games

MDPI

Article

# Security Investment, Hacking, and Information Sharing between Firms and between Hackers

**Kjell Hausken**

Faculty of Social Sciences, University of Stavanger, 4036 Stavanger, Norway; kjell.hausken@uis.no; Tel.: +47-51-831632

Academic Editor: Christos Dimitrakakis
Received: 5 April 2017; Accepted: 21 May 2017; Published: 25 May 2017

**Abstract:** A four period game between two firms and two hackers is analyzed. The firms first defend and the hackers thereafter attack and share information. Each hacker seeks financial gain, beneficial information exchange, and reputation gain. The two hackers' attacks and the firms' defenses are inverse U-shaped in each other. A hacker shifts from attack to information sharing when attack is costly or the firm's defense is cheap. The two hackers share information, but a second more disadvantaged hacker receives less information, and mixed motives may exist between information sharing and own reputation gain. The second hacker's attack is deterred by the first hacker's reputation gain. Increasing information sharing effectiveness causes firms to substitute from defense to information sharing, which also increases in the firms' unit defense cost, decreases in each firm's unit cost of own information leakage, and increases in the unit benefit of joint leakage. Increasing interdependence between firms causes more information sharing between hackers caused by larger aggregate attacks, which firms should be conscious about. We consider three corner solutions. First and second, the firms deter disadvantaged hackers. When the second hacker is deterred, the first hacker does not share information. Third, the first hacker shares a maximum amount of information when certain conditions are met. Policy and managerial implications are provided for how firms should defend against hackers with various characteristics.

**Keywords:** information sharing; cyber security; game theory; asset allocation; cyber war; contest success function; security investment; policy

## 1. Introduction

### *1.1. Background*

The Internet enables cyber hackers to attack and gain information from firms, requiring firms to design a variety of defensive security measures. So many firms, institutions, elections, etc. have been hacked that assessing who may be exempt is challenging or impossible. This raises the issue of counter measures. The gathering, analysis and sharing of information has been launched as one counter measure. Encouraging information sharing, the US federal government recommends Security Based Information Sharing Organizations (SB/ISOs), e.g., Information Sharing & Analysis Centers (ISACs), CERT, INFRAGARD, etc. Kampanakis [1] elaborates upon attempts to standardize security information sharing. Cyber attacks and information sharing differ in that the former demands funding, planning, effort, competence, infrastructure, etc., while the latter may be practically costless except providing the information, which today is possible in almost innumerable ways. One benefit of information sharing for firms are that if several firms know what each firm knows individually, they may benefit collectively in preventing future security breaches. That may improve their reputation, and enhance sales and profits. One benefit of information sharing for hackers is that if they cooperate, they

may become more successful. Hackers may be malevolent agents, but may also be firms exploiting rival firms.

### *1.2. Early and General Literature*

Novshek and Sonnenschein [2], Gal-Or [3], Shapiro [4], Kirby [5], and Vives [6] consider information sharing in duopolies, oligopolies, and trade associations. Cremonini and Nizovtsev [7] show that well-protected targets can deter strategic attackers through signaling. Fultz and Grossklags [8] conceptualize distributed security attacks. Herley [9] considers collisions among attackers. Lin [10] assesses how hacking practices are institutionalized. Sarvari, et al. [11] evaluate criminal networks. August, et al. [12] assess how software network structure and security risks are impacted by cloud technology. Dey, et al. [13] assess quality competition and market segmentation in the security software market. Dey, et al. [14] analyze the security software market, including network effects and hacker behavior. Galbreth and Shor [15] evaluate how the enterprise software industry is impacted by malevolent agents. Chul Ho, et al. [16] consider double moral hazard when contracting information security. Ransbotham and Mitra [17] develop a model of paths to information security compromise.

### *1.3. Information Sharing among Firms*

Information sharing among firms to defend against cyber attacks has received scrutiny. Gordon, et al. [18] evaluate how information sharing affects information security, focusing on the cost side effects. They show that firms have a tradeoff between investing in information security and free riding, which may cause under-investment in security. Gal-Or and Ghose [19] assess the competition in the product market on information sharing and security investment, focusing on the demand side effects. Hausken [20,21] determines that information sharing and security investment for two firms are inverse U-shaped in the aggregate attack, impacted by their interdependence.

Making different assumptions, Gal-Or and Ghose [19] find that security investments and information sharing are strategic complements, while Hausken [21] finds that they are strategic substitutes. Gordon, Loeb and Lucyshyn [18] determine that sharing information induces a firm to invest less in information security.

