

A STRATEGIC ANALYSIS OF INFORMATION SHARING AMONG CYBER HACKERS

Kjell Hausken

Faculty of Social Sciences, University of Stavanger, Stavanger, Norway

ABSTRACT

We build a game theory model where the market design is such that one firm invests in security to defend against cyber attacks by two hackers. The firm has an asset, which is allocated between the three market participants dependent on their contest success. Each hacker chooses an optimal attack, and they share information with each other about the firm's vulnerabilities. Each hacker prefers to receive information, but delivering information gives competitive advantage to the other hacker. We find that each hacker's attack and information sharing are strategic complements while one hacker's attack and the other hacker's information sharing are strategic substitutes. As the firm's unit defense cost increases, the attack is inverse U-shaped and reaches zero, while the firm's defense and profit decrease, and the hackers' information sharing and profit increase. The firm's profit increases in the hackers' unit cost of attack, while the hackers' information sharing and profit decrease. Our analysis also reveals the interesting result that the cumulative attack level of the hackers is not affected by the effectiveness of information sharing between them and, moreover, is also unaffected by the intensity of joint information sharing. We also find that as the effectiveness of information sharing between hackers increases relative to the investment in attack, the firm's investment in cyber security defense and profit are constant, the hackers' investments in attacks decrease, and information sharing levels and hacker profits increase. In contrast, as the intensity of joint information sharing increases, while the firm's investment in cyber security defense and profit remain constant, the hackers' investments in attacks increase, and the hackers' information sharing levels and profits decrease. Increasing the firm's asset causes all the variables to increase linearly, except information sharing which is constant. We extend our analysis to endogenize the firm's asset and this analysis largely confirms the preceding analysis with a fixed asset. We use the software Mathematica 10.1 (www.wolfram.com) to program the model mathematically with equilibrium constraints, and perform numerical analysis illustrated graphically.

Keywords: Information sharing, security investment, asset allocation, cyber war, contest, decision analysis, game theory, numerical analysis.

Manuscript first received/*Recebido em*: 21/12/2014 Manuscript accepted/*Aprovado em*: 10/05/2015

Address for correspondence / *Endereço para correspondência*

Kjell Hausken, Faculty of Social Sciences University of Stavanger 4036 Stavanger, Norway
E-mail: kjell.hausken@uis.no

Published by/ *Publicado por*: TECSI FEA USP – 2015 All rights reserved.

Acknowledgement: I thank Anindya Ghose for useful discussions, Ross Anderson for suggestions that led to some additional analysis, Dean Abrams for inquiring about this phenomenon which led to the completion of this paper, and anonymous reviewers for useful comments.

1. INTRODUCTION

With the emergence of the Internet, cyber hackers are offered more opportunities to misappropriate or corrupt an organization's data resources. The list of cyber attacks increases every year. One especially costly attack, with damage estimates from \$225 million to \$4 billion dollars, was the 2011 data breach in Epsilon, the world's largest provider of marketing and handling services (to e.g. JP Morgan Chase and Best Buy), to obtain email addresses to be used for criminal activities.¹ Well established firms such as Citibank, Microsoft and the National Aeronautics and Space Administration (NASA), among others have been targeted and hacked by cyber perpetrators.

For a while now, it has been recognized that a key factor required for improving computer and information security is the gathering, analysis and information sharing related to successful, as well as unsuccessful attempts at computer security breaches. To encourage information sharing among organizations, the US federal government has encouraged the establishment of Security Based Information Sharing Organizations (SB/ISOs) of various kinds, such as Information Sharing & Analysis Centers (ISACs), Computer Emergency Response Team (CERT), INFRAGARD, etc. Similar initiatives have been taken elsewhere in the world.

There are several positive aspects to sharing information about security incidents and vulnerabilities. These benefits include both the prevention of further security breaches in the future (e.g., identifying and repairing vulnerabilities in their information security systems) as well as increased sales resulting from more effective security products and better security reputation among consumers. Questions on information sharing, economic incentives and social welfare similar to those noted above have been previously studied in the context of other organizations. Of particular relevance is the extensive literature on trade associations (TAs). Previous relevant work includes in the literature on oligopolies, cooperative relationships, joint ventures, and trade associations (Gal-Or 1986, Kirby 1988, Novshek and Sonnenschein 1982, Shapiro 1986, Vives 1990). More recently, information sharing among firms to defend against cyber attacks has been analyzed by Gordon, Loeb and Lucyshyn (2003), Gal-Or and Ghose (2005), and Hausken (2007, 2009). The focus of Gordon et al. (2003) is on how information sharing affects the overall level of information security. They highlight the tradeoff that firms face between improved information security and the potential for free riding, which can lead to under-investment in security expenditures. While Gordon et al. (2003) focus on the cost side effects of security breaches and information sharing, Gal-or and Ghose (2005) focus on the demand side effects and highlight the strategic implication of competition in the product market on information sharing and security technology investment levels. Hausken (2007) finds that information

¹ For a list of the 25 biggest cyber attacks in history, generated May 6, 2013, see <http://list25.com/25-biggest-cyber-attacks-in-history/>, retrieved July 16, 2015.

sharing and security investment for two firms are inverse U shaped in the aggregate attack, and interlinked through the interdependence between firms and the firm's unit cost of security investment.

Information sharing among hackers is different. Firms subject to attacks would naturally prefer that such information sharing and cooperation among hackers does not take place. As part of their activities, hackers compile information about firms' vulnerabilities and defense strategies, attempt to gain access to the information the firms collect about their security breaches and share the information among each other, and can also make it publicly available.

What motivates hackers to hack? Howard (1997) identified the five possible objectives for hackers - financial gain, a desire for challenges, political gain, a desire to cause destruction, and leisure activities.² Some research has pointed out that greed, power, and revenge are superseding curiosity and other positive motivations (Jordan and Taylor 1998). Some work in sociology and computer science (Raymond 2001) on the motivation of hackers has pointed out that because of issues such as reputation and competition amongst hackers in order to get more recognition within the community, hackers may have incentives to not share information with each other. Indeed hackers actively compete with one another to write the best software, frequently one-upping each other in displays of coding prowess. Combining hacker egos with their practice of sharing fixes amongst one another and the sheer joy hackers take from hacking, one can clearly understand how reputation plays a large role as pointed out by Ritchie (2000). On the other hand, there have also been discussions about how hackers generally do not believe in keeping secrets and are quite keen to share information (Brunker 1998)³ and not necessarily compete for reputation from a sociological view (Risan 2000). We believe there are reasons for both viewpoints but the key issue is to understand what happens when hackers do share information with each other.

This paper explores the following research questions: Generally, what are the security problems when hackers share information with each other? More specifically, how does a hacker strike a balance between information sharing and attack? How does a firm protect against hackers sharing information with each other combined with attacking the firm? Which factors impact the players' strategies?

We analyze the hypothetical case of two hackers who may share information about a firm's vulnerabilities, in addition to deciding on the size of their attacks. The firm can be any collective or individual actor, including public or private agencies, subject to attack. The firm invests in information security to defend against the attacks. Naturally, each hacker prefers to receive information from the other hacker, but is reluctant to give information, though there are benefits from joint information sharing. We assume that both hackers and the defending firm are strategic actors. The opponent does not have a given, fixed, or immutable strategy, which has been common in much of prior research in information security. The absence of an assumption about a fixed threat, or a fixed defense, enables a much richer analysis.

² He further developed a taxonomy of the hacking process involving the attacker, tools, access, results and objectives of attacks. Kjaerland (2005) extended this work to account for the target or victim of an attack.

³ Hackers: Knights-errant or knaves? <http://msnbc.msn.com/id/3078783/>

In a related stream of work, Png, Tang and Wang (2005) focus on the strategic interaction among end-users and between users and hackers in a setting with a continuum of user types, and show that users' effort in fixing depends on hackers' targeting and vice-versa. Prior work (Choi, Fershtman, and Gandal 2004; Nizovtsev and Thursby 2005; Arora, Caulkins, and Telang 2005) has examined issues such as incentives for security specialists to disclose security flaws and provide the appropriate patches. Other work (Cavusoglu, Mishra and Raghunathan 2005; Anderson 2001) has examined issues such as users' incentives to invest in intrusion detection systems. For example, Cavusoglu, Mishra and Raghunathan (2005) and Anderson (2001) observe that many systems fail due to misplaced incentives rather than technical reasons. Also, Pinker (2007) considers warnings and the deployment of physical resources as two important defensive mechanisms available to governments combating terrorism.

While the two hackers may be interpreted as two individual agents seeking to exploit a firm, one can also interpret them as two firms who decide to gang up on a third rival firm to exploit its asset. The reason for this broad interpretation is that the terms "attack" and "defense" can be understood as metaphors. As Hirshleifer (1995) puts it, "falling also into the category of interference struggles are political campaigns, rent-seeking maneuvers for licenses and monopoly privileges (Tullock 1967), commercial efforts to raise rivals' costs (Salop and Scheffman 1983), strikes and lockouts, and litigation – all being conflicting activities that need not involve actual violence." Attack and defense are subcategories of attack-oriented and defensive competition.

Information sharing is technically complicated to analyze. Since our objective is to analyze information sharing among hackers, and not how the firm defends in a possibly different manner against two hackers who may be configured differently, we focus attention on two equivalent hackers which makes the analysis tractable. This allows analyzing more specifically, the tradeoffs between information sharing and cyber attack, which are the two strategic choice variables for each hacker, in interaction with a defending firm which has one strategic choice variable—the level of investment in its security.

One main difference with respect to costs between cyber attacks 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 carries cost of a different nature, and may sometimes be even costless for each hacker aside from the time spent on transferring the information. Attackers in the cyber era of course have information storage capacity, and they may even have compiled and stored information in an organized and secure manner. Deciding to share information with another hacker may not involve more than sending an electronic mail, or storing the information on a disk and delivering it. In other words, designing cyber attacks entail explicit costs on part of the hackers since all investments are generally costly, while information sharing has different kinds of costs or no costs. However, the competitive advantage given to a hacker through information sharing can be construed as an implicit cost. Furthermore, exchange of information per service can be costly. Also, obtaining a better share of the profit of the attack, and then sharing itself entails a cost for those shares. With respect to benefits, sharing or selling information e.g. on the deep end can be highly lucrative.

In related work on firms defending against cyber attacks, Gal-Or and Ghose (2005) find that security investments and information sharing are strategic complements. Gordon et al. (2003) find that when firms share information, each firm has reduced incentives to invest in information security. Hausken (2007) finds that security investments and information sharing are strategic substitutes. This paper examines these issues for two

hackers. An important difference is that whereas two firms incur information leakage costs when sharing information about their vulnerabilities and security breaches, two hackers sharing information about a firm's vulnerabilities do not incur costs in the same manner. In fact, as a hacker shares information about a firm with another hacker, the firm itself is the main entity suffering through incurring information leakage costs which are possible and often likely in all information transfers.

