilde{u}_j$, and applying Appendix 5 for $\bar{w}$. □

When the social planner controls both information sharing and security investment, it refrains from imposing dysfunctionally high information sharing such as in the simultaneous game where the social planner controls only information sharing. Comparing (19) and (A.38), note that $\bar{t} > \tilde{t}$, which means that the social planner eliminates free riding in security investment, requiring the firms to invest more than when the firms individually choose security investment. Whether this gives higher profit for the firms depends also on the attacker, which the social planner does not control. When the attacker has a unit cost C of attack that is sufficiently high, as expressed with the rightmost inequality in (26), the firms prefer the simultaneous game where the social planner controls both information sharing and security investment. The reason is that the attacker draws an advantage from the two period game when its unit cost of attack is low, which enables it to launch a detrimental attack in the second period.[7]

The aggregate attack and defense are no longer the same when the social planner controls both information sharing and security investment, see (A.37) and (7). Comparing (A.38) and (8) for the symmetric case, the aggregate defense t_i^A increases, the aggregate attack T_i^A decreases, and the agent's profit U decreases. Hence the firms' profits u increases due to eliminating free riding. Both Eqs. (17) and (18) are positive, where we have inserted $C = c$ and $C = 0$ to simplify complex expressions. This means that for these special cases, it is beneficial to let a social planner control both information sharing and secu-rity investment. We propose the following policy advice.

Policy advice 5. *A social planner that controls both information sharing and security investment in a simultaneous game imposes less information sharing than a social planner that controls only information sharing, but more than the individual optimum. The reason is that a social planner controlling only information sharing compensates for not controlling security investment, to which the firms respond by free riding on security investment.*

Line 7 in Table 1 shows the equilibrium solution. Information sharing decreases back to $s = 0.25$, as in the two period game. But, security investment which is now controlled by the social planner increases substantially to $t = 0.75$. Hence no free riding. Neither the aggregate defense nor attack remain the same. The attacker responds to the improved defense by increasing the attack marginally from to $T = 1$, but earns a lower profit $U = 1$. The firms, however, enjoy the high social welfare $w = 1.125$.

[7] Many games can be envisioned when two firms, an attacker, and a social planner are involved. The author has analyzed some of these other games, but they are not included due to space constraints. For example, the social planner may choose information sharing and security investment in the first period, while the attacker chooses the attack in the second period, or vice versa. Alternatively, a three period game may be envisioned (which can be sequenced in six different ways). Also, a game can be envisioned where the social planner controls the attacker as well, though the social planner will then eliminate the attack.

To sum up our example, consider Fig. 4 which for the same parameter values shows the security investment and social welfare with individual optimization (Section 3), and when the social planner controls information sharing in a two period game (Section 6.1) and simultaneous game (Section 6.2). (The aggregate defense and attack remain the same.) Zero information sharing gives high security investment. As information sharing increases to the first vertical line $s = 0.0625$ (individual optimization), security investment decreases and social welfare increases. As information sharing increases to the second vertical line $s = 0.25$ (two period game), security investment decreases and social welfare increases to its maximum. As information sharing increases to the third vertical line $s = 0.375$ (simultaneous game), security investment decreases and social welfare decreases from its maximum.

8.2. Two period game

This section assumes that the social planner controls information sharing and security investment in the first period, while the attacker controls the attack in the second period. Appendix 6 gives the solution which is the same as for the simultaneous game for information sharing, while security investment and the attack are different. The symmetric case becomes

$$\begin{aligned}
&t = \frac{Cr}{4c^2} - \frac{c\gamma^2}{2(\phi_1 - \phi_2 - \phi_3)} \geqslant 0, \quad s = \frac{c\gamma}{2(\phi_1 - \phi_2 - \phi_3)}, \quad T = \frac{(2c - C)r}{4c^2} \geqslant 0 \\
&t_i^A = \frac{Cr(1+\alpha)}{4c^2}, \quad T_i^A = \frac{(2c - C)r(1+\alpha)}{4c^2}, \quad \frac{t_i^A}{T_i^A} = \frac{C}{2c - C} \\
&u = \frac{Cr}{4c} + \frac{c^2\gamma^2}{4(\phi_1 - \phi_2 - \phi_3)}, \quad w = 2u, \quad U = \frac{(2c - C)^2 r}{2c^2}
\end{aligned} \tag{27}$$

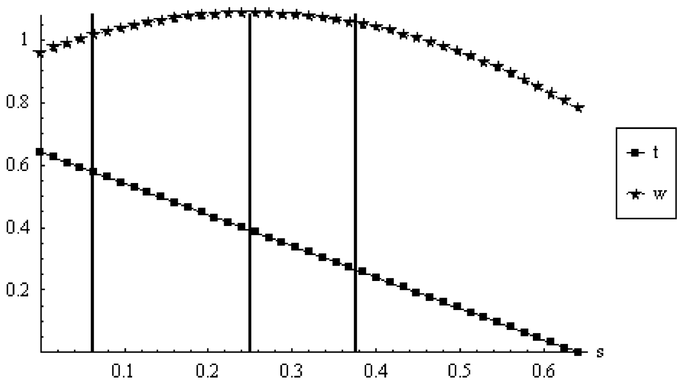

Fig. 4. Security investment and social welfare as functions of information sharing, cf. Section 8.1.

Proposition 8. (*i*) *Social optimal information sharing when the social planner controls both information sharing and security investment is the same in the two period and simultaneous game.* (*ii*) *In the symmetric case* $r_i = r_j = r$, $c_i = c_j = c$, $c < C$ *causes larger security investment and profit for the firms, and lower attack and profit for the agent, in the two period game than in the simultaneous game.*

Proof. (i) Follows from comparing (A.33) with Appendix 6. (ii) Follows from comparing (27) and (A.38). □

This proposition shows that when the defense efficiency $1/c$ of the firms is higher than the attack efficiency $1/C$ of the agent, then a social planner who controls both information sharing and security investment is more beneficial for the firms in a two period game than in a simultaneous game. Allowing a social planner to move first is beneficial for the firms when advantaged in terms of defense efficiency, but not when disadvantaged in terms of defense efficiency. As a second mover, the agent observes the high defense, and reduces the attack below that of the simultaneous game. Even more detrimentally to the agent, when $c \leqslant C/2$, the attack in (27) ceases, causing zero profit to the agent. Line 7 in Table 1 is for the two period and simultaneous game always equivalent for information sharing, but is for $c = C$ equivalent for all the variables.

Policy advice 6. *Allowing a social planner to control both information sharing and security investment in a two period game where the social planner moves first is the most beneficial control scenario when the firms' defense efficiencies are high. If these are sufficiently high, the attack is deterred altogether.*

9. Which games and control scenarios do the agent and social planner prefer

Table 2 shows the social welfare and agent profit for the various sections.