Gao, et al. [22] consider how two firms with complementary information assets approach information sharing and security investments. Liu, et al. [23] show that complementary firms share information, and substitutable firms free ride and require a social planner to ensure information sharing. Mallinder and Drabwell [24] investigate information sharing and data sensitivity. Choras [25] assesses technical, human, organizational, and regulatory dimensions related to information sharing and network security. Tamjidyamcholo, et al. [26] relate information sharing to self-efficacy, trust, reciprocity, and shared language. Rocha Flores, et al. [27] assess how behavioral information security governance and national culture impact information sharing. Tamjidyamcholo, et al. [28] find that knowledge sharing depends crucially on perceived consequences, affect, and facilitating conditions, and marginally on social factors.

In a related stream of work, Png and Wang [29] consider user precautions vis-à-vis enforcement against attackers, and strategic interaction among end-users and between users and hackers with a continuum of user types. They show that users' effort in fixing depends on hackers' targeting and vice-versa. Prior work e.g., by Choi, et al. [30], Nizovtsev and Thursby [31], Arora, et al. [32], and Temizkan, et al. [33]) has considered incentives to disclose security flaws and provide patches. Cavusoglu, et al. [34] and Moore, et al. [35] argue that misplaced incentives rather than technical reasons may cause systems failure. See Skopik, et al. [36] for a review.

### *1.4. Information Sharing among Hackers*

Hackers sharing information operate differently. It has hardly been studied except statically by Hausken [37] and in a repeated game by Hausken [38]. Firms being hacked prefer to avoid

or obstruct anything that may give hackers a competitive edge, such as sharing information or otherwise cooperating to improve their attacks. Hackers gather information about firms' weaknesses, vulnerabilities, defenses, and information firms gather about security breaches. Hackers may choose to share this information with each other, and/or make it publicly available.

Raymond [39] argues that hackers may prefer not to share information due to competition and, as also argued by Ritchie [40], to enhance one's reputation. However, Brunker [41] offers the contrasting argument that hackers seldom keep secrets. This paper allows the role of both competition and seeking reputation thus accounting for the multiple possibilities.

### *1.5. This Paper's Contribution*

In this paper, we make the context especially realistic by simultaneously studying the impact of information sharing amongst hackers and information sharing amongst firms. The analysis endogenizes firms' decisions to share information and allows comparison between the firms' strategies when they share information vis-à-vis when they do not. The analysis strengthens the managerial implications compared with isolated analyses of information sharing between hackers, or information sharing between firms.

More specifically, this paper analyzes two hackers who may share information about firms' vulnerabilities, in addition to deciding on the size of their attacks. The firms invest in information security to defend against the attacks, and additionally share information with each other after the first hackers attack. Naturally, each hacker prefers to receive information from the other hacker, but may be reluctant to deliver information, though there are benefits from joint information sharing. We assume that both hackers and the defending firm are strategic players. 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.

The two hackers and two firms are considered as unitary players. Firms are usually collective players. Hackers may also be collective players. For non-unitary players that are sufficiently aligned e.g., regarding preferences, or can somehow be assigned similar preferences, Simon's [42] principle of near-decomposability may be applicable. That means that players that are not entirely unitary may be interpreted as unitary as an approximation. For example, firms may perceive each hacker as some unidentified player out there which may either be coordinated, uncoordinated, or may perhaps even consist of disparate players who do not know each other but may have a common objective. Similarly, each firm may be a division within a company, or a conglomerate that is somehow able to design a unitary defense and share information with another conglomerate.

We build a model where a hacker has a triple motivation. The first is attacking for financial gain, e.g., through stealing assets like credit card information of the firms' customers. The second is information exchange with the other hacker for joint benefit and synergy to lay the foundation for future superior exploits. The third is to obtain reputation, e.g., through sharing information on websites etc., showcasing the flaws in the firms' security, and demonstrating in various ways the hacker's capabilities to the world.

Hackers often conduct concerted attacks, which means that they work together and benefit from each other's penetration. In our model first the firms defend against the first hacker. Second, the first hacker attacks the firms and shares information with the second hacker. Third, the firms share information with each other and defend against the second hacker. Fourth, the second hacker uses the information from the first hacker and attacks the firms. After the attacks, hackers share their information and experiences with other hackers in various hacking community forums, and more hackers will or may launch similar attacks on the same firms or similar firms. Characteristics of the information are the type of firewalls (e.g., network layers or packet filters, application-layers, proxy servers, network address translation), encryption techniques (e.g., hashing, private-key cryptography, public-key cryptography), access control mechanisms, intrusion detection systems, etc. employed by the firms, the training and procedures of the firms' security experts, the nature of the defense, and the

properties of the vulnerabilities. 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 firms' vulnerabilities and defense.