We use credible specific functional forms to generate exact analytical solutions for the variables. Sacrificing generality, a successful specification demonstrates internal consistency, illumination, and ranges of parameter values for equilibrium existence.

The rest of the paper is as follows. Section 2 presents the model. We start with the case when the firm's asset is exogenous. Section 3 analyzes the model and presents some numeric analysis to provide insights. In section 4 we endogenize the firm's asset, so that the firm makes a tradeoff between producing the asset and security investment needed for defending it. Section 5 assumes an upper constraint on each hacker's probability of gaining the asset before the hacker is shut down, and provides some basic insights. Section 6 discusses various extensions and limitations. Section 7 concludes with some discussion of the implications of our study.

2. Model

Consider a firm with an asset r and two equivalent hackers i and j launching cyber attacks to acquire portions of the firm's asset. The firm invests t to defend its asset, and the defense expenditure is f , where $\partial f / \partial t > 0$. The hackers invest T_i and T_j , respectively, to attack the asset, with attack expenditures F_i and F_j , respectively, where $\partial F_i / \partial T_i > 0$ and $\partial F_j / \partial T_j > 0$. For simplicity, we consider a linear function given by $f = ct$, $F_i = \theta T_i$, $F_j = \theta T_j$, where c is the unit cost (inefficiency) of cyber defense and θ is the unit cost (inefficiency) of cyber attack. Competent players have lower unit costs than less competent players due to their ability to execute attacks more efficiently with less effort. An incompetent player has infinite unit cost, lacking the ability to attack or defend. An attack means attempting to break through the security defense of the firm in order to appropriate something of value to the firm⁴. For simplicity, we assume risk-neutral actors. This assumption does not change the nature of the argument. The expenditures ct , θT_i , θT_j can be interpreted as expenses in capital and/or labor. The game is shown in Figure 1.

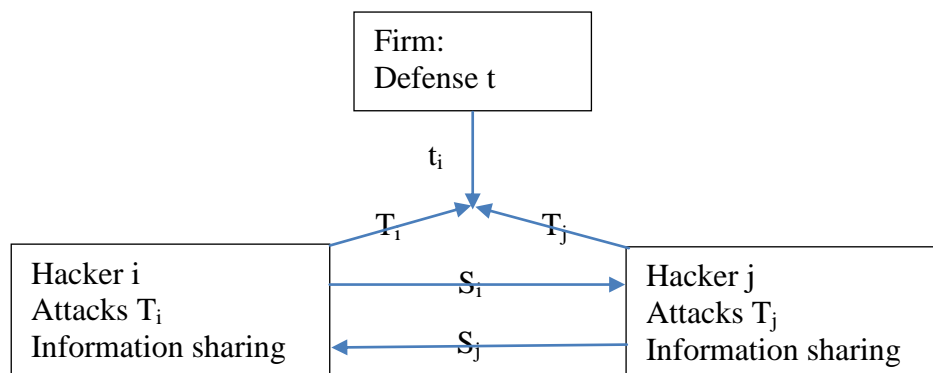


Figure 1. Interaction between a firm and two hackers.

⁴ This could be customer related information, business strategy information or accounting related information.

The cyber contest between the firm and the two hackers for the asset r takes the common ratio form (Tullock 1980). In the absence of information sharing, we consider the contest success function

$$g = \frac{t}{t+T_i+T_j}, \quad G^i = \frac{T_i}{t+T_i+T_j}, \quad G^j = \frac{T_j}{t+T_i+T_j}, \quad (1)$$

where g , G^i and G^j are the probabilities that the firm, hacker i , and hacker j , respectively, retain the asset. The three probabilities sum to one, $g+G^i+G^j=1$. As expected, the first probability satisfies $\partial g / \partial t > 0$, $\partial g / \partial T_i < 0$, $\partial g / \partial T_j < 0$. That is, the firm benefits from its own security investment, and suffers from the attacks launched by the two hackers. Similarly, the second probability satisfies $\partial G^i / \partial t < 0$, $\partial G^i / \partial T_i > 0$, $\partial G^i / \partial T_j < 0$, and similarly for the third probability. These probabilities imply that each hacker benefits from its own investment, but suffers a loss from the investment made by the firm and an attack by the other hacker on the firm.

Hausken (2007) analyzes two interdependent firms subject to cyber attacks, and shows how increasing interdependence causes increased information sharing and decreased security investment. An attack against one firm gets partly propelled further to the other firm due to the interdependence, and a firm's defense operates both against direct attacks and indirect attacks, where the latter are those proceeding through the other firm due to the interdependence.

With two hackers, the interdependence between these operates differently for the following reasons. First, an attack launched by hacker i is directed against the firm, and it does not make sense to consider this attack as somehow also proceeding through hacker j to the firm. Secondly, the defense set up by the firm operates against the total sizes T_i and T_j of the two attacks. However, a change in T_i by hacker i may affect the defense t by the firm, which in turn affects the attack T_j by hacker j , so in this sense there is indirect interdependence between the hackers.

As a hacker's attack level increases, it compiles more information about the firm's vulnerabilities. Characteristics of the information are the type of firewalls, encryption techniques, access control mechanisms, intrusion detection systems, etc. employed by the firm, the training and procedures of the firm's security experts, the nature of the defense, and the properties of the vulnerabilities. A lot of this information is publicly available.

We assume that hacker i decides to share an amount S_i of information with hacker j , and that hacker j similarly decides to share an amount S_j of information with hacker i . We define S_i as the information amount that hacker j receives from hacker i and that hacker j not already controls. Information already controlled by hacker j has been obtained elsewhere, or by hacker j 's own interpretation, for which hacker i 's sharing was not needed. To ensure tractability we quantify information along one dimension. Naturally, hacker i prefers to receive information from hacker j since it gets thereby more insight into the firm's vulnerabilities and defensive strengths, which makes it better equipped to launch a successful attack. Analogously, hacker j prefers to receive information from hacker i . Based on this reasoning, we assume that hacker i 's overall attack has a strength equal to $T_i + \gamma S_j$, and that hacker j 's overall attack has a similar strength of size $T_j + \gamma S_i$, where the parameter γ measures the effectiveness of information sharing S_j relative to the attack T_i in

the composition of the overall attack. γ varies between 0 and 1. With such information sharing, the contest success functions in (1) become equal to

$$h = \frac{t}{t + T_i + \gamma S_j + T_j + \gamma S_i}, \quad H^i = \frac{T_i + \gamma S_j}{t + T_i + \gamma S_j + T_j + \gamma S_i}, \quad H^j = \frac{T_j + \gamma S_i}{t + T_i + \gamma S_j + T_j + \gamma S_i}. \quad (2)$$

These three probabilities capture three important consequences from information sharing: First, it incorporates the fact that the firm suffers a loss from information sharing among the hackers. Second, hacker i benefits from receiving information from hacker j , but suffers a loss in utility from delivering information since hacker j gets a competitive advantage. This follows because γS_j is present in the numerator in the second probability in (2), while both γS_j and γS_i are present in the denominator. Consequently, the hackers can be expected to free ride on each other's information sharing, and to the extent (2) is descriptive, no information sharing will occur. For the second probability in (2), $\partial H^i / \partial S_i < 0$ and $\partial H^i / \partial S_j > 0$, and analogously for the third probability $\partial H^j / \partial S_j < 0$ and $\partial H^j / \partial S_i > 0$.⁵

As the hackers share information with each other, synergies emerge. For instance, they discuss the available information, transformation occurs, missing pieces are filled in, and reasoning based on the joint information generates new knowledge. Joint information sharing by the two hackers can thus be expected to generate even deeper insight into the firm's vulnerabilities and defense. To model this effect, we introduce the multiplicative term $S_i S_j$, and a parameter λ , $\lambda \geq 0$, which scales the intensity of joint information sharing. If $\lambda = 0$, the two hackers are unable to utilize joint sharing. The upper limit to λ is such that information shared by the two hackers is not more valuable than if the same amount of information is generated by only one hacker. Multiplicative terms are common in the literature to express joint interaction. With such joint information sharing, the contest success functions in (2) can be written as

$$k = \frac{t}{t + T_i + \gamma S_j + T_j + \gamma S_i + \lambda S_i S_j}, \quad (3)$$

$$K^i = \frac{T_i + \gamma S_j + (\lambda/2) S_i S_j}{t + T_i + \gamma S_j + T_j + \gamma S_i + \lambda S_i S_j}, \quad K^j = \frac{T_j + \gamma S_i + (\lambda/2) S_i S_j}{t + T_i + \gamma S_j + T_j + \gamma S_i + \lambda S_i S_j}.$$

For simplicity we let the two hackers share the benefit of their joint sharing so that each of them receives $(\lambda/2) S_i S_j$. Equation (3) expresses the tradeoff each hacker makes between how much information to share and how much to withhold. Intuitively, it prefers to share sufficient information so that it reaps the benefits of joint information sharing. However, if it shares too much information, the other hacker is given an undue advantage because it can get a larger portion of the firm's asset. This places an upper limit on how much information is optimal for a hacker to share.

Gal-Or and Ghose (2005) and Hausken (2007) assume that two firms sharing information about their security breaches incur information leakage costs. Such costs are to a firm's disadvantage. Basically, leakage of security vulnerabilities could increase

⁵ We assume that information can be scaled along one dimension like prior work (Gordon et al. 2003, Gal-Or and Ghose 2005, Hausken 2007). Generally, information is multi-faceted, of different kinds, and with different degrees of importance for different purposes. In our context, a one-dimensional concept of information can be interpreted to mean that different kinds of information are given different weights according to their relative importance.

consumers' apprehension of transacting with a firm. As a result some consumers may find it optimal to switch from one firm to its rival, thereby reducing its demand. When two hackers share information they possess about the firm's vulnerabilities, security breaches, and defense characteristics, there can be substantial information leakage which is borne by the firm. These leakage costs occur when the hackers share the information among themselves, which exposes the firm more thoroughly, and when they make their information publicly available. We assume that the leakage costs incurred by the firm caused by information sharing by the two hackers is given by the function $g = \phi_1(S_i^2 + S_j^2) + \phi_2 S_i S_j$, where ϕ_1 and ϕ_2 are non-negative parameters. First, $\partial g / \partial S_i \geq 0$ and $\partial g / \partial S_j \geq 0$ since the firm suffers from information sharing by both hackers. Second, $\partial^2 g / \partial S_i^2 \geq 0$ and $\partial^2 g / \partial S_j^2 \geq 0$ due to possible deleterious ripple effects of security breaches. This is accounted for by the quadratic presence of both S_i^2 and S_j^2 in the term $\phi_1(S_i^2 + S_j^2)$. Joint information sharing by both hackers is especially detrimental for the firm due to synergy including the possibility that the hackers fill in the missing pieces in their information to gain an improved information base. This is accounted for by the interaction term $\phi_2 S_i S_j$ which is large when both S_i and S_j are large. Mathematically, $\partial^2 g / \partial S_i \partial S_j \geq 0$ since intensified sharing by the hackers increases the marginal leakage costs incurred by the firm.