We first consider the agent. The agent profit is the same for Sections 3, 6.1, 6.2 since, as we observed in Section 4, the agent's attacks and profit depend on the aggregate defense, and not on how the firms allocate between security investment and information sharing. The agent profit is the same for Sections 7 and 8.1 for the same reason. In some cases, e.g. when the social planner has not committed to a defense in the first period, the agent may have a choice whether to attack simultaneously with the social planner, or to postpone the attack to the second period. Considering the symmetric case in Section 8 where the social planner controls both information sharing and security investment, the agent prefers the simultaneous game when the profit U in (A.38) is larger than the profit in the two period game in (27), that is, when

$$\frac{2c^2 r}{[C+c]^2} > \frac{(2c-C)^2 r}{2c^2} \Rightarrow c/C < 1 \tag{28}$$

Table 2
Social welfare w and agent profit U in symmetric game

Section	Optimization	w	U
3	Individual firm and agent optimization, (8)	$\frac{2Cr(C+c\alpha)}{[C+c(1+\alpha)]^2}+\frac{2c^2\alpha\gamma^2[(2-\alpha)\phi_1+\alpha\phi_2-(1-\alpha)\phi_3]}{(2\phi_1-\phi_3)^2}$	$\frac{2c^2r(1+\alpha)^2}{[C+c(1+\alpha)]^2}$
6.1	Social planner controls information sharing: Two period game, (19)	$\frac{2Cr(C+c\alpha)}{[C+c(1+\alpha)]^2}+\frac{c^2\gamma^2}{2(\phi_1-\phi_2-\phi_3)}$	$\frac{2c^2r(1+\alpha)^2}{[C+c(1+\alpha)]^2}$
6.2	Social planner controls information sharing: Simultaneous game, (A.25)	$\frac{2C(C+c\alpha)}{(C+c(1+\alpha))^2}r+\frac{c^2(1-\alpha^2)\gamma^2}{2(\phi_1-\phi_2-\phi_3)}$	$\frac{2c^2r(1+\alpha)^2}{[C+c(1+\alpha)]^2}$
7	Social planner controls security investment: Simultaneous game, (24)	$\frac{2C^2r}{(C+c)^2}+\frac{2c^2\alpha\gamma^2[(2+\alpha)\phi_1+\alpha\phi_2-\phi_3]}{(1+\alpha)^2(2\phi_1-\phi_3)^2}$	$\frac{2c^2r}{[C+c]^2}$
8.1	Social planner controls both information sharing and security investment: Simultaneous game, (A.38)	$\frac{2C^2r}{(C+c)^2}+\frac{c^2\gamma^2}{2(\phi_1-\phi_2-\phi_3)}$	$\frac{2c^2r}{[C+c]^2}$
8.2	Social planner controls both information sharing and security investment: Two period game, (27)	$\frac{Cr}{2c}+\frac{c^2\gamma^2}{2(\phi_1-\phi_2-\phi_3)}$	$\frac{(2c-C)^2r}{2c^2}$

When $c/C=1$, the equal unit costs cause the agents to be equally strong, and the agent is indifferent between the two games. As c/C decreases below 1, the social planner grows stronger. To prevent the social planner from exploiting its first mover advantage when in a stronger position, the agent prefers the simultaneous game. Conversely, as c/C increases above 1, the social planner becomes weaker, and the agent prefers to exploit or expose the social planner's weakness by letting it move first with modest and costly security investment.

We second consider the social planner. For the symmetric case in Section 8 where the social planner controls both information sharing and security investment, the social planner prefers the simultaneous game when the social welfare w in (A.38) is larger than the social welfare in the two period game in (27), that is, when

$$\frac{2C^2r}{(C+c)^2}+\frac{c^2\gamma^2}{2(\phi_1-\phi_2-\phi_3)}>\frac{Cr}{2c}+\frac{c^2\gamma^2}{2(\phi_1-\phi_2-\phi_3)}$$
$$\Rightarrow (C-c)^2<0, \quad \textit{never satisfied} \tag{29}$$

Hence the social planner unconditionally prefers the two period game, which requires more commitment as discussed in Section 6.1, and is indifferent between the two games when $c/C=1$.

The other control scenarios are more elaborate to compare, so let us consider variation relative to the baseline parameter values in Table 1, i.e. $\alpha=c=C=0.5$, $\gamma=\phi_2=1$, $r=\phi_1=2$, $\phi_3=0$. Fig. 5 lets α vary, and plots the social welfare and agent profit. The number behind the variables, w or U, refers to

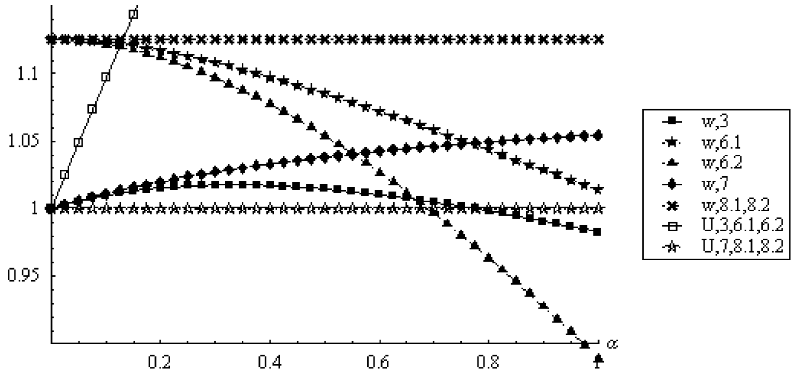

Fig. 5. Social welfare and agent profit as functions of interdependence α, cf. Section 9.

the section number. With individual optimization, or when the social planner controls information sharing, the agent's profit increases from 1. When the social planner controls security investment (regardless of whether also controlling information sharing), the agent earns lower profit at 1. The social welfare is lowest with individual optimization, with the one exception that the social planner controls information sharing in the simultaneous game and $\alpha > 2/3$. This finding is supported by Proposition 5 and the discussion thereafter in Section 6.2. Lacking control over security investment, the social planner dictates unreasonably large information sharing, especially when the interdependence is high, causing the firms to free ride, and to prefer individual optimization. However, social welfare is always higher when the social planner controls security investment, compared with individual optimization. With low interdependence, the firms prefer the social planner to control information sharing, and with high interdependence, the firms prefer the social planner to control security investment. The most preferable control scenario for the firms is that the social planner controls both information sharing and security investment.

Resetting $\alpha = 0.5$, Fig. 6 lets c vary. With individual optimization, or when the social planner controls information sharing, the agent's profit is highest when $c < 1$. In accordance with (28), when $c > 0.5$ the agent prefers the two period game where the social planner controls both information sharing and security investment, rather than the simultaneous game where the social planner controls at least security investment, and conversely when $c < 0.5$. The social welfare decreases in c towards a minimum and increases when c becomes especially large. The reason for this increase is that the firms substitute from especially costly security investment and into information sharing. Recall that $\gamma = 1$ means that information from the other firm is as valuable as own security investment when it comes to contesting the agent's attack. The social welfare is lowest with individual optimization, but here with the one exception that the social planner controls security investment in the simultaneous game and

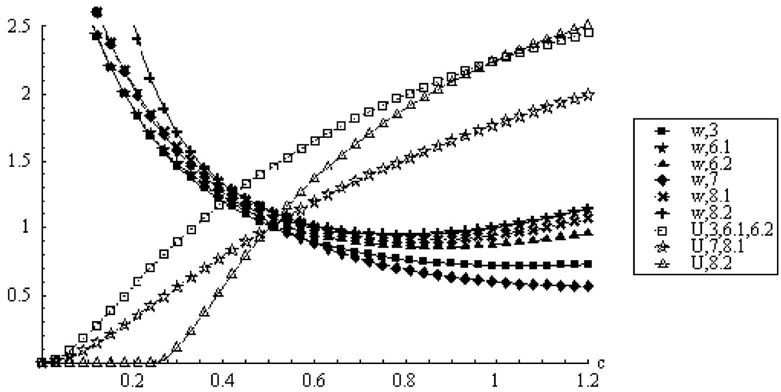

Fig. 6. Social welfare and agent profit as functions of unit cost c of investment, cf. Section 9.