We interpret "attack" and "defense" broadly, inspired by Hirshleifer [43], who states that "falling also into the category of interference struggles are political campaigns, rent-seeking maneuvers for licenses and monopoly privileges [44], commercial efforts to raise rivals' costs [45], strikes and lockouts, and litigation—all being conflicting activities that need not involve actual violence". In the model we use credible specific functional forms to produce exact analytical solutions for the variables. In return for the sacrifice of generality, a successful specification demonstrates internal consistency, illumination, and ranges of parameter values where the various equilibriums exist.

## 2. Model

We develop a sequential move four period model for the interaction between two hackers $i$ and $j$ and two firms $A$ and $B$. The players are fully rational and have complete information. Table 1 provides the nomenclature. Figure 1 illustrates the four time periods in the game. Figure 2 shows the interaction between the players.

**Table 1.** Nomenclature, *iv* = independent variable, *dv* = dependent variable, *p* = parameter.

| | | |
|---|---|---|
| $t_{Qi}$ | Firm $Q$'s defense against hacker $i$ in period 1, $Q = A,B$ | *iv* |
| $t_{Qj}$ | Firm $Q$'s defense against hacker $j$ in period 3, $Q = A,B$ | *iv* |
| $s_Q$ | Firm $Q$'s information sharing with the other firm in period 3, $Q = A,B$ | *iv* |
| $T_{Qi}$ | Hacker $i$'s attack against firm $Q$ in period 2, $Q = A,B$ | *iv* |
| $T_{Qj}$ | Hacker $j$'s attack against firm $Q$ in period 4, $Q = A,B$ | *iv* |
| $S_i$ | Hacker $i$'s information sharing with hacker $j$ in period 2 | *iv* |
| $u_Q$ | Firm $Q$'s expected utility, $Q = A,B$ | *dv* |
| $U_k$ | Hacker $k$'s expected utility, $k = i,j$ | *dv* |
| $S_j$ | Hacker $j$'s information sharing with hacker $i$ in period 4 | *p* |
| $v_k$ | Each firm's asset value before hacker $k$'s attack, $k = i,j$ | *p* |
| $V_k$ | Hacker $k$'s valuation of each firm before its attack, $k = i,j$ | *p* |
| $c_k$ | Each firm's unit defense cost before hacker $k$'s attack, $k = i,j$ | *p* |
| $C_k$ | Hacker $k$'s unit attack cost, $k = i,j$ | *p* |
| $\alpha$ | Interdependence between the firms | *p* |
| $\gamma$ | Information sharing effectiveness between firms | *p* |
| $\phi_1$ | Each firm's unit cost (inefficiency) of own information leakage | *p* |
| $\phi_2$ | Each firm's unit benefit (efficiency) of the other firm's information leakage | *p* |
| $\phi_3$ | Each firm's unit benefit (efficiency) of joint information leakage | *p* |
| $\Gamma_k$ | Hacker $k$'s information sharing effectiveness with the other hacker, $k = i,j$ | *p* |
| $\Lambda_k$ | Hacker $k$'s utilization of joint information sharing, $k = i,j$ | *p* |
| $\Omega_k$ | Hacker $k$'s reputation gain parameter, $k = i,j$ | *p* |