Observe the difference between this leakage cost function and the one proposed by Gal-Or and Ghose (2005) when firms rather than hackers share information. First, when firms share information, there has to be a positive cost proportional to S_i^2 for firm i when firm i shares information, and a negative cost (benefit) proportional to S_j^2 for firm i when firm j shares information. Second, the interaction term $S_i S_j$ has to be negative for both firms since, as Gal-Or and Ghose (2005) formulate it, "intensified sharing by the competitor reduces the marginal leakage costs incurred by the firm."

Equation (3) models how each hacker prefers to receive information from the other hacker, and how both hackers share the benefit of their joint sharing. Although the information leakage costs are borne by the firm, the hackers can suffer indirectly. When information about a firm's vulnerabilities is leaked to another hacker, and especially if it is leaked to the public, the firm may or will learn about its vulnerabilities and may come up with a stronger defense which means that the variable t may increase. This in turn affects how the hackers choose their strategic variables T_i , T_j , S_i , and S_j .

The profits u , U_i , U_j , of the firm, hacker i , and hacker j , respectively, are given by

$$u = \frac{t}{t + T_i + \gamma S_j + T_j + \gamma S_i + \lambda S_i S_j} r - ct - [\phi_1(S_i^2 + S_j^2) + \phi_2 S_i S_j], \quad (4)$$

$$U_i = \frac{T_i + \gamma S_j + (\lambda/2) S_i S_j}{t + T_i + \gamma S_j + T_j + \gamma S_i + \lambda S_i S_j} r - \theta T_i, \quad U_j = \frac{T_j + \gamma S_i + (\lambda/2) S_i S_j}{t + T_i + \gamma S_j + T_j + \gamma S_i + \lambda S_i S_j} r - \theta T_j.$$

3. Analysis

The firm's free choice variable is the security defense expenditure level t . Hacker i 's free choice variables are the level of security attack T_i and the level of information sharing S_i . Analogously, hacker j 's free choice variables are T_j and S_j . The game proceeds as follows. The firm and the two hackers choose their free choice variables

simultaneously and independently to maximize profits. Calculating $\partial U_i / \partial S_i = 0$ and solving with respect to S_j gives

$$S_j = \frac{t - T_i + T_j - \frac{2\gamma^2}{\lambda} + \sqrt{\left(t - T_i + T_j - \frac{2\gamma^2}{\lambda}\right)^2 - 8T_i \frac{\gamma^2}{\lambda}}}{2\gamma} \tag{5}$$

This leads to the following observation:

Observation 1. (i) Each hacker’s investment in an attack and the level of information sharing are strategic complements such that increasing one causes an increase in the other, and vice versa. (ii) One hacker’s attack and the other hacker’s information sharing are strategic substitutes such that increasing one causes a decrease in the other, and vice versa.⁶

Observation 1(i) follows since $\partial S_j / \partial T_j > 0$. Observation 2(i) follows since $\partial S_j / \partial T_i < 0$. Verbally, an increase (decrease) in T_j on the right hand side of (5) causes an increase (decrease) in S_j on the left hand side. Similarly, an increase (decrease) in T_i on the right hand side of (5) causes a decrease (increase) in S_j on the left hand side.

Observation 1 states that if one hacker were to increase its attack, then it also increases its level of information sharing. However, if a hacker receives more information from the other hacker, then it cuts back on its own attack level. It is useful at this stage to compare this result with prior work that looks at information sharing between two firms. When two firms share information and defend against one external hacker, Hausken (2007) finds that information sharing and security investments of the two firms are strategic substitutes. Gordon et al. (2003) find strategic substitutability under certain assumptions in the sense that when firms share information, each firm has reduced incentives to invest in information security.⁷ Gal-Or and Ghose (2003, 2005) find strategic complementarity so that that increased security investment by one firm leads to increased security investment and increased information sharing by its competitor.

Next we derive the first order conditions. By setting $\partial u / \partial t = 0$, $\partial U_i / \partial T_i = 0$, $\partial U_i / \partial S_i = 0$, and thereafter substituting $T = T_i = T_j$ and $S = S_i = S_j$ in equilibrium, gives the three first order conditions.

$$FOC \ t: \frac{r(2T + S(2\gamma + \lambda S))}{(t + 2(T + \gamma S) + \lambda S^2)^2} - c = 0, \tag{6}$$

$$FOC \ T: \frac{2r(t + T + \gamma S) + r\lambda S^2}{2(t + 2(T + \gamma S) + \lambda S^2)^2} - \theta = 0, \tag{7}$$

⁶ Ideally one would like to generalize the above observation into a broader result using the implicit function approach after total differentiation of the three first-order conditions and sign the Hessian Matrix using Cramer’s Rule. We tried doing that. However, the resultant Hessian Matrix is impossible to sign without making some strong assumption about parameter values. Hence, we do not state this result as a formal Proposition. However, it is important to point out that the qualitative nature of the intuition and insights are the same. Hence, we focus on discussing the results in the form of an Observation and contrast them with results from prior work.

⁷ Information sharing and security investment are not pure strategic substitutes in Gordon et al.’s (2003) study. They provide necessary and sufficient conditions for information sharing to lead to increased or decreased security investment.

$$FOC \ S: 2\gamma(T + \gamma S) + \lambda S(\gamma S - t) = 0. \quad (8)$$

Solving with respect to t , T , S , setting $K=K^i=K^j$ and $U=U_i=U_j$ in (3) and (4), and inserting into the profit functions u and U and gives the following interior solution:

$$t = \frac{2r(2\theta - c)}{(2\theta + c)^2}, T = 2c \left(\frac{r}{(2\theta + c)^2} - \frac{2\gamma^2\theta}{(2\theta - c)^2\lambda} \right), S = \frac{2c\gamma}{(2\theta - c)\lambda}, k = 1 - \frac{2c}{2\theta + c}, K = \frac{c}{2\theta + c},$$

$$u = \frac{r(2\theta - c)^2}{(2\theta + c)^2} - \frac{4c^2\gamma^2(2\phi_1 + \phi_2)}{((2\theta - c)\lambda)^2}, U = c \left(\frac{cr}{(2\theta + c)^2} + \frac{4\gamma^2\theta^2}{(2\theta - c)^2\lambda} \right) \text{ where } 2\theta > c, r > \frac{2\gamma^2\theta(2\theta + c)^2}{(2\theta - c)^2\lambda} \quad (9)$$

The hackers' overall attack level, which can also be referred to as the cumulative attack level, as seen from the two numerators in the last two expressions of equation (4), dependent on investment, information sharing, and joint information sharing and equals the following:

$$T_A = T + \gamma S + (\lambda/2)S^2 = \frac{2cr}{(2\theta + c)^2} \quad (10)$$

In equilibrium, T_A is independent of γ and λ . This also explains why the firm's defense level t is independent of γ and λ , and u is independent of γ and λ when there are no leakage costs, i.e., when $\phi_1 = \phi_2 = 0$. Further, note that the probabilities k and K of the asset, where $k + 2K = 1$, accruing to the firm and to each hacker, respectively, are independent of γ and λ , and of the asset r . This leads to the following result.

Proposition 1 (i) *The probability of the asset accruing to each hacker is equal to the ratio of the firm's unit cost of investment c , to the sum of the unit costs of investment of all the three actors, $2\theta + c$.*

(ii) *The cumulative attack level T_A of the hackers is independent of both the effectiveness of information sharing, γ , and the intensity of the joint information sharing, λ .*

(iii) *Further, the cumulative attack level (i) increases in the unit cost of the firm's cyber defense at a decreasing rate, (ii) decreases in the unit cost of the hacker's cyber attack at an increasing rate and (iii) increases in the value of the firm's asset. That is, $\partial T_A / \partial c > 0$, $\partial^2 T_A / \partial c^2 < 0$, $\partial T_A / \partial \theta < 0$, $\partial^2 T_A / \partial \theta^2 > 0$, $\partial T_A / \partial r > 0$, $\partial^2 T_A / \partial r^2 = 0$.*

An interesting result is that the cumulative attack level T_A of the hackers is not affected by the effectiveness γ of information sharing between hackers and moreover, is also unaffected by intensity λ of joint information sharing. This result can have some ramifications. For instance, organizations are always worried about the extent to which information sharing between hackers can adversely affect them. Our analysis reveals that the strength of the total attack is only related to the extent of the firm's unit cost of cyber defense, the hackers' unit costs of attack and the asset value of the firm. If it turns out that information sharing between hackers does not enhance the attack intensities, then there is less cause for concern from such information sharing than it is thought to be.

Proposition 2. *As the unit cost of the cyber defense of the firm increases towards the sum of the unit costs of the cyber attack of the two hackers, (that is, as c increases towards 2θ), the firm's security investment and the hackers' information sharing*

decrease toward zero but remain strictly positive, $t > 0$ and $S > 0$. Conversely, the hackers' attack level T reduces to zero for a value of c that is strictly below 2θ .

Observe in (9) how each hacker's unit cost θ is always preceded by 2, while the firm's unit cost c is preceded by 1, that is, it is equal to c . This occurs because there are two hackers, but only one firm. Furthermore, the firm does not defend itself when $2\theta < c$. When the firm's unit cost is larger than the double unit cost of each hacker, then the firm gives up its asset due to its intrinsic inefficiency in protecting its asset. The inequality can also be phrased as $1/c < 1/2\theta$ or as $2/c < 1/\theta$. This means that the defense efficiency $1/c$ of the firm must be at least 50% of the attack efficiency of each hacker in order for the firm to find it worthwhile to invest in some level of cyber defense. When the firm does not invest at all in defense, the two hackers share the firm's asset and do not share information.

When $T = 0$ according to Proposition 1, solving the first order conditions for t and S in (6) and (8) gives a third order equation set which is voluminous to set up and tedious to analyze generally. We thus confine our general discussion to the interior solution. The following proposition specifies the dependence of the six variables t , T , S , u , U , and K on the five parameters c , θ , γ , λ , r .