$c > 0.56$. This finding is supported by Proposition 6(ii) which states that the social planner dictates more security investment than when the firms optimize individually. This is especially costly when the unit cost c of security investment is high, and the firms free ride on information sharing. The most beneficial control scenario for the social planner is to control both information sharing and security investment in a two period game, but controlling only information sharing in a two period game is also beneficial when the unit cost c of security investment is high. With high c this benefit is higher than when controlling both information sharing and security investment in a simultaneous game.

10. Conclusion

Information sharing and security investment gradually become more important for accounting and public policy. The establishment of Security Based Information Sharing Organizations, and the 2002 Sarbanes-Oxley Act, have strengthened internal controls. Accounting means representing information in certain formats and on chosen media, and administering controls for generating and disseminating information with tradeoffs between availability and confidentiality. Assessing costs and benefits of information sharing and security investment, interlinked with other strategies to gain competitive advantage, needs an accounting foundation. The security of an interlinked information system depends on the strategies about information sharing and security investment chosen by all actors, those that are players in it, those that attempt to regulate and reshape it, and those that attempt to shut it down, which opens a role for public policy.

This article considers two firms subject to cyber attacks by an external agent. The firms defend themselves by sharing information with each other, and investing in security. The agent chooses the optimal attacks, which is costly and consists in breaking through the security defense to appropriate something of value in the firms. The firms collect information about security breaches. Each firm prefers to receive information about the other firm's security breaches. Providing information to the other firm is costly because of the risk of leakage. The article analyzes the extent to which a firm has incentives to provide information voluntarily to the other firm, and the tradeoffs each firm makes between sharing information and investing in security.

The classical free rider dilemma explains why information sharing often does not occur, as also found by Gordon et al. (2003). This article shows that information sharing increases linearly in the interdependence between firms, and is zero with negative or no interdependence. The US telecommunications industry is highly interdependent, and also quite competitive, with substantial information sharing. We suggest that it is the interdependence between firms, and not the competitiveness, that is the key determinator of information sharing. Future empirical research may consider industries with different degrees of interdependence, competitiveness, and other characteristics to determine the impact on information sharing.

As the unit cost of security investment increases, a firm shifts its emphasis toward more information sharing to maintain its defense, given that the interdependence is positive. This shift is such that information sharing increases linearly more in one's own than in the other firm's unit cost of security investment. High unit cost of security investment, interdependence, and effectiveness of information sharing relative to security investment boost information sharing. Information sharing and aggregate attack are interlinked through the interdependence and the firm's unit cost of security investment. Both increase in the interdependence.

Security investment depends fundamentally on almost all the parameters in the model. In contrast, information sharing depends on fewer concerns which are the interdependence between firms, the information sharing parameters, and both firms' unit costs of security investment. A firm's aggregate defense, which is a weighted sum of information sharing and security investment, is inverse U shaped in the aggregate attack. When the defense is weak, the agent is successful even with a modest attack. As the defense increases, so does the attack toward a maximum, and it thereafter decreases. When the defense is sufficiently strong, the agent gives up and refrains from attacking. The security investment and aggregate defense are maximum when the attack is large enough to pose a threat, while at the same time the firms can limit that threat by designing a sufficient defense.

For the symmetric case, information sharing increases, and security investment decreases, in the interdependence. The agent's profit increases in the interdependence, since both firms then can be attacked more thoroughly. A main finding in this article is that high interdependence between firms facilitates information sharing. When, additionally, the unit cost of security investment is large, information sharing increases further. This suppresses free riding in information sharing, and the firms' profit increases in the interdependence. A two period game where the firms choose information sharing in the first period, while security investments and attacks occur in the second period, implies that not even interdependence between firms can generate information sharing.

Individual optimization implies free riding especially in information sharing, but also in security investment with positive interdependence since the firms cash in on each other's investments. Security Based Information Sharing Organizations (SB/ISOs) have emerged to facilitate increased information sharing. To understand the operation of such organizations, a social planner is analyzed which, together with budget control mechanisms, control information sharing only, security investment only, or both, in a simultaneous game, and two period game.

Two period games where the social planner moves in the first period are realistic when the social planner is reputed, when the recommendations are taken seriously, and especially when the recommendations are enforceable. In a two period game where the social planner chooses information sharing in the first period, and equal unit costs of security investment, social optimal information sharing is higher than the individual optimum, especially with low interdependence, and the social welfare loss from free riding in information sharing is positive. However, the firms respond by free riding more on security investment. Removing free riding on information sharing causes increased information leakage costs, but these are lower than the gains from reduced security investment.

When security investment is given, the social welfare is inverse U shaped in information sharing, and decreases in the attack. Too low information sharing is dysfunctional since a firm can boost its aggregate defense through information sharing. Too high information sharing is also dysfunctional since the information sharing leakage costs become unbearable.

In cases when SB/ISOs have limited reputation and capacity to operate in advance, a simultaneous game is realistic. The social welfare in a simultaneous game is lower than in the two period game since the social planner recommends unreasonably high information sharing in the simultaneous game, to which the firms respond by free riding more on security investment. The aggregate defense is the same for individual optimization and when a social planner controls information sharing in a two period or simultaneous game, though profits change.

A simultaneous game can be quite dysfunctional. The social planner knows that it can dictate information sharing, but it cannot do so in advance. It compensates for this by recommending an unreasonably high level of information sharing, and more unreasonable when the interdependence is high, causing the firms to free ride on security investment. Without interdependence, the simultaneous and two period game recommend the same levels of information sharing, which is higher than zero information sharing for the individual optimum.

The firms always prefer a social planner in a two period game where the social planner controls information sharing. Because of the very high information sharing imposed by a social planner in a simultaneous game, the firms prefer a social planner in a simultaneous game when the interdependence is low, since free riding in information sharing is then substantial, and otherwise prefer to self regulate information sharing.

These results raise the issue of whether a social planner, combined with various control and budget mechanisms, should control both information sharing and security investment. For the simultaneous game, interestingly, the social planner recommends the same information sharing as in the two period game when controlling only information sharing. The social planner refrains from imposing dysfunctionally high information sharing, and eliminates free riding in security investment. Neither the aggregate defense nor attack remain the same. Whether this gives higher profit for the firms depends also on the attacker, which the social planner does not control. When the attacker has a high unit cost of attack, the firms prefer the simultaneous game where the social planner controls both information sharing and security investment.

For the two period game where the social planner moves first, and controls both information sharing and security investment, information sharing remains the same. In the symmetric case, if the firms' unit cost of security investment is lower than the agent's unit cost of attack, the two period game causes larger security investment and profit for the firms, and lower attack and profit for the agent, than the simultaneous game. Allowing a social planner to control both information sharing and security investment in a two period game where the social planner moves first is the most beneficial control scenario when the firms' defense efficiencies are high. If these are sufficiently high, the attack is deterred altogether.

A final alternative is that a social planner or budget controls security investment only. This may occur through budget constraints within firms, managerial decisions, agreements, policies, laws, procedures. For this case information sharing depends also on the attacker's characteristics. The attack is inverse U shaped in information sharing. A firm's individually optimal information sharing in a simultaneous game when the social planner controls security investment, but not information sharing, is lower than in the individual optimization case without the social planner's control when the unit cost of security investment is not too high compared with the other firm, which is always satisfied in the symmetric case. This means that a firm free rides even more on information sharing when security investment is dictated by a social planner or budget. In other words, the social planner compensates for not controlling information sharing by imposing unreasonably high security investment, analogously to the case above where the social planner compensates for not controlling security investment by imposing unreasonably high information sharing.