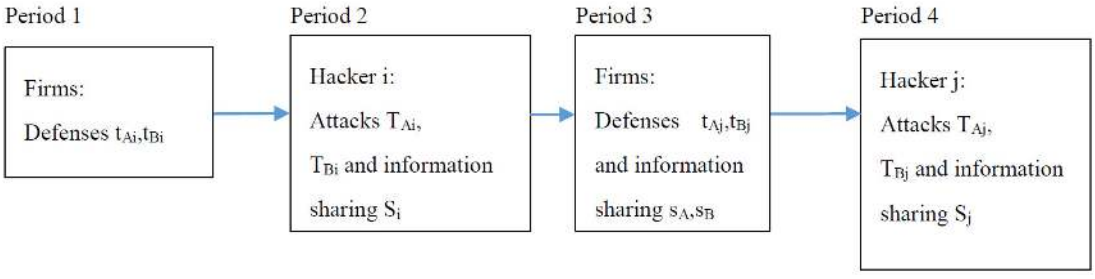


**Figure 1.** Four period game.

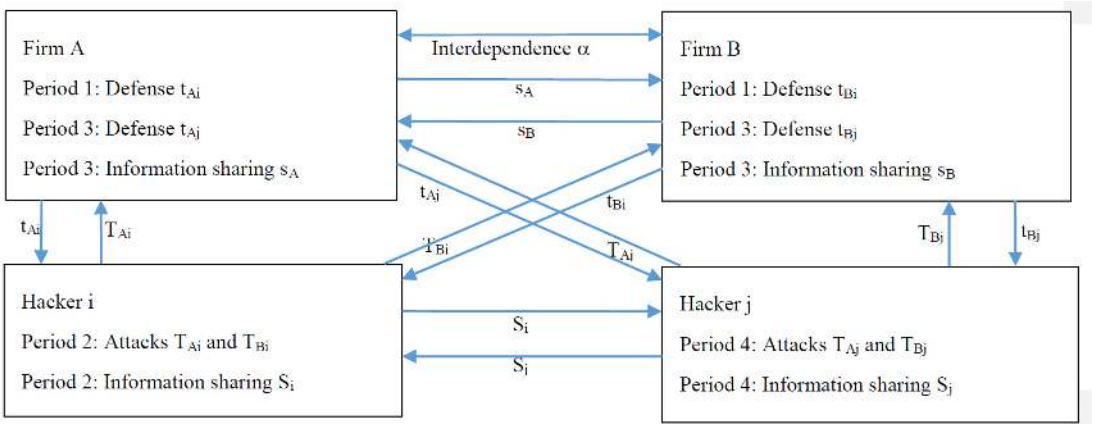


**Figure 2.** Interaction between two firms and between two hackers.

Period 1: Both firms exert defense efforts $t_{Ai}$ and $t_{Bi}$ to protect against potential future attacks.

Period 2: Hacker $i$, without loss of generality, exerts attack effort $T_{Ai}$ against firm $A$ and attack effort $T_{Bi}$ against firm $B$, and shares with hacker $j$ information $S_i$ which includes knowledge about the firms' vulnerabilities. Hacker $i$ knows that hacker $j$ does not already possess the information $S_i$ before it is provided. The actual breach, if the attacker succeeds so that a breach occurs, and to the extent a breach occurs, occurs in period 2.

Period 3: Knowing that hacker $i$ may or may not share its information gained from the attack in period 1 with other hackers, the firms exert defense efforts $t_{Aj}$ and $t_{Bj}$ against firms $A$ and $B$ to protect against future attacks. Additionally, firms $A$ and $B$ share information $s_A$ and $s_B$, respectively, with each other based on what they learned from the two attacks by hacker $i$.

Period 4: Hacker $j$ exerts attack efforts $T_{Aj}$ and $T_{Bj}$ against firms $A$ and $B$ to obtain further information, and shares information $S_j$ with hacker $i$ for future joint benefit. The actual breach by hacker $j$, if it occurs and to the extent it occurs, occurs in period 4. Hacker $j$ is either another attacker than hacker $i$, or a combination of attackers considered as unitary, or a combination of attackers including hacker $i$.

In period 1 the firms have one strategic choice variable each which are their defenses $t_{Ai}$ and $t_{Bi}$. The firms do not know which hacker attacks first, but prepare by defending against any hacker. In period 2 hacker $i$, which is the first hacker that happens to attack, has three strategic choice variables which are the attacks $T_{Ai}$ and $T_{Bi}$ and information sharing $S_i$. Information $S_i$ is delivered by hacker $i$ to hacker $j$ in period 2. Hacker $i$ chooses $T_{Ai}$ and $T_{Bi}$ before $S_i$, using the attacks to gather information, but since the three choices are made in period 2, it is mathematically sufficient to state that $T_{Ai}$, $T_{Bi}$ and $S_i$ are made in period 2. The firms' defense efforts in period 1 last two periods, and thereafter have to be renewed. In period 3 the firms again have one strategic choice variable each which are their defenses $t_{Aj}$ and $t_{Bj}$. In period 4 hacker $j$ has two strategic choice variables which are the attacks $T_{Ai}$ and $T_{Bi}$, and information $S_j$ is a parameter since the game ends after period 4. Hacker $j$ uses the information $S_i$ from hacker $i$ when exerting its attacks. In real life subsequent defense, attacks and information sharing occur after period 4, with $S_j$ as a free choice variable. However, considering more periods than the four in Figure 1 is beyond this paper's scope.