Proposition 3. Focus attention on interior solutions and assume $\phi_1 = \phi_2 = 0$. Then,

(i) the firm's investment in cyber defense decreases at an increasing rate in the level of its own unit cost. Further, the hackers' level of information sharing increases at an increasing rate in the level of the firm's unit cost of cyber defense. Finally, the firm's profit decreases at an increasing rate in its own unit cost. That is, $\partial t / \partial c < 0$, $\partial^2 t / \partial c^2 > 0$, $\partial S / \partial c > 0$, $\partial^2 S / \partial c^2 > 0$, $\partial u / \partial c < 0$, $\partial^2 u / \partial c^2 > 0$.

(ii) the hackers' level of information sharing and pay-offs decrease at an increasing rate in the level of their unit cost of cyber attacks. That is, $\partial S / \partial \theta < 0$, $\partial^2 S / \partial \theta^2 > 0$, $\partial U / \partial \theta < 0$, $\partial^2 U / \partial \theta^2 > 0$. Further, when $c/2 < \theta < 3c/2$, the firm's investment in cyber defense increases at a decreasing rate in the level of the hackers' unit cost of cyber attacks. That is, $\partial t / \partial \theta > 0$, $\partial^2 t / \partial \theta^2 < 0$ when $c/2 < \theta < 3c/2$.

(iii) the firm's investment in cyber security is independent of the effectiveness of information sharing, γ , i.e., $\partial t / \partial \gamma = 0$. Further, with respect to the effectiveness of information sharing, γ , a hacker's investment in cyber attacks is decreasing at a decreasing rate, their level of information sharing is increasing linearly and their pay-offs are increasing at an increasing rate. That is, $\partial T / \partial \gamma < 0$, $\partial^2 T / \partial \gamma^2 < 0$, $\partial S / \partial \gamma > 0$, $\partial^2 S / \partial \gamma^2 = 0$, $\partial U / \partial \gamma > 0$, $\partial^2 U / \partial \gamma^2 > 0$.

(iv) with respect to the intensity of the joint information sharing, λ , a hacker's investment in cyber attacks is increasing at a decreasing rate, the level of information sharing between hackers is decreasing at an increasing rate and their pay-offs are decreasing at an increasing rate. That is, $\partial T / \partial \lambda > 0$, $\partial^2 T / \partial \lambda^2 < 0$, $\partial S / \partial \lambda < 0$, $\partial^2 S / \partial \lambda^2 > 0$, $\partial U / \partial \lambda < 0$, $\partial^2 U / \partial \lambda^2 > 0$.

(v) with respect to the value of the firm's asset, r , the firms' investment in cyber security and the hacker's investment in cyber attacks are increasing linearly. That is, $\partial t / \partial r > 0$, $\partial^2 t / \partial r^2 = 0$, $\partial T / \partial r > 0$, $\partial^2 T / \partial r^2 = 0$. Moreover, with respect to the value of the firm's asset, while the hackers' pay-offs increase linearly, their level of information sharing does not change. That is, $\partial S / \partial r = 0$, $\partial U / \partial r > 0$, $\partial^2 U / \partial r^2 = 0$.

(vi) the probability of the firm's asset accruing to each hacker increases at a decreasing rate in the level of the firm's unit cost of cyber defense and decreases at an increasing rate with its own unit cost. That is, $\partial K / \partial c > 0$, $\partial^2 K / \partial c^2 < 0$, $\partial K / \partial \theta < 0$, $\partial^2 K / \partial \theta^2 > 0$. Conversely, the firm's probability decreases at an increasing rate in its own unit cost while it increases at a decreasing rate in the hackers' unit cost. That is, $\partial k / \partial c < 0$, $\partial^2 k / \partial c^2 > 0$, $\partial k / \partial \theta > 0$, $\partial^2 k / \partial \theta^2 < 0$.

Figures 1-5 illustrate Propositions 1-3, and additionally account for the corner solutions. The parameter values are $c = \gamma = \lambda = 0.5$, $\theta = 1$, $r = 10$, $\phi_1 = \phi_2 = 0$, except in that figure where that parameter varies. Division with 5 and 2 are done for scaling purposes. As the firm's unit cost of security investment c (i.e. the level of inefficiency) increases from zero in Figure 2, the firm's investment in cyber security decreases convexly, while the hacker's investment in attack becomes inverse U shaped. A very low c implies that the firm's security investment is highly efficient which reduces any incentives for the hacker to attack. On the other hand, a high value of c causes the hacker to cut back on its attack level since the firm's defense is so modest. The hackers' attack is largest when c is around 0.5 in which case the hackers and firm are approximately equally matched in the sense that the firm's defense is neither overwhelming nor modest. Information sharing increases in a convex manner in c , and compensates for the decrease in attack levels as c increases from around 0.5 to 1.04. This convex increase is quite interesting. It means that as the firm becomes burdened by an increasing unit cost, the hackers boost their information sharing substantially, to the detriment of the firm, and benefit of the hackers. The phenomenon is quite common. Security becomes so expensive that the firm cuts back on it. The hackers respond by increasing their attack when the defense is strong, and decreasing their attack when it is no longer needed against a weak defense. But information sharing continues to increase.

Figure 2 is consistent with Proposition 3(i) when $c < 1.04$ which gives an interior solution. When $c > 1.04$, the hackers withdraw from attacking the asset ($T=0$) and focus attention on information sharing. Although such a high c is usually uncommon in practice, the model predicts a new phenomenon for this case emerges which is determined by solving the third order equation set that arises from (6) and (8) when $T=0$. The hackers start to free ride on each other's information sharing so that the optimal level of information sharing S decreases. This is collectively detrimental for the hackers and the firm's profit increases until $S=0$. Of course, the optimal level of investment by a firm in its security investment t decreases in the unit cost, but more moderately. Interestingly, Gordon et al. (2003) who focus on the cost side effects of information sharing on the overall level of security, also demonstrate similar free riding effects in information sharing using a very different model. The free-rider dilemma with respect to security investments is further analyzed by Anderson (2001).

Figure 3 shows how the variables change as a function of the unit cost of attack θ . The level of attack investment of the hackers, T , is low when θ is high, and is inverse U

shaped otherwise. The firm's defense level t also behaves in a similar manner. As θ decreases, information sharing increases, and so does the hackers' profit levels. On the other hand, the firm's profit decreases as θ decreases due to the intensity of the attack. Figure 3 is consistent with Proposition 3(ii) when $\theta > 0.37$ which gives an interior solution. As θ decreases below a critical value given by $\theta = 0.37$, the attack level T decreases to zero and information sharing takes over. Note that since θ is present only in the first order condition for T in (7), and not present in (6) and (8), the four variables t , S , u , U are constant when $\theta < 0.37$.

Figure 4 depicts the dependence on γ which measures how effective information sharing is relative to the attack in the composition of the overall attack. When $\gamma = 0$, there is no information sharing since it is not beneficial, but the attack is substantial. As γ increases, information sharing increases linearly and the attack level decreases convexly, eventually reaching zero as in Figure 2. The firm's defense level and profit is independent of γ for the interior solution as specified in Proposition 2. Figure 4 is consistent with Proposition 3(iii) when $\gamma < 0.95$ which gives an interior solution. As γ increases above $\gamma = 0.95$, where $T = 0$, the development is similar to Figure 2, where S decreases to zero, after which t and u are constant.

Figure 5 delineates the dependence on the intensity λ of joint information sharing. Substantial free riding in information sharing emerges as λ increases, causing S to decrease concavely. The hackers' compensate by increasing the attack T concavely, preserving the overall attack level T_A constant as in Proposition 1. This also ensures that the firm's security investment and pay off remains constant. The free riding among the hackers causes their profit U to decrease concavely. Figure 5 is consistent with Proposition 3(iv) when $\lambda > 0.14$ which gives an interior solution. As λ decreases below $\lambda = 0.14$ where $T = 0$, information sharing and hacker profit decrease to zero when $\lambda = 0.06$, below which t and u are constant.

Figure 6 plots the dependence on the firm's asset r . Note that all the variables increase linearly in r except information sharing, S , which is independent of r . That is, a firm's cyber security investment level, the hackers' cyber attack levels and their pay-offs increase in the value of the firm's asset. Figure 5 is consistent with Proposition 3(v) when $r > 2.78$ which gives an interior solution. As the asset value decreases below a critical value given by $r = 2.78$, the hackers do not find investing in an attack worthwhile, and consequently set their attack levels $T = 0$. As r decreases below a critical level given by $r = 1.12$, information sharing levels, S , and hacker profit, U , decrease to zero, while the firm's investment in cyber security, t , and its pay-off, u , are constant, similar to Figure 5. In sum, Figures 2, 4 and 5 provide some common insights. Similarly, Figures 1 and 3 provide some common insights.

4. Endogenizing the firm's asset

Considering the asset r as exogenously given is common in the rent seeking literature. However, rents and assets frequently have to be produced. Furthermore, since firms have limited resources, they make a tradeoff between producing the asset and investing in cyber security to defend it. This calls attention for the need to examine cases where the firm decided to endogenize the asset.

Hausken (2005) has compared and contrasted rent seeking models and production and conflict models. To consider the latter assume that the firm has a resource R (e.g. a capital good, or labor) which can be divided into effort p to produce (build) the asset, and security investment t to defend or protect the asset from attack. With unit

conversion costs a and b , respectively, of transforming the resource into defending versus producing the asset, the budget constraint for the firm is

$$R = at + bp \quad (11)$$

Assume that the production function for the asset takes the following simple form,

$$p = (R - at) / b \quad (12)$$

which follows from solving (11) with respect to p , and which means a linear production function. Substituting r with p in (4), and removing ct since the defense expenditure of security investment is now endogenized, (4) becomes

$$u = \frac{t}{t + T_i + \gamma S_j + T_j + \gamma S_i + \lambda S_i S_j} (R - at) / b - \left[\phi_1 (S_i^2 + S_j^2) + \phi_2 S_i S_j \right],$$

$$U_i = \frac{T_i + \gamma S_j + (\lambda/2) S_i S_j}{t + T_i + \gamma S_j + T_j + \gamma S_i + \lambda S_i S_j} (R - at) / b - \theta T_i, \quad (13)$$

$$U_j = \frac{T_j + \gamma S_i + (\lambda/2) S_i S_j}{t + T_i + \gamma S_j + T_j + \gamma S_i + \lambda S_i S_j} (R - at) / b - \theta T_j$$