To facilitate increased information sharing, firms are well advised to build up increased interdependence with other firms. To the extent costs of security investment increase, firms need to assess the tradeoff toward sharing more information, in the light of incentives on both sides to free ride. As the volume and scope of cyber attacks and industrial espionage increase, firms are advised to collect, categorize, and distribute, in the optimal amounts specified in this article, information about security breaches through SB/ISOs to other firms. A social planner needs to pay explicit attention to how the magnitude and scope of its control scenario interacts with budget control mechanisms, to ensure that it recommends and enforces optimal strategies, to avoid that firms do not respond suboptimally with free riding in strategies outside the social planner's control.

Acknowledgements

An earlier version of this article was presented at the May 24, 2006 Annual Forum on "Financial Information Systems and Cyber Security: A Public Policy Perspective", Robert H. Smith School of Business, University of Maryland. I thank seminar participants, William Lucyshyn, editor Martin P. Loeb, and two anonymous referees for their useful comments.

Appendix 1. Individual firm and agent optimization, cf. Section 3

The two firms' FOCs are

$$\begin{aligned}
\frac{\partial u_i}{\partial t_i} &= \frac{T_i + \alpha T_j}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} r_i - c_i = 0 \\
\frac{\partial u_j}{\partial t_j} &= \frac{T_j + \alpha T_i}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} r_j - c_j = 0 \\
\frac{\partial u_i}{\partial s_i} &= \frac{T_i + \alpha T_j}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} \alpha\gamma r_i - 2\phi_1 s_i + \phi_3 s_j = 0 \\
\frac{\partial u_j}{\partial s_j} &= \frac{T_j + \alpha T_i}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} \alpha\gamma r_j - 2\phi_1 s_j + \phi_3 s_i = 0
\end{aligned} \tag{A.1}$$

The agent's FOCs are

$$\begin{aligned}\frac{\partial U}{\partial T_i} &= \frac{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} r_i \\ &\quad + \frac{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} \alpha r_j - C = 0 \\ \frac{\partial U}{\partial T_j} &= \frac{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} \alpha r_i \\ &\quad + \frac{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} r_j - C = 0\end{aligned} \tag{A.2}$$

Dividing the first line in (A.2) with α and subtracting the second line gives

$$T_i + \alpha T_j = \sqrt{\frac{[t_i + \gamma s_j + \alpha(t_j + \gamma s_i)](1+\alpha) r_i}{C}} - [t_i + \gamma s_j + \alpha(t_j + \gamma s_i)] \tag{A.3}$$

Dividing the second line in (A.2) with α and subtracting from the first line gives

$$T_j + \alpha T_i = \sqrt{\frac{[t_j + \gamma s_i + \alpha(t_i + \gamma s_j)](1+\alpha) r_j}{C}} - [t_j + \gamma s_i + \alpha(t_i + \gamma s_j)] \tag{A.4}$$

Inserting (A.3) and (A.4) into (A.1) gives

$$\begin{aligned}\sqrt{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)} &= \frac{\sqrt{C r_i (1+\alpha)}}{C + c_i(1+\alpha)} \\ \sqrt{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)} &= \frac{\sqrt{C r_j (1+\alpha)}}{C + c_j(1+\alpha)} \\ \sqrt{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)} &= \frac{\alpha\gamma\sqrt{C r_i (1+\alpha)}}{C\alpha\gamma + (1+\alpha)(2\phi_1 s_i - \phi_3 s_j)} \\ \sqrt{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)} &= \frac{\alpha\gamma\sqrt{C r_j (1+\alpha)}}{C\alpha\gamma + (1+\alpha)(2\phi_1 s_j - \phi_3 s_i)}\end{aligned} \tag{A.5}$$

Equating the first and third line in (A.5) gives an equation with s_i and s_j. Equating the second and fourth line in (A.5) gives a second equation with s_i and s_j. Solving these two equations gives

$$s_i = \frac{\alpha\gamma(2\phi_1 c_i + \phi_3 c_j)}{(2\phi_1 - \phi_3)(2\phi_1 + \phi_3)}, \quad s_j = \frac{\alpha\gamma(2\phi_1 c_j + \phi_3 c_i)}{(2\phi_1 - \phi_3)(2\phi_1 + \phi_3)} \tag{A.6}$$

Inserting (A.6) into (A.5) and solving with respect to t_i and t_j gives

$$\begin{aligned} t_i &= \frac{C}{1-\alpha} \left. \frac{r_i}{[C + c_i(1+\alpha)]^2} - \frac{\alpha r_j}{[C + c_j(1+\alpha)]^2} \right) - \gamma s_j \\ t_j &= \frac{C}{1-\alpha} \left. \frac{r_j}{[C + c_j(1+\alpha)]^2} - \frac{\alpha r_i}{[C + c_i(1+\alpha)]^2} \right) - \gamma s_i \end{aligned} \tag{A.7}$$

Inserting (A.6) and (A.7) into (A.3) and (A.4) and solving with respect to T_i and T_j gives

$$\begin{aligned} T_i &= \frac{(1+\alpha)}{(1-\alpha)} \left. \frac{c_i r_i}{[C + c_i(1+\alpha)]^2} - \frac{\alpha c_j r_j}{[C + c_j(1+\alpha)]^2} \right) \\ T_j &= \frac{(1+\alpha)}{(1-\alpha)} \left. \frac{c_j r_j}{[C + c_j(1+\alpha)]^2} - \frac{\alpha c_i r_i}{[C + c_i(1+\alpha)]^2} \right) \end{aligned} \tag{A.8}$$

Inserting into (4) gives

$$\begin{aligned} u_i &= \frac{C}{C + c_i(1+\alpha)} r_i - c_i t_i - (\phi_1 s_i^2 - \phi_2 s_j^2 - \phi_3 s_i s_j) \\ u_j &= \frac{C}{C + c_j(1+\alpha)} r_j - c_j t_j - (\phi_1 s_j^2 - \phi_2 s_i^2 - \phi_3 s_i s_j) \\ U &= (1+\alpha)^2 \left. \frac{c_i^2 r_i}{[C + c_i(1+\alpha)]^2} + \frac{c_j^2 r_j}{[C + c_j(1+\alpha)]^2} \right) \end{aligned} \tag{A.9}$$

Differentiating (7) gives

$$\frac{\partial T_i^A}{\partial \alpha} = \frac{2C c_i r_i (1+\alpha)}{[C + c_i(1+\alpha)]^3} \tag{A.10}$$

$$\frac{\partial T_i^A}{\partial c_i} = \frac{r_i (1+\alpha)^2 [C - c_i(1+\alpha)]}{[C + c_i(1+\alpha)]^3} \tag{A.11}$$

$$\frac{\partial T_i^A}{\partial r_i} = \frac{c_i (1+\alpha)^2}{[C + c_i(1+\alpha)]^2} \tag{A.12}$$

$$\frac{\partial t_i^A}{\partial \alpha} = \frac{C r_i [C - c_i(1+\alpha)]}{[C + c_i(1+\alpha)]^3} \tag{A.13}$$

$$\frac{\partial t_i^A}{\partial C} = \frac{r_i (1+\alpha) [-C + c_i(1+\alpha)]}{[C + c_i(1+\alpha)]^3} \tag{A.14}$$