Calculating $\partial u / \partial t = 0$, $\partial U_i / \partial T_i = 0$, $\partial U_i / \partial S_i = 0$, and thereafter setting $T = T_i = T_j$ and $S = S_i = S_j$ in equilibrium, gives the three first order conditions given as follows:

$$FOC \ t: 2R(T + \gamma S) + R\lambda S^2 - at(t + 4T + 2S(2\gamma + \lambda S)) = 0 \quad (14)$$

$$FOC \ T: \frac{(R - at)(2(t + T + \gamma S) + \lambda S^2)}{2b(t + 2(T + \gamma S) + \lambda S^2)^2} - \theta = 0 \quad (15)$$

$$FOC \ S: 2\gamma(T + \gamma S) + \lambda S(\gamma S - t) = 0 \quad (16)$$

Solving the above first order conditions with respect to t , T , S , gives us the following interior solution:

$$t = \frac{4R}{7a + 2b\theta + \sqrt{a^2 + 12ab\theta + 4b^2\theta^2}} > 0,$$

$$T = \left[-a\gamma^2(a^3 + 15a^2b\theta + 48ab^2\theta^2 + 12b^3\theta^3) + bR\theta(a^2 + 8ab\theta - 4b^2\theta^2)\lambda \right. \\ \left. + \sqrt{a^2 + 12ab\theta + 4b^2\theta^2}(-a\gamma^2(a^2 + 9ab\theta + 10b^2\theta^2) + bR\theta(a + 2b\theta)\lambda) \right] / \quad (17)$$

$$\left[8b^2\theta^2(a^2 + 7ab\theta + 2b^2\theta^2 + (a + b\theta)\sqrt{a^2 + 12ab\theta + 4b^2\theta^2})\lambda \right] > 0,$$

$$S = \frac{\gamma(a - 2b\theta + \sqrt{a^2 + 12ab\theta + 4b^2\theta^2})}{4b\theta\lambda} > 0$$

Focusing attention on the interior solution, Figures 6-11 illustrate how these variables change with respect to a given parameter. The other parameter values are set to similar levels as in section 3, that is $\gamma = \lambda = 0.5$, $\theta = 1$, $\phi_1 = \phi_2 = 0$. Additionally consider $a = b = 1$ and $R = 10$. Figure 7 shows how these variables change with respect to the unit defense cost a , and is similar to Figure 2 for the unit cost c , partly preserving the curvature. The firm's cyber security investment level, t , and its pay-off function, u ,

decreases convexly. On the other hand, the hackers' attack levels, T , is inverse U shaped, while their information sharing level S and pay-off functions U increase linearly.

Figure 8 shows the dependence on the firm's unit production cost b . An increase in b is uniformly detrimental for all the variables causing them to decrease in a convex manner with the exception of T which is inverse U shaped. The reason is that when b is very low, the firm can easily increase its security investment t because such investments are highly efficient. This causes the hackers to reduce their attack investment levels and rely on higher levels of information sharing instead. Figure 9 shows the dependence on the unit cost of attack θ , and is similar to Figure 3 for 4 of the 5 variables, preserving the curvature. That is, T is inverse U shaped, u increases concavely, and S and U decrease convexly. The one exception is t which decreases in Figure 9 and is inverse U shaped in Figure 3. Differences like that are expected when endogenizing the firm's asset. Figure 10 shows the dependence on γ which measures the effectiveness of information sharing relative to the attack in the composition of the overall attack. Figure 10 is similar to Figure 4, and preserves a similar curvature for the different variables. That is, t and u are constant, while T decreases concavely, S increases linearly, and U increases convexly. Figure 11 shows the dependence on the intensity λ of joint information sharing. Figure 11 is similar to Figure 5, preserving the curvature. That is, t and u are constant, T increases convexly, and S and U decrease convexly. Figure 12 shows the dependence on the firm's resource R . Note that similar to Figure 6, all the variables increase linearly in r except information sharing, S , which is independent of r . Summing up, we find that endogenizing the firm's asset largely confirms the analysis with a fixed asset in Section 3. An increase in the unit production cost of the firm is detrimental for all the five variables except the hackers' attack level which is inverse U shaped.

5. An upper bound on each hacker's probability of gaining the asset

In this section we discuss an extension where the hackers may not want to exceed a certain limit with regard to the probability of gaining the firm's asset. This can happen when hackers are apprehensive of undue attention and visibility that can cause them to be proactively targeted by the firm. If the hacker is subject to enforcement, it would not enjoy any benefit from targeting the firm's asset beyond a certain limit. One of the key phenomena that has emerged over the last five years is that various kinds of software tools or code used for hacking (such as malware embedded in consumer software) are now being written for explicit financial rewards rather than for other purposes such as reputation. Indeed, a growing trend is that of a parallel economy of hackers, quite in the spirit of Adam Smith's division of labor, in which some hackers specialize in tool creation, others trade vulnerabilities, others buy and sell credit card numbers, and then of course there are those who engage in spamming and phishing. This is starting to assume many of the aspects of the above-ground market, including externalities. For example, pay-TV operators now wait until one bad agent has established itself as the monopoly provider of forged smartcards (first-to-market usually removes incentives for further investment in forgery as it can undercut later competitors). Once this agent has $x\%$ of the market, which may be 5% or some other percentage dependent on the pay-TV operators tolerance and benefit-cost analysis, they will close it down or the government can shut it down.⁸

Just as it is virtually impossible to secure a computer against the most persistent hacker, it is also virtually impossible for a serial hacker to avoid detection and capture.

⁸ We thank Ross Anderson for pointing this out and suggesting this example.

No one can expect to succeed against all opponents forever. Indeed it has been documented that "cyber detectives" are out there laying traps for and ultimately apprehending "cyber criminals" (Kremen 1998). Besides the US, a large number of countries have adopted statutes designed to protect electronic commerce and information stored on computers internally. In many instances these countries cooperate with the United States in order to apprehend hackers operating inside their borders (Platt 1996). These laws can increase the penalties from being caught and as such may reduce the hackers' incentives to grab more than a certain probability of gaining the target's assets. This section provides some preliminary insights into the profits of the hacker and the firm in such situations.

In our model, recall from (9) that the probability of gaining the firm's asset accruing to each hacker is given by $K = c/(2\theta+c)$ when both hackers are symmetric in their capabilities. Let Q denote the threshold value of the firm's asset acquired by each hacker beyond which the hackers are actively traced and targeted by enforcement authorities in order to be closed down. This could be an external agent like a government institution, or it could be a division within the firm itself which operates under other incentives and constraints than those assumed in the model in this paper. Thus, if the probability of gaining the firm's asset accruing to each hacker is larger than this constraint, i.e., if $K > Q$, where the firm takes into account how many hackers operate near this threshold, each hacker exceeding the threshold gets closed down in some manner.

Assume that the threshold Q , and also the unit costs c and θ of defense and attack, are common knowledge. The new optimization problem for each hacker then becomes as follows. If $K < Q$, which means that the firm's threshold for being hacked is so large that it accepts the probability K that its asset r is confiscated by each hacker, then the solution in (9) and the discussion in the previous sections apply. Conversely, if $K > Q$, each hacker gets closed down if it is not intelligent, earning zero profit as its investment and information sharing eventually decrease to zero. (At the moment when it gets closed down, no longer earning a probability of gaining the asset, its profit is negative determined by its cost expenditure θT where T is given in (9).) If $K > Q$ and each hacker is intelligent, it chooses to hack so that the probability is $K = Q - \varepsilon$ of gaining the asset where $\varepsilon > 0$ is arbitrarily small but positive, which means that it hacks marginally less than the threshold level which causes its elimination. Since there are two hackers, these together earn the probability $2(Q - \varepsilon)$ of gaining the asset, while the firm retains the remaining probability $1 - 2(Q - \varepsilon)$. Using (3), (4) and (10), the probabilities of gaining the asset earned by the firm and each hacker are

$$k = \frac{t}{t + 2T_A} = 1 - 2(Q - \varepsilon), \quad K = \frac{T_A}{t + 2T_A} = \frac{1 - k}{2} = Q - \varepsilon \quad (18)$$

This implies that the cumulative attack level is given by

$$T_A = \frac{Q - \varepsilon}{1 - 2(Q - \varepsilon)} t \quad (19)$$

Suppose there are no leakage costs, i.e., $\phi_1 = \phi_2 = 0$. Consider first the case when the firm decides to keep its investment level t the same as in (9). Then, the firm's profit is given by

$$u = kr - ct = \left(1 - 2(Q - \varepsilon) - \frac{2c(2\theta - c)}{(2\theta + c)^2} \right) r \tag{20}$$

If each hacker chooses its overall attack T_A to consist of security investment only, and no information sharing, that is, $T_A = T$ and $S = 0$, its profit is given by

$$U = Kr - \theta T = \left(1 - \frac{2\theta(2\theta - c)}{(2\theta + c)^2 [1 - 2(Q - \varepsilon)]} \right) (Q - \varepsilon) r \tag{21}$$

Two main changes are possible to this solution where an intelligent hacker hacks with a limited probability $K = Q - \varepsilon$ of gaining the asset, to avoid being caught. First, the firm may choose an alternative level of investment t than the solution in (9). That is, the firm may realize that each of two hackers are intelligent and will choose $T_A = T$ as determined in (19) which is dependent on t . Since the probabilities accruing to each hacker are fixed and predetermined as in (18), this becomes a coordination game where the firm and each hacker adjust their investments t and T so that (18) is satisfied. To minimize their costs, one solution is that both parties reduce their investments t and T toward zero while (18) is satisfied, though that solution seems hard to occur in practice.

The other possible change to the solution in (20) and (21) is that the hacker chooses another allocation between security investment and information sharing instead of setting $T_A = T$ and $S = 0$. A simple solution is to assume that the hackers agree that investment is costly while information sharing is not, and hence choose only to share information. That is, $T_i = T_j = T = 0$. Setting the left hand side of (10) equal to the right hand side of (19) gives

$$\gamma S + (\lambda/2)S^2 = \frac{Q - \varepsilon}{1 - 2(Q - \varepsilon)} t \tag{22}$$

Substituting the value of $t = \frac{2r(2\theta - c)}{(2\theta + c)^2}$ gives us the following equation

$$S = \frac{-\gamma + \frac{\sqrt{\gamma^2(-1 + 2(Q - \varepsilon))(c + 2\theta)^2 + 4r(Q - \varepsilon)(c - 2\theta)\lambda}}{\sqrt{-1 + 2(Q - \varepsilon)(c + 2\theta)}}}{\lambda} \tag{23}$$

The firm's profit u remains as in (20) while each hacker's profit is given by

$$U = Kr = (Q - \varepsilon)r. \tag{24}$$

6. Extensions and limitations

In our analysis, we have only considered symmetric equilibrium, implying that both hackers have equal characteristics and thus are equally efficient in utilizing the shared security information in attacking firms. A future extension could involve looking at asymmetric situations between hackers, where hackers have unequal characteristics in various respects. Asymmetry is analytically more challenging, with less likelihood of analytical solutions for the most general scenarios. Our results are robust to some extensions such as changes in timelines of the game. For example, it is possible to envisage a scenario in which all three actors first chose security attacks T_i , T_j and t , and then in the next stage, the two hackers choose sharing levels S_i , S_j simultaneously. The notion that cyber security investments are long term decisions, and chosen before

information sharing decisions, is in principle easy to change. Our preliminary analysis reveals that there is no major qualitative change in results in such a game. Further, another limitation is that we have only considered a scenario with two hackers. Generalizing this research to include n hackers could be an interesting extension but becomes analytically tedious in our setup. However, we conjecture that many of the qualitative insights of our model carry through to a situation with more than two hackers. A difference is that a firm facing more than two hackers is subject to an opposition which may share information in more sophisticated manners than what is accounted for in the current model which distinguishes between effectiveness of information sharing and intensity of joint information sharing. Other extensions are to different kinds of security investment, and distinguishing between different kinds of information that hackers can share. Information is multidimensional. It may pertain to high level or low level security breaches, methods and success of earlier attacks, identities of hackers, and secrets about research, development, future plans, trade, capacities, personnel dispositions, etc. Despite these limitations, we believe that our model addresses an important issue, and hope that the proposed approach may be used as a starting point for additional research in this area.

7. Conclusion

The paper considers a scenario where one firm is subject to a cyber attack by two external hackers. The hackers choose the optimal level of information to share with each other about the firm's vulnerabilities and security breaches, and choose the optimal attack levels. The firm chooses the optimal defense, which is costly and consists in investing in information technology security to protect its asset. The hackers collect information in various manners, and attempt to gain access to the information the firms collect about their security breaches. Each hacker prefers to receive information from the other hacker about the firm's vulnerabilities. Providing information to the other hacker places the other hacker in a better position when competing for the firm's asset. The hackers benefit from joint information sharing. The paper analyzes the extent to which a hacker has incentives to provide information voluntarily to the other hacker, and the tradeoffs each hacker makes between sharing information and investing in an attack, which is costly. Each hacker thus has two free choice variables, and the firm has one free choice variable. The paper shows that each hacker's attack and information sharing are strategic complements such that increasing one causes an increase in the other, and vice versa. Conversely, one hacker's attack and the other hacker's information sharing are strategic substitutes such that increasing one causes a decrease in the other, and vice versa.

The paper defines an overall attack for the hacker which is a weighted sum of three components: (i) the investment in an attack, (ii) the amount of information sharing, and (iii) the amount of joint information sharing. Each of the two hackers substitutes between these three components such that the relative weights of the second and third components do not, remarkably, affect the defense security investment of the defending firm, and also do not affect the probabilities of gaining the asset accruing to each hacker and the firm. For the special case of no leakage costs, the firm's profit is also unaffected by the relative weights of the second and third components. The firm is affected by the hackers' overall attack level, and not their tradeoffs between the three components. The overall investment in attack increases concavely in the firm's unit defense cost, decreases convexly in the hackers' unit cost of attack, and increases linearly in the firm's asset.

As the firm's unit cost of security investment increases from zero towards twice the hackers' unit cost of attack, the attack follows an inverse U shaped function and reaches zero while the firm's security investment and the hackers' information sharing levels remain positive. Specifically, while the firm's cyber security investment and profit decrease convexly, the hackers' information sharing increases convexly, and the hackers' profits increase as well.

As the hackers' unit cost of attack increases, the firm's profit increases, while the hackers' information sharing and profit decrease convexly. The firm's defense and the hackers' attack are inverse U shaped for some regions in the parameter space. As the effectiveness of information sharing relative to the investment in cyber attack in the composition of the overall attack increases, the firm's defense and profit are constant, the hacker's attack levels decrease convexly, their information sharing increases linearly, and their profit increases convexly.

As the intensity of joint information sharing increases, the firm's defense and profit are constant, the attack increases concavely, and the hackers' information sharing and profit decrease convexly. Increasing the firm's asset causes all the variables to increase linearly, except information sharing which is constant. We also find that endogenizing the firm's asset largely confirms the analysis with a fixed asset. Increasing the unit production cost is detrimental for all the five variables except the hackers' attack which is inverse U shaped.

A few policy implications and managerial insights of the analyses merit some discussion. First, our analysis reveals that the cumulative attack level of the hackers is not affected by the effectiveness of information sharing between them and, moreover, it is also unaffected by the intensity of joint information sharing. If it turns out that information sharing between hackers does not enhance their attack intensities, then there is possibly less cause for concern from such information sharing than it is thought to be. This result can have some ramifications on firms' incentives and strategies regarding their adversarial contest with hackers especially in situations involving industrial espionage which is widely being touted as new mantra for hackers. It also undermines to some extent, the importance of the truthful revelation of information by hackers to each other.

Second, our analysis suggests the need to raise firms' awareness that hackers not only choose strategically how much to invest in an attack, and that hackers may compete with each other in attacking more successfully, but also that hackers may cooperate through sharing information with each other about a firm's vulnerabilities. Firms may defend themselves by designing their security investments such that when it is breached by one hacker, the sensitive information may quickly become obsolete which limits the potential vulnerability if the information is transferred elsewhere. Also, if a firm knows the identity of the hacker that has breached its security, it may focus on not only blocking future attacks by this hacker, but also on providing incentives to the hacker so that the sensitive information does not get transferred to other hackers. Such incentives can be of monetary, informational, or political nature.

Finally, if a hacker's information sharing can be reduced, strategic complementarity with the hacker's attack also reduces the latter. This suggests compartmentalization, in some sense or other, the interaction of hackers with each other or designing incentives to isolate them from each other rather than treating them as one monolithic group which acts in unison. Moreover, the fact that the intensity of information sharing and effectiveness of sharing have opposite impact on hackers'

investment in attacks, their information sharing levels and profits provides further insights into mechanisms that firms can design to take preventive measures and thwart cyber attacks.

Appendix

Proof of Proposition 1

Proof: The proof follows from inserting (9) into (10) and considering the signs of the first and second derivatives of (10). These are

$$\frac{\partial T_A}{\partial c} = \frac{2r(2\theta - c)}{(2\theta + c)^3}, \frac{\partial^2 T_A}{\partial c^2} = -\frac{4r(4\theta - c)}{(2\theta + c)^4}, \frac{\partial T_A}{\partial \theta} = -\frac{8cr}{(2\theta + c)^3}, \frac{\partial^2 T_A}{\partial \theta^2} = \frac{48cr}{(2\theta + c)^4}, \frac{\partial T_A}{\partial r} = \frac{2c}{(2\theta + c)^2} \quad (\text{A1})$$

Proof of Proposition 2

Insert $c=2\theta-\varepsilon$ into (9) where $\varepsilon>0$ is arbitrarily small but positive. This causes the second term within the bracket in the expression for T to be arbitrarily large and positive, which means that the expression for T becomes negative with arbitrarily large absolute value. Since the hackers' attack cannot be negative, this gives $T=0$, $t>0$, $S>0$ for a sufficiently small ε . QED.

Proof of Proposition 3

This follows from considering the signs of the first and second derivatives of (9).

$$\begin{aligned} \frac{\partial t}{\partial c} &= -\frac{2r(6\theta - c)}{(2\theta + c)^3}, \frac{\partial^2 t}{\partial c^2} = \frac{4r(10\theta - c)}{(2\theta + c)^4}, \\ \text{(i)} \quad \frac{\partial T}{\partial c} &= \frac{4\gamma^2\theta(2\theta + c)^4 - 2r\lambda(2\theta - c)^4}{(c^2 - 4\theta^2)^3\lambda}, \frac{\partial^2 T}{\partial c^2} = -\frac{4r(4\theta - c)}{(2\theta + c)^4} - \frac{8\gamma^2\theta(4\theta + c)}{(2\theta - c)^4\lambda}, \\ \frac{\partial S}{\partial c} &= \frac{4\gamma\theta}{(2\theta - c)^2\lambda}, \frac{\partial^2 S}{\partial c^2} = \frac{8\gamma\theta}{(2\theta - c)^3\lambda}, \frac{\partial u}{\partial c} = -\frac{8r(2\theta - c)\theta}{(2\theta + c)^3}, \frac{\partial^2 u}{\partial c^2} = \frac{16r(4\theta - c)\theta}{(2\theta + c)^4} \end{aligned} \quad (\text{A2})$$

$$\begin{aligned} \text{(ii)} \quad \frac{\partial t}{\partial \theta} &= \frac{4r(-2\theta + 3c)}{(2\theta + c)^3}, \frac{\partial^2 t}{\partial \theta^2} = \frac{16r(2\theta - 5c)}{(2\theta + c)^4}, \frac{\partial S}{\partial \theta} = -\frac{4c\gamma}{(2\theta - c)^2\lambda}, \frac{\partial^2 S}{\partial \theta^2} = \frac{16c\gamma}{(2\theta - c)^3\lambda}, \\ \frac{\partial U}{\partial \theta} &= -c^2 \left(\frac{4r}{(2\theta + c)^3} + \frac{8\gamma^2\theta}{(2\theta - c)^3\lambda} \right), \frac{\partial^2 U}{\partial \theta^2} = 8c \left(\frac{3cr}{(2\theta + c)^4} + \frac{c\gamma^2(4\theta + c)}{(2\theta - c)^4\lambda} \right) \end{aligned} \quad (\text{A3})$$

$$\begin{aligned} \text{(iii)} \quad \frac{\partial t}{\partial \gamma} &= 0, \frac{\partial T}{\partial \gamma} = -\frac{8c\gamma\theta}{(2\theta - c)^2\lambda}, \frac{\partial^2 T}{\partial \gamma^2} = -\frac{8c\theta}{(2\theta - c)^2\lambda}, \frac{\partial S}{\partial \gamma} = \frac{2c}{(2\theta - c)\lambda}, \frac{\partial^2 S}{\partial c^2} = 0, \\ \frac{\partial U}{\partial \gamma} &= \frac{8c\gamma\theta^2}{(2\theta - c)^2\lambda}, \frac{\partial^2 U}{\partial c^2} = \frac{8c\theta^2}{(2\theta - c)^2\lambda} \end{aligned} \quad (\text{A4})$$

$$\begin{aligned} \text{(iv)} \quad \frac{\partial t}{\partial \lambda} &= 0, \frac{\partial T}{\partial \lambda} = \frac{4c\gamma^2\theta}{(2\theta - c)^2\lambda^2}, \frac{\partial^2 T}{\partial \lambda^2} = -\frac{8c\gamma^2\theta}{(2\theta - c)^2\lambda^3}, \\ \frac{\partial S}{\partial \lambda} &= -\frac{2c\gamma}{(2\theta - c)\lambda^2}, \frac{\partial^2 S}{\partial \lambda^2} = \frac{4c\gamma}{(2\theta - c)\lambda^3}, \frac{\partial U}{\partial \lambda} = -\frac{4c\gamma^2\theta^2}{(2\theta - c)^2\lambda^2}, \frac{\partial^2 U}{\partial \lambda^2} = \frac{8c\gamma^2\theta^2}{(2\theta - c)^2\lambda^3} \end{aligned} \quad (\text{A5})$$