Differentiating the utilities for the symmetric case gives

$$\frac{\partial u}{\partial \alpha} = c\left[\frac{Cr(c(1-\alpha)-C)}{[C+c(1+\alpha)]^2} + \frac{c\gamma^2[2(1-\alpha)(\phi_1-\phi_3)+2\alpha\phi_2+\phi_3]}{(2\phi_1-\phi_3)^2}\right]$$

$$\lim_{c\to\infty}\frac{\partial u}{\partial \alpha} = \infty \tag{A.15}$$

$$\frac{\partial U}{\partial \alpha} = \frac{4c^2Cr(1+\alpha)}{[C+c(1+\alpha)]^3} \tag{A.16}$$

Appendix 2. A social planner controls information sharing in a two period game, cf. Section 6.1

Proof of Proposition 4. (i) Follows from inserting $c_i = c_j$ into (17) and comparing with $s_i = c_i\alpha\,\gamma/(2\phi_1 - \phi_3)$ in (8). The factor $1/\alpha$ follows since $2(\phi_1 - \phi_2 - \phi_3) < 2\phi_1 - \phi_3$. (ii) Follows from inserting (10), (11), (17) into (12) and applying $\tilde{w} = \tilde{u}_i + \tilde{u}_j$ for the social optimum, and inserting (A.6), (A.7) and (A.8) into (A.9) and applying $w = u_i + u_j$ for the individual optimum. The inequalities follow from differentiating (18). (iii) Follows from inserting into (17) and (6).

Appendix 3. A social planner controls information sharing in a simultaneous game, cf. Section 6.2

Proof of Proposition 5. (i) The denominators in (17) and (19) are equivalent. Comparing the numerators, $\hat{s}_i \geqslant \tilde{s}_i$ follows immediately. Observe $\phi_1 - \phi_2$ once in the numerator in (19) and twice (multiplicatively) in the denominator. Replacing the three occurrences of $\phi_1 - \phi_2$ with ϕ_1 gives a lower amount $\hat{s}_{iL}$ of information sharing which we write as

$$\hat{s}_{iL} = \frac{\gamma\phi_1(c_j+\alpha c_i)}{2(\phi_1-\phi_3)(\phi_1+\phi_3)} + \frac{\gamma\phi_3(c_i+\alpha c_j)}{2(\phi_1-\phi_3)(\phi_1+\phi_3)} \leqslant \hat{s}_i \tag{A.17}$$

We write (6) as

$$s_i = \frac{\alpha\gamma\phi_1 c_i}{(2\phi_1-\phi_3)(2\phi_1+\phi_3)/2} + \frac{\alpha\gamma\phi_3 c_j/2}{(2\phi_1-\phi_3)(2\phi_1+\phi_3)/2} \tag{A.18}$$

Both numerators in (A.17) are larger than the corresponding numerators in (A.18). The denominators in (A.17) can be written as $2\phi_1^2 - 2\phi_3^2$, which is lower than the denominators in (A.18) which can be written as $2\phi_1^2 - \phi_3^2/2$. Hence $\hat{s}_{iL} > s_i$. (ii) Follows from inserting $c_i = c_j$ into (19) and (17) and comparing with $s_i = c_i\alpha\gamma/(2\phi_1 - \phi_3)$ in (8). The factor $(1+\alpha)/\alpha$ increases from 2 to infinity as α decreases from one to zero, and follows since $2(\phi_1 - \phi_2 - \phi_3) < 2\phi_1 - \phi_3$. (iii) Follows from inserting (10), (11), (17) into (12) and applying $\tilde{w} = \tilde{u}_i + \tilde{u}_j$ for the two period social optimum, and applying Appendix 3 for the simultaneous social optimum. (iv) Follows from inserting into (A.9) and (A.24). (v) Follows from inserting into (19) and (6).

Assume that each firm continues to control its security investment, t_i and t_j, with FOCs as in (A.1). A social planner controls information sharing s_i and s_j and maximizes the joint profit $w = u_i + u_j$. This gives the FOCs

$$
\begin{aligned}
\frac{\partial u_i}{\partial t_i} &= \frac{T_i + \alpha T_j}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} r_i - c_i = 0 \\
\frac{\partial u_j}{\partial t_j} &= \frac{T_j + \alpha T_i}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} r_j - c_j = 0 \\
\frac{\partial w}{\partial s_i} &= \frac{T_i + \alpha T_j}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} \alpha\gamma r_i \\
&\quad + \frac{T_j + \alpha T_i}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} \gamma r_j \\
&\quad - 2\phi_1 s_i + 2\phi_2 s_i + 2\phi_3 s_j = 0 \\
\frac{\partial w}{\partial s_j} &= \frac{T_j + \alpha T_i}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} \alpha\gamma r_j \\
&\quad + \frac{T_i + \alpha T_j}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} \gamma r_i \\
&\quad - 2\phi_1 s_j + 2\phi_2 s_j + 2\phi_3 s_i = 0
\end{aligned}
\tag{A.19}
$$

The agent's FOCs are as in Appendix 1, s o (A.2), (A.3) and (A.4) remain valid. Inserting (A.3) and (A.4) into (A.19) gives

$$
\begin{aligned}
\frac{\partial u_i}{\partial t_i} &= \frac{\sqrt{Cr_i}}{\sqrt{1+\alpha}\sqrt{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}} - \frac{C}{(1+\alpha)} - c_i = 0 \\
\frac{\partial u_j}{\partial t_j} &= \frac{\sqrt{Cr_j}}{\sqrt{1+\alpha}\sqrt{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}} - \frac{C}{(1+\alpha)} - c_j = 0 \\
\frac{\partial w}{\partial s_i} &= \frac{\gamma\sqrt{C}}{\sqrt{1+\alpha}} \left. \frac{\sqrt{r_j}}{\sqrt{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}} + \frac{\alpha\sqrt{r_i}}{\sqrt{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}} \right) \\
&\quad - \gamma C - 2[(\phi_1 - \phi_2)s_i - \phi_3 s_j] = 0 \\
\frac{\partial w}{\partial s_j} &= \frac{\gamma\sqrt{C}}{\sqrt{1+\alpha}} \left. \frac{\sqrt{r_i}}{\sqrt{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}} + \frac{\alpha\sqrt{r_j}}{\sqrt{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}} \right) \\
&\quad - \gamma C - 2[(\phi_1 - \phi_2)s_j - \phi_3 s_i] = 0
\end{aligned}
\tag{A.20}
$$

Solving the first equation in (A.20) with respect to $\sqrt{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}$, solving the second equation with respect to $\sqrt{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}$, and inserting into the last two equations, gives two equations in s_i and s_j. Solving these two equations gives

$$
\begin{aligned}
s_i &= \frac{\gamma[(\phi_1 - \phi_2)(c_j + \alpha c_i) + \phi_3(c_i + \alpha c_j)]}{2(\phi_1 - \phi_2 - \phi_3)(\phi_1 - \phi_2 + \phi_3)} \\
s_j &= \frac{\gamma[(\phi_1 - \phi_2)(c_i + \alpha c_j) + \phi_3(c_j + \alpha c_i)]}{2(\phi_1 - \phi_2 - \phi_3)(\phi_1 - \phi_2 + \phi_3)}
\end{aligned} \tag{A.21}
$$

Inserting (A.21) into the first two equations in (A.20) and solving with respect to t_i and t_j gives

$$
\begin{aligned}
t_i &= \frac{C}{1-\alpha} \left. \frac{r_i}{[C + c_i(1+\alpha)]^2} - \frac{\alpha r_j}{[C + c_j(1+\alpha)]^2} \right) - \gamma s_j \\
t_j &= \frac{C}{1-\alpha} \left. \frac{r_j}{[C + c_j(1+\alpha)]^2} - \frac{\alpha r_i}{[C + c_i(1+\alpha)]^2} \right) - \gamma s_i
\end{aligned} \tag{A.22}
$$