$$\text{(v)} \quad \frac{\partial t}{\partial r} = \frac{2(2\theta - c)}{(2\theta + c)^2}, \frac{\partial T}{\partial r} = \frac{2c}{(2\theta + c)^2}, \frac{\partial U}{\partial r} = \frac{c^2}{(2\theta + c)^2} \quad (\text{A6})$$

$$\begin{aligned}
 \text{(vi)} \quad \frac{\partial K}{\partial c} &= \frac{2\theta}{(2\theta+c)^2}, \quad \frac{\partial^2 K}{\partial c^2} = -\frac{4\theta}{(2\theta+c)^3}, \quad \frac{\partial K}{\partial \theta} = -\frac{2c}{(2\theta+c)^2}, \quad \frac{\partial^2 K}{\partial \theta^2} = \frac{8c}{(2\theta+c)^3}, \\
 \frac{\partial k}{\partial c} &= -\frac{4\theta}{(2\theta+c)^2}, \quad \frac{\partial^2 k}{\partial c^2} = \frac{8\theta}{(2\theta+c)^3}, \quad \frac{\partial k}{\partial \theta} = \frac{4c}{(2\theta+c)^2}, \quad \frac{\partial^2 k}{\partial \theta^2} = -\frac{16c}{(2\theta+c)^3}
 \end{aligned}
 \tag{A7}$$

References

- Anderson, R. (2001). Why information security is hard: An economic perspective. Proceedings of the 17th Annual Computer Security Applications Conference, December 10-14, New Orleans,
- Arora, A., R. Krishnan, R. Telang, Yang, Y., 2005. An empirical analysis of vendor response to software vulnerability disclosure. Working Paper, Carnegie Mellon University, August 2005.
- Cavusoglu, H., B. Mishra, B., Raghunathan, S., 2005. The value of intrusion detection systems in information technology security architecture. *Information Systems Research* 16, 1, 28-46.
- Choi, J., C. Fershtman, Gandal, N., 2005. The economics of internet security. Department of Economics, Michigan State University, December 6, 2005.
- 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. *Information Systems Research* 16 (2), 186-208.
- Gordon, L.A., Loeb, M., 2001. Using information security as a response to competitor analysis systems. *Communications of the ACM* 44, 9, 70-75.
- 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, 95-111.
- Gordon, L.A., Loeb, M., Lucyshyn, W., 2003. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* 22 (7), 461-485.
- Gordon, L.A., Loeb, M., Lucyshyn, W., Richardson, R., 2004. 2004 CSI/FBI computer crime and security survey. *Computer Security Journal* XX (3), 33-51.
- Hausken, K., 2005, Production and conflict models versus rent seeking models, *Public Choice* 123, 59-93.
- Hausken, K. (2006), Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment, *Journal of Accounting and Public Policy* 25, 6, 629-665.
- Hausken, K. (2007), Information Sharing among Firms and Cyber Attacks, *Journal of Accounting and Public Policy* 26, 6, 639-688.
- Hausken, K. (2009), "Security Investment and Information Sharing for Defenders and Attackers of Information Assets and Networks," in Rao, H.R. and Upadhyaya, S.J. (eds.), *Information Assurance, Security and Privacy Services*, Handbooks in

- Information Systems, Volume 4, Emerald Group Pub Ltd, United Kingdom, 503-534.
- Howard, J., 1997. Analysis of security incidents on the Internet. Unpublished Doctoral Dissertation, Carnegie Mellon University, www.cert.org/research/JHThesis/Start.htm .
- Hirshleifer, J., 1995. Anarchy and its breakdown. *Journal of Political Economy* 103(1), 26-52.
- Kirby, A., 1988. Trade associations as information exchange mechanisms. *RAND Journal of Economics* 29 (1), 138-146.
- Kjaerland, M., 2005. A classification of computer security incidents based on reported attack data, *Journal of Investigative Psychology and Offender Profiling* 2, 105-120.
- Kremen, H., 1998. Apprehending the computer hacker: The collection and use of evidence. *Computer Forensics Online*.
- Kunreuther, H., Heal, G., 2003. Interdependent security. *The Journal of Risk and Uncertainty* 26, 2/3, 231-249.
- Lin. Y., 2003. The institutionalization of hacking practices. *Ubiquity*. Volume 4, Issue 4.
- Nizovtsev, D., M. Thursby. 2005. Economic analysis of incentives to disclose software Vulnerabilities. Working Paper.
- Novshek, W., Sonnenschein, H., 1982. Fulfilled expectations in Cournot duopoly with information acquisition and release. *Bell Journal of Economics* 13 (1), 214-218.
- Pinker, E.J. (2007), An Analysis of Short-Term Responses to Threats of Terrorism, *Management Science* 53, 6, 865–880.
- Png, I., C. Tang, Wang, Q., 2006. Information security: User precautions and hacker targeting. Working Paper, National University of Singapore.
- Platt, C. 1996. *Anarchy Online (Net Crime/Net Sex)*, Harper Collins, New York..
- Raymond, E., 2001. *The cathedral and the bazaar: Musings on linux and open source by an accidental revolutionary*. Revised edition. O'Reilly.
- Ritchie, C., 2000. A look at the security of the open source development model. Technical Report, Oregon State University.
- Risan, L., 2000. Hackers produce more than software, they produce hackers. Version 2.1 http://folk.uio.no/lr_isan/Linux/Identity_games/
- Salop, S.C., Scheffman, D., 1983. Raising rivals' costs. *A.E.R. Papers and Proceedings*, 73, 267-271.
- Shapiro, C., 1986. Exchange of cost information in oligopoly. *Review of Economic Studies* 53 (3), 433–446.
- Tullock, G., 1967. The welfare costs of tariffs, monopolies, and theft. *Western Economic Journal* 5, 224-232.
- Tullock, G., 1980. Efficient rent seeking. In: J. Buchanan, R. Tollison and G. Tullock, (Eds.), *Towards a Theory of the Rent-Seeking Society*, College Station, Texas A&M University Press, pp. 97-112.
- Vives, X., 1990. Trade association disclosure rules, incentives to share information, and welfare. *RAND Journal of Economics* 21 (3), 409–430.

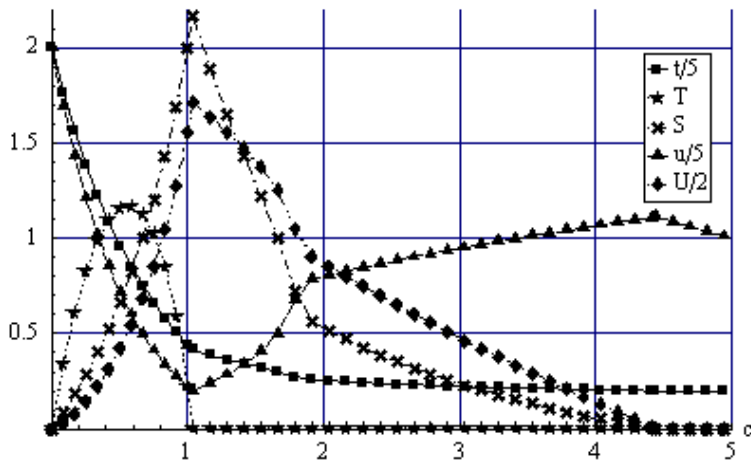


Figure 2: The variables t , T , S , u , U as functions of the firm's unit cost c .

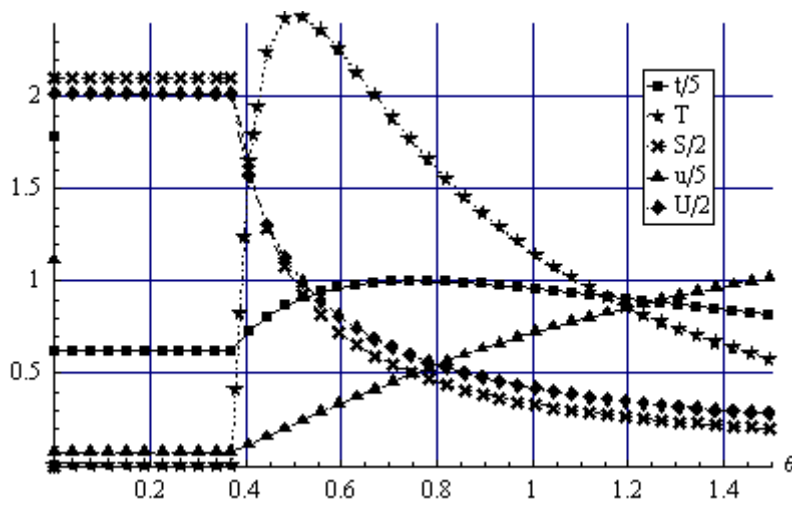


Figure 3: The variables t , T , S , u , U as functions of the hackers' unit cost θ .

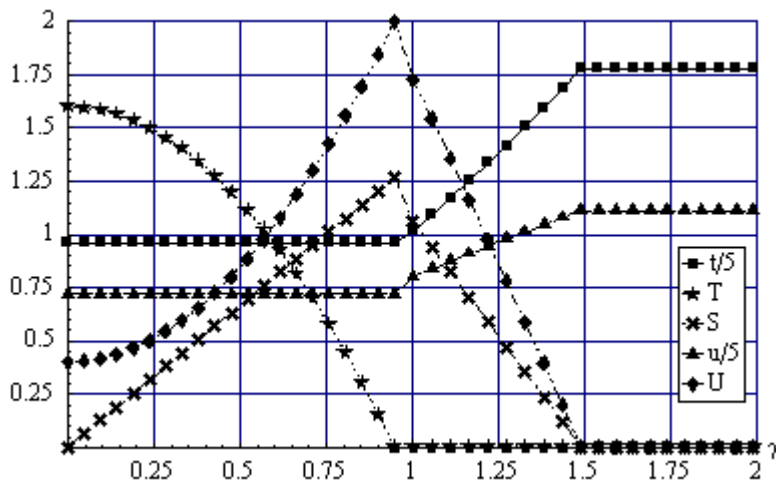


Figure 4: t , T , S , u , U as functions of the hackers' information sharing effectiveness parameter γ .

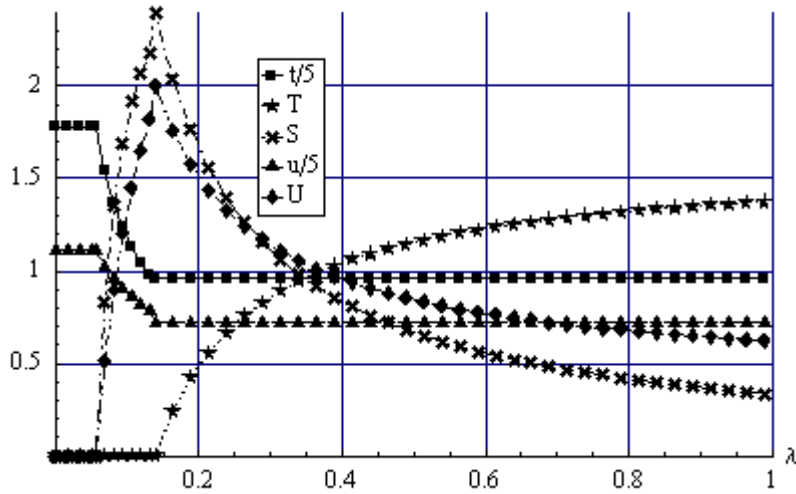


Figure 5: The variables t , T , S , u , U as functions of the intensity of joint information sharing λ .

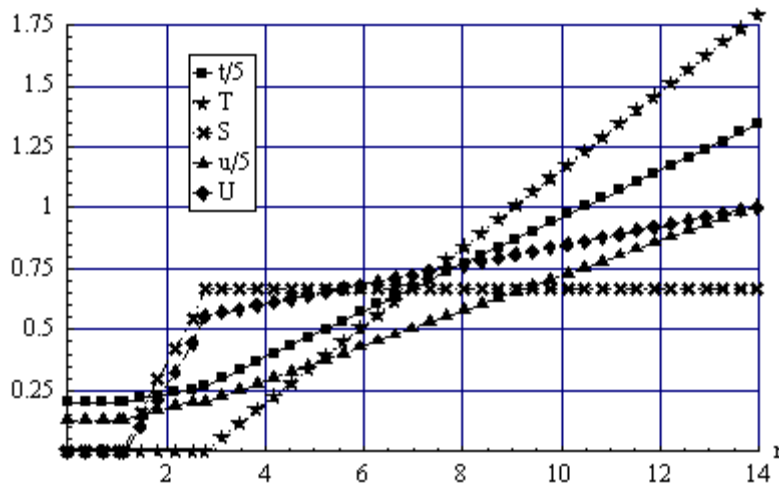


Figure 6: The variables t , T , S , u , U as functions of the firm's asset r .

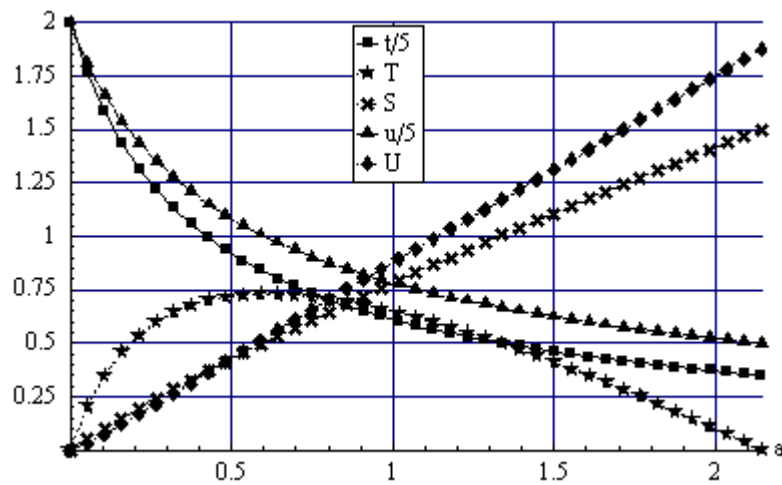


Figure 7: t , T , S , u , U as functions of the hackers' unit defense cost a .

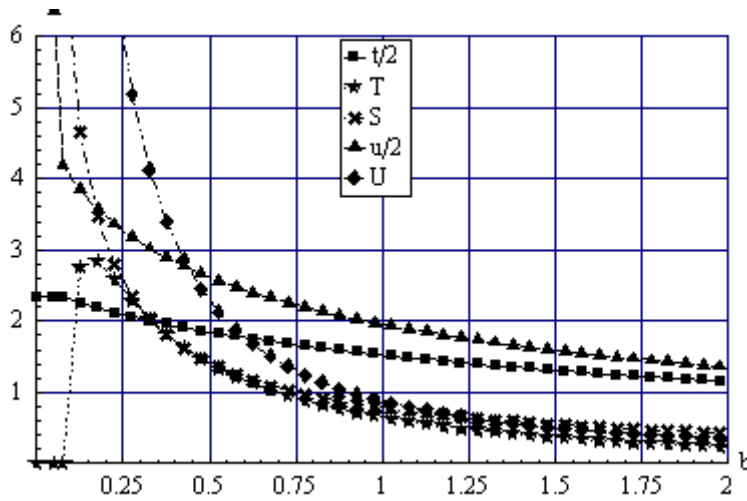


Figure 8: t, T, S, u, U as functions of the firm's unit production cost b .

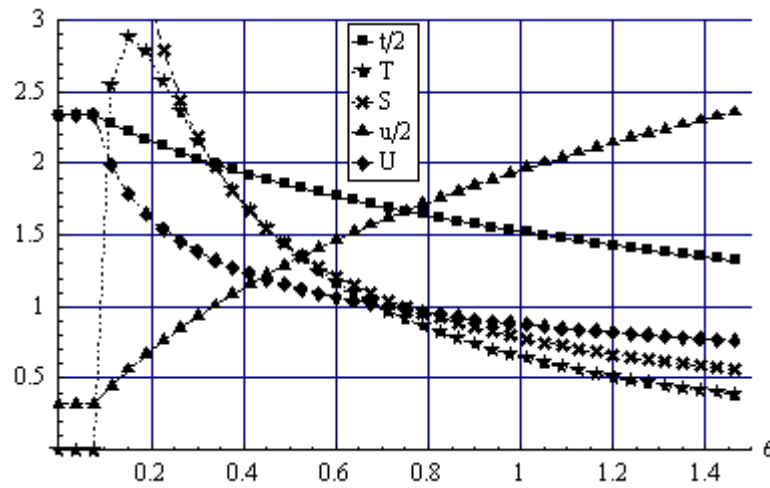


Figure 9: t, T, S, u, U as functions of the hackers' unit cost θ .

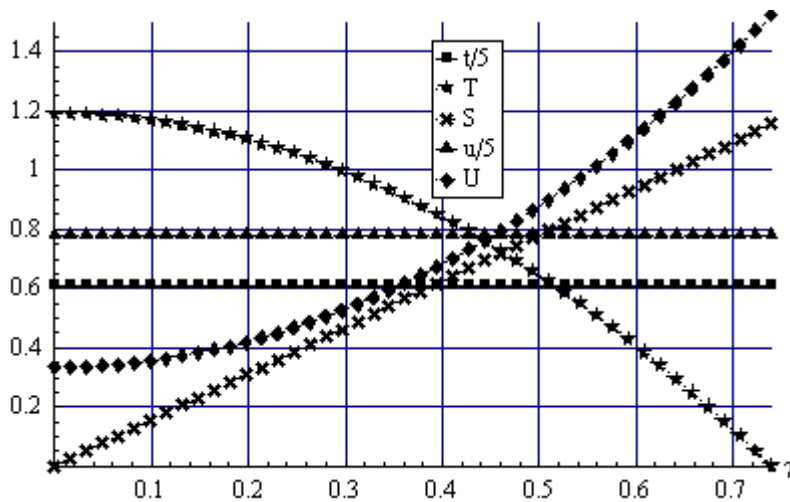


Figure 10: t, T, S, u, U as functions of the information sharing effectiveness γ .

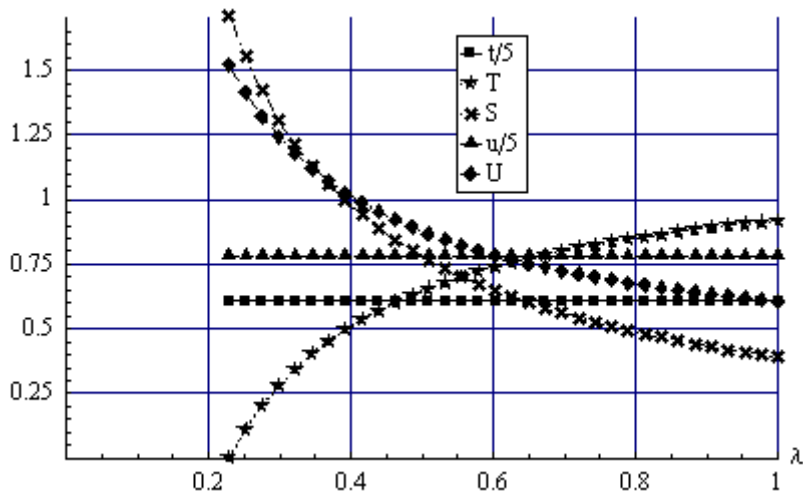


Figure 11: t , T , S , u , U as functions of the intensity of joint information sharing λ .

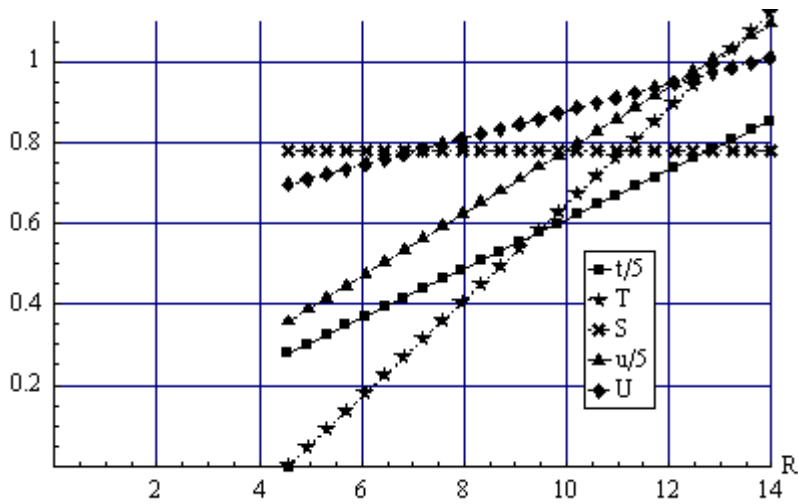


Figure 12: t , T , S , u , U as functions of the firm's resource R .