Inserting (A.21) and (A.22) into (A.3) and (A.4) and solving with respect to T_i and T_j gives

$$
\begin{aligned}
T_i &= \frac{(1+\alpha)}{(1-\alpha)} \left. \frac{c_i r_i}{[C + c_i(1+\alpha)]^2} - \frac{\alpha c_j r_j}{[C + c_j(1+\alpha)]^2} \right) \\
T_j &= \frac{(1+\alpha)}{(1-\alpha)} \left. \frac{c_j r_j}{[C + c_j(1+\alpha)]^2} - \frac{\alpha c_i r_i}{[C + c_i(1+\alpha)]^2} \right)
\end{aligned} \tag{A.23}
$$

which is equivalent to (A.8). Inserting into (4) and $w = u_i + u_j$ gives

$$
\begin{aligned}
u_i &= \frac{C}{[C + c_i(1+\alpha)]} r_i - c_i t_i - (\phi_1 s_i^2 - \phi_2 s_j^2 - \phi_3 s_i s_j) \\
u_j &= \frac{C}{[C + c_j(1+\alpha)]} r_j - c_j t_j - (\phi_1 s_j^2 - \phi_2 s_i^2 - \phi_3 s_i s_j) \\
w &= \frac{C}{[C + c_i(1+\alpha)]} r_i + \frac{C}{[C + c_j(1+\alpha)]} r_j \\
&\quad - c_i t_i - c_j t_j - [(\phi_1 - \phi_2)(s_i^2 + s_j^2) - 2\phi_3 s_i s_j] \\
U &= (1+\alpha)^2 \left. \frac{c_i^2 r_i}{[C + c_i(1+\alpha)]^2} + \frac{c_j^2 r_j}{[C + c_j(1+\alpha)]^2} \right)
\end{aligned} \tag{A.24}
$$

The aggregate attack and defense are the same as in (7). The symmetric case becomes

$$
\begin{aligned}
t &= \frac{Cr}{(C+c(1+\alpha))^2} - \frac{c(1+\alpha)\gamma^2}{2(\phi_1-\phi_2-\phi_3)} \geqslant 0 \\
s &= \frac{c(1+\alpha)\gamma}{2(\phi_1-\phi_2-\phi_3)}, \quad T = \frac{cr(1+\alpha)}{[C+c(1+\alpha)]^2} \\
t_i^A &= \frac{Cr(1+\alpha)}{[C+c(1+\alpha)]^2}, \quad T_i^A = \frac{cr(1+\alpha)^2}{[C+c(1+\alpha)]^2}, \quad \frac{t_i^A}{T_i^A} = \frac{C}{c(1+\alpha)} \\
u &= \frac{C(C+c\alpha)}{(C+c(1+\alpha))^2} r + \frac{c^2(1-\alpha^2)\gamma^2}{4(\phi_1-\phi_2-\phi_3)}, \quad w = 2u \\
U &= \frac{2c^2 r(1+\alpha)^2}{[C+c(1+\alpha)]^2}
\end{aligned}
\tag{A.25}
$$

Appendix 4. Social planner controls security investment: Simultaneous game, cf. Section 7

The social planner's FOCs are

$$
\begin{aligned}
\frac{\partial w}{\partial t_i} &= \frac{T_i+\alpha T_j}{[t_i+\gamma s_j+T_i+\alpha(t_j+\gamma s_i+T_j)]^2} r_i \\
&\quad + \frac{T_j+\alpha T_i}{[t_j+\gamma s_i+T_j+\alpha(t_i+\gamma s_j+T_i)]^2} \alpha r_j - c_i = 0 \\
\frac{\partial w}{\partial t_j} &= \frac{T_j+\alpha T_i}{[t_j+\gamma s_i+T_j+\alpha(t_i+\gamma s_j+T_i)]^2} r_j \\
&\quad + \frac{T_i+\alpha T_j}{[t_i+\gamma s_j+T_i+\alpha(t_j+\gamma s_i+T_j)]^2} \alpha r_i - c_j = 0
\end{aligned}
\tag{A.26}
$$

The remaining four FOCs are as in (A.1) and (A.2). Solving these gives

$$
s_i = \frac{\alpha\gamma[2(c_i-\alpha c_j)\phi_1+(c_j-\alpha c_i)\phi_3]}{(1-\alpha^2)(2\phi_1-\phi_3)(2\phi_1+\phi_3)}, \quad s_j = \frac{\alpha\gamma[2(c_j-\alpha c_i)\phi_1+(c_i-\alpha c_j)\phi_3]}{(1-\alpha^2)(2\phi_1-\phi_3)(2\phi_1+\phi_3)}
\tag{A.27}
$$

$$
\begin{aligned}
t_i &= C(1-\alpha) \left. \frac{r_i}{[(c_i-\alpha c_j)+C(1-\alpha)]^2} - \frac{\alpha r_j}{[(c_j-\alpha c_i)+C(1-\alpha)]^2} \right) - \gamma s_j \\
t_j &= C(1-\alpha) \left. \frac{r_j}{[(c_j-\alpha c_i)+C(1-\alpha)]^2} - \frac{\alpha r_i}{[(c_i-\alpha c_j)+C(1-\alpha)]^2} \right) - \gamma s_i
\end{aligned}
\tag{A.28}
$$

$$T_i = \frac{r_i(c_i - \alpha c_j)}{[(c_i - \alpha c_j) + C(1-\alpha)]^2} - \frac{\alpha r_j(c_j - \alpha c_i)}{[(c_j - \alpha c_i) + C(1-\alpha)]^2}$$
$$T_j = \frac{r_j(c_j - \alpha c_i)}{[(c_j - \alpha c_i) + C(1-\alpha)]^2} - \frac{\alpha r_i(c_i - \alpha c_j)}{[(c_i - \alpha c_j) + C(1-\alpha)]^2} \tag{A.29}$$

Inserting into (4) and $w = u_i + u_j$ gives

$$u_i = \frac{C(1-\alpha)}{[(c_i - \alpha c_j) + C(1-\alpha)]} r_i - c_i t_i - (\phi_1 s_i^2 - \phi_2 s_j^2 - \phi_3 s_i s_j)$$
$$u_j = \frac{C(1-\alpha)}{[(c_j - \alpha c_i) + C(1-\alpha)]} r_j - c_j t_j - (\phi_1 s_j^2 - \phi_2 s_i^2 - \phi_3 s_i s_j)$$
$$w = u_i + u_j$$
$$U = \frac{(c_i - \alpha c_j)}{[(c_i - \alpha c_j) + C(1-\alpha)]} r_i + \frac{(c_j - \alpha c_i)}{[(c_j - \alpha c_i) + C(1-\alpha)]} r_j - C(T_i + T_j) \tag{A.30}$$

Appendix 5. Social planner controls both information sharing and security investment: simultaneous game, cf. Section 8.1

The social planner's FOCs are

$$\frac{\partial w}{\partial t_i} = \frac{T_i + \alpha T_j}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} r_i + \frac{T_j + \alpha T_i}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} \alpha r_j - c_i = 0$$
$$\frac{\partial w}{\partial t_j} = \frac{T_j + \alpha T_i}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} r_j + \frac{T_i + \alpha T_j}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} \alpha r_i - c_j = 0$$
$$\frac{\partial w}{\partial s_i} = \frac{T_i + \alpha T_j}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} \alpha\gamma r_i + \frac{T_j + \alpha T_i}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} \gamma r_j - 2\phi_1 s_i + 2\phi_2 s_i + 2\phi_3 s_j = 0 \tag{A.31}$$
$$\frac{\partial w}{\partial s_j} = \frac{T_j + \alpha T_i}{[t_j + \gamma s_i + T_j + \alpha(t_i + \gamma s_j + T_i)]^2} \alpha\gamma r_j + \frac{T_i + \alpha T_j}{[t_i + \gamma s_j + T_i + \alpha(t_j + \gamma s_i + T_j)]^2} \gamma r_i - 2\phi_1 s_j + 2\phi_2 s_j + 2\phi_3 s_i = 0$$

The agent's FOCs are as in Appendix 1, so (A.2), (A.3) and (A.4) remain valid. Inserting (A.3) and (A.4) into (A.31) gives

$$
\begin{aligned}
&\frac{\sqrt{r_i}}{\sqrt{t_i+\gamma s_j+\alpha(t_j+\gamma s_i)}}+\frac{\alpha\sqrt{r_j}}{\sqrt{t_j+\gamma s_i+\alpha(t_i+\gamma s_j)}}=\frac{c_i+C}{\sqrt{C}}\sqrt{1+\alpha}\\
&\frac{\sqrt{r_j}}{\sqrt{t_j+\gamma s_i+\alpha(t_i+\gamma s_j)}}+\frac{\alpha\sqrt{r_i}}{\sqrt{t_i+\gamma s_j+\alpha(t_j+\gamma s_i)}}=\frac{c_j+C}{\sqrt{C}}\sqrt{1+\alpha}\\
&\frac{\sqrt{r_j}}{\sqrt{t_j+\gamma s_i+\alpha(t_i+\gamma s_j)}}+\frac{\alpha\sqrt{r_i}}{\sqrt{t_i+\gamma s_j+\alpha(t_j+\gamma s_i)}}\\
&\qquad=\frac{2[(\phi_1-\phi_2)s_i-\phi_3 s_j]+\gamma C}{\gamma\sqrt{C}}\sqrt{1+\alpha}\\
&\frac{\sqrt{r_i}}{\sqrt{t_i+\gamma s_j+\alpha(t_j+\gamma s_i)}}+\frac{\alpha\sqrt{r_j}}{\sqrt{t_j+\gamma s_i+\alpha(t_i+\gamma s_j)}}\\
&\qquad=\frac{2[(\phi_1-\phi_2)s_j-\phi_3 s_i]+\gamma C}{\gamma\sqrt{C}}\sqrt{1+\alpha}
\end{aligned}
\tag{A.32}
$$

Equating the first and fourth line in (A.32) gives an equation with s_i and s_j. Equating the second and third line in (A.32) gives a second equation with s_i and s_j. Solving these two equations gives

$$
s_i=\frac{\gamma[(\phi_1-\phi_2)c_j+\phi_3 c_i]}{2(\phi_1-\phi_2-\phi_3)(\phi_1-\phi_2+\phi_3)},\quad s_j=\frac{\gamma[(\phi_1-\phi_2)c_i+\phi_3 c_j]}{2(\phi_1-\phi_2-\phi_3)(\phi_1-\phi_2+\phi_3)}
\tag{A.33}
$$

Inserting (A.33) into (A.32) and solving with respect to t_i and t_j gives

$$
\begin{aligned}
t_i&=C(1-\alpha)\left(\frac{r_i}{[(c_i-\alpha c_j)+C(1-\alpha)]^2}-\frac{\alpha r_j}{[(c_j-\alpha c_i)+C(1-\alpha)]^2}\right)-\gamma s_j\\
t_j&=C(1-\alpha)\left(\frac{r_j}{[(c_j-\alpha c_i)+C(1-\alpha)]^2}-\frac{\alpha r_i}{[(c_i-\alpha c_j)+C(1-\alpha)]^2}\right)-\gamma s_i
\end{aligned}
\tag{A.34}
$$

Inserting (A.33) and (A.34) into (A.3) and (A.4) and solving with respect to T_i and T_j gives

$$
\begin{aligned}
T_i&=\frac{r_i(c_i-\alpha c_j)}{[(c_i-\alpha c_j)+C(1-\alpha)]^2}-\frac{\alpha r_j(c_j-\alpha c_i)}{[(c_j-\alpha c_i)+C(1-\alpha)]^2}\\
T_j&=\frac{r_j(c_j-\alpha c_i)}{[(c_j-\alpha c_i)+C(1-\alpha)]^2}-\frac{\alpha r_i(c_i-\alpha c_j)}{[(c_i-\alpha c_j)+C(1-\alpha)]^2}
\end{aligned}
\tag{A.35}
$$

Inserting into (4) and $w = u_i + u_j$ gives

$$\begin{aligned}
u_i &= \frac{C(1-\alpha)}{[(c_i - \alpha c_j) + C(1-\alpha)]} r_i - c_i t_i - (\phi_1 s_i^2 - \phi_2 s_j^2 - \phi_3 s_i s_j) \\
u_j &= \frac{C(1-\alpha)}{[(c_j - \alpha c_i) + C(1-\alpha)]} r_j - c_j t_j - (\phi_1 s_j^2 - \phi_2 s_i^2 - \phi_3 s_i s_j) \\
w &= \frac{C(1-\alpha)}{[(c_i - \alpha c_j) + C(1-\alpha)]} r_i + \frac{C(1-\alpha)}{[(c_j - \alpha c_i) + C(1-\alpha)]} r_j - c_i t_i - c_j t_j \\
&\quad - [(\phi_1 - \phi_2)(s_i^2 + s_j^2) - 2\phi_3 s_i s_j] \\
U &= \frac{r_i(c_i - \alpha c_j)}{[(c_i - \alpha c_j) + C(1-\alpha)]} + \frac{r_j(c_j - \alpha c_i)}{[(c_j - \alpha c_i) + C(1-\alpha)]} \\
&\quad - C(1-\alpha) \quad \frac{r_i(c_i - \alpha c_j)}{[(c_i - \alpha c_j) + C(1-\alpha)]^2} + \frac{r_j(c_j - \alpha c_i)}{[(c_j - \alpha c_i) + C(1-\alpha)]^2}\Bigg)
\end{aligned} \tag{A.36}$$

The aggregate attack and defense are

$$t_i^A = \frac{Cr_i(1-\alpha)^2(1+\alpha)}{[(c_i - \alpha c_j) + C(1-\alpha)]^2}, \quad T_i^A = \frac{r_i(c_i - \alpha c_j)(1-\alpha^2)}{[(c_i - \alpha c_j) + C(1-\alpha)]^2} \tag{A.37}$$

The symmetric case becomes

$$\begin{aligned}
t &= \frac{Cr}{(C+c)^2} - \frac{c\gamma^2}{2(\phi_1 - \phi_2 - \phi_3)} \geqslant 0 \\
s &= \frac{c\gamma}{2(\phi_1 - \phi_2 - \phi_3)}, \quad T = \frac{cr}{[C+c]^2} \\
t_i^A &= \frac{Cr(1+\alpha)}{[C+c]^2}, \quad T_i^A = \frac{cr(1+\alpha)}{[C+c]^2}, \quad \frac{t_i^A}{T_i^A} = \frac{C}{c} \\
u &= \frac{C^2 r}{(C+c)^2} + \frac{c^2\gamma^2}{4(\phi_1 - \phi_2 - \phi_3)}, \quad w = 2u, \quad U = \frac{2c^2 r}{[C+c]^2}
\end{aligned} \tag{A.38}$$

Appendix 6. Social planner controls both information sharing and security investment: two period game, cf. Section 8.2

The agent's FOCs for the second period are given by (A.2). Inserting (A.3)-(A.4) into $w = u_i + u_j$, and determining the FOCs for the social planner for the first period gives

$$\frac{\partial w}{\partial t_i} = \frac{\sqrt{C}}{2\sqrt{1+\alpha}} \quad \frac{\sqrt{r_i}}{\sqrt{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}} + \frac{\alpha\sqrt{r_j}}{\sqrt{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}}\Bigg) - c_i = 0$$

$$\frac{\partial w}{\partial t_j} = \frac{\sqrt{C}}{2\sqrt{1+\alpha}} \quad \frac{\sqrt{r_j}}{\sqrt{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}} + \frac{\alpha\sqrt{r_i}}{\sqrt{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}}\Bigg) - c_j = 0$$

$$\frac{\partial w}{\partial s_i} = \frac{\gamma\sqrt{C}}{2\sqrt{1+\alpha}} \quad \frac{\sqrt{r_j}}{\sqrt{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}} + \frac{\alpha\sqrt{r_i}}{\sqrt{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}}\Bigg)$$

$$- 2\phi_1 s_i + 2\phi_2 s_i + 2\phi_3 s_j = 0$$

$$\frac{\partial w}{\partial s_j} = \frac{\gamma\sqrt{C}}{2\sqrt{1+\alpha}} \quad \frac{\sqrt{r_i}}{\sqrt{t_i + \gamma s_j + \alpha(t_j + \gamma s_i)}} + \frac{\alpha\sqrt{r_j}}{\sqrt{t_j + \gamma s_i + \alpha(t_i + \gamma s_j)}}\Bigg)$$

$$- 2\phi_1 s_j + 2\phi_2 s_j + 2\phi_3 s_i = 0 \tag{A.39}$$

Solving these and applying (A.3)-(A.4) gives (A.33) for information sharing, and

$$t_i = \frac{C(1-\alpha)}{4} \quad \frac{r_i}{(c_i - \alpha c_j)^2} - \frac{\alpha r_j}{(c_j - \alpha c_i)^2}\Bigg) - \gamma s_j$$

$$t_j = \frac{C(1-\alpha)}{4} \quad \frac{r_j}{(c_j - \alpha c_i)^2} - \frac{\alpha r_i}{(c_i - \alpha c_j)^2}\Bigg) - \gamma s_i \tag{A.40}$$

$$T_i = \frac{1}{4} \quad \frac{r_i[2(c_i - \alpha c_j) - C(1-\alpha)]}{(c_i - \alpha c_j)^2} - \frac{\alpha r_j[2(c_j - \alpha c_i) - C(1-\alpha)]}{(c_j - \alpha c_i)^2}\Bigg)$$

$$T_j = \frac{1}{4}\left(\frac{r_j[2(c_j - \alpha c_i) - C(1-\alpha)]}{(c_j - \alpha c_i)^2} - \frac{\alpha r_i[2(c_i - \alpha c_j) - C(1-\alpha)]}{(c_i - \alpha c_j)^2}\right) \tag{A.41}$$

The profits are

$$u_i = \frac{C(1-\alpha)}{2(c_i - \alpha c_j)} r_i - c_i t_i - (\phi_1 s_i^2 - \phi_2 s_j^2 - \phi_3 s_i s_j)$$

$$u_j = \frac{C(1-\alpha)}{2(c_j - \alpha c_i)} r_j - c_j t_j - (\phi_1 s_j^2 - \phi_2 s_i^2 - \phi_3 s_i s_j), \quad w = u_i + u_j \tag{A.42}$$

$$U = \left(1 - \frac{C(1-\alpha)}{2(c_i - \alpha c_j)}\right) r_i + \left(1 - \frac{C(1-\alpha)}{2(c_j - \alpha c_i)}\right) r_j - C(T_i + T_j)$$

References

Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *J. Comput. Security* 11 (3), 431–448.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. The effect of internet security breach announcements on shareholder wealth. *Int. J. Electron. Commerce* 9 (1), 69–104.

Gal-Or, E., 1985. Information sharing in oligopoly. *Econometrica* 53 (2), 329–343.

Gal-Or, E., Ghose, A., 2003. The economic consequences of sharing security information. In: *Proceedings of the Second Workshop on Economics and Information Security*, May 29–30, University of Maryland.

Gal-Or, E., Ghose, A., 2005. The economic incentives for sharing security information. *Inform. Syst. Res* 16 (2), 186–208.

Ghose, A., 2007. Information disclosure and regulatory compliance: Economic issues and research directions. In: Rao, H.R., Gupta, M., Upadhyaya, S. (Eds.), *Managing information assurance in financial services*, Idea Group.

Gordon, L.A., Loeb, M., 2001. Using information security as a response to competitor analysis systems. *Commun. ACM* 44 (9), 70–75.

Gordon, L.A., Loeb, M., 2002. The economics of information security investment. *ACM Trans. Informat. Syst. Security* 5 (4), 438–457.

Gordon, L.A., Loeb, M., 2003. Expenditures on competitor analysis and information security: A managerial accounting perspective. In: Bhimani, A. (Ed.), *Management Accounting in the New Economy.* Oxford University Press, pp. 95–111.

Gordon, L.A., Loeb, M., Lucyshyn, W., 2003. Sharing information on computer systems security: An economic analysis. *J. Account. Public Policy* 22 (6), 461–485.

Gordon, L.A., Loeb, M., Lucyshyn, W., Richardson, R., 2006a. *2006 CSI/FBI computer crime and security survey,* http://www.gocsi.com/.

Gordon, L.A., Loeb, M., Lucyshyn, W., Sohail, T., 2006b. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *J. Account. Public Policy* 25 (5), 503– 530. Hausken, K., 2006a. Income, interdependence, and substitution effects affecting incentives for security investment. *J. Account. 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. *Informat. Syst. Frontiers* 8 (5), 338–349.

Kirby, A., 1988. Trade associations as information exchange mechanisms. *RAND J. Econ.* 29 (1), 138–146.

Kunreuther, H., Heal, G., 2003. Interdependent security. *J. Risk Uncertainty* 26 (2/3), 231–249.

Novshek, W., Sonnenschein, H., 1982. Fulfilled expectations in cournot duopoly with information acquisition and release. Bell J. *Econ.* 13 (1), 214–218.

Schechter, S., Smith, M., 2003. How much security is enough to stop a thief? In: *Proceedings of the Financial Cryptography Conference*, Guadeloupe, January.

Schenk, M., Schenk, M., 2002. Defining the value of strategic security. *Secure Business Quart.* 1 (1), 1–6.

Shapiro, C., 1986. Exchange of cost information in oligopoly. *Rev. Econ. Stud.* 53 (3), 433–446.

Skaperdas, S., 1996. Contest success functions. *Econ. Theory* 7, 283–290.

Tanaka, H., Matsuura, K., Sudoh, O., 2005. Vulnerability and information security investment: An empirical analysis of E-local government in Japan. *J. Account. Public Policy* 24, 37–59.

Vives, X., 1990. Trade association disclosure rules, incentives to share information, and welfare. *RAND J. Econ.* 21 (3), 409–430.

Ziv, A., 1993. Information sharing in oligopoly: The truth-telling problem. *RAND J. Econ.* 24 (3), 455–465.