Each firm has an asset valued as $v_i$ before hacker $i$'s attack, and valued as $V_i$ by hacker $i$. The firms invest $t_{Ai}$ and $t_{Bi}$ to defend their assets, with defense expenditures $f_{Ai}$ and $f_{Bi}$, where $\partial f_{Ai}/\partial t_{Ai} > 0$ and $\partial f_{Bi}/\partial t_{Bi} > 0$. To obtain financial gain, hacker $i$ invests $T_{Ai}$ and $T_{Bi}$ to attack the assets, with attack expenditures $F_{Ai}$ and $F_{Bi}$, where $\partial F_{Ai}/\partial T_{Ai} > 0$ and $\partial F_{Bi}/\partial T_{Bi} > 0$. We consider, for simplicity, linear functions $f_{Ai} = c_i t_{Ai}$, $f_{Bi} = c_i t_{Bi}$, $F_{Ai} = C_i T_{Ai}$, and $F_{Bi} = C_i T_{Bi}$, where $c_i$ is the unit cost (inefficiency) of cyber defense for both firms and $C_i$ is the unit cost (inefficiency) of cyber attack for hacker $i$. Highly competent players (defenders or attackers) have lower unit costs than less competent

players since they can exert efforts (defense or attack) more efficiently with less effort. An incompetent player has infinite unit cost, and is incapable of defending or attacking. An attack means attempting to break through the security defense of the firm in order to appropriate something that is valuable to the firm. Examples are customer related information, business strategy information or accounting related information. We assume, for simplicity, risk-neutral players, which does not change the nature of the argument. The expenditures $c_i t_{Ai}$, $c_i t_{Bi}$, $C_i T_{Ai}$, and $C_i T_{Bi}$ can be interpreted as expenses in capital and/or labor.

Hacker $i$ has a triple motivation of financial gain through the attacks $T_{Ai}$ and $T_{Bi}$, information exchange with hacker $j$ for mutual benefit, and reputation gain through information sharing $S_i$. Information sharing $S_i$ has three interpretations in this model; that it is provided exclusively to hacker $j$, provided exclusively to the entire hacking community, and released publicly.

For the first motivation, the cyber contest between hacker $i$ and firm $Q$, $Q = A,B$, takes the common ratio form [46,47]. We consider the contest success function

$$g_{Qi}^{\alpha=0} = \frac{T_{Qi}}{T_{Qi} + t_{Qi}} \tag{1}$$

which is the probability that hacker $i$ wins and the firm loses the contest, $\partial g_{Qi}^{\alpha=0}/\partial T_{Qi} > 0$, $\partial g_{Qi}^{\alpha=0}/\partial t_{Qi} < 0$, where $\alpha = 0$ means independent firms. This means that firm $Q$ benefits from its own security investment, and suffers from hacker $i$'s attack. When penetration occurs, the loss incurred by firm $Q$ may not be the same as the value gained by hacker $i$. Moreover, hacker $i$ may attack a subset of the firm's assets, and the same subset may be valued differently by hacker $i$ and firm $Q$. This is accounted for by the different valuations $v_i$ by each firm and $V_i$ by hacker $i$. Hacker $i$'s utility is thus its benefit $g_{Qi}^{\alpha=0} V_{Qi}$ minus its expenditure $C_i T_{Qi}$. Firm $Q$'s utility is its initial asset value $v_i$ minus its loss $g_{Qi}^{\alpha=0} v_{Qi}$ minus its expenditure $c_{Qi} t_{Qi}$. Applying (1), the utilities from the first attack for hacker $i$ and firm $Q$, respectively, are

$$U_i^{first,\alpha=0} = \frac{T_{Ai}}{T_{Ai} + t_{Ai}} V_i + \frac{T_{Bi}}{T_{Bi} + t_{Bi}} V_i - C_i T_{Ai} - C_i T_{Bi}, \quad u_Q^{first} = v_i - \frac{T_{Qi}}{T_{Qi} + t_{Qi}} v_i - c_i t_{Qi} \tag{2}$$

As in Kunreuther and Heal [48] and Hausken [21,49], we assume interdependence $\alpha$ between the firms, so that an attack on one firm gets transferred with a proportionality parameter $\alpha$ as an attack on the other firm. Analogously, one firm's defense also defends the other firm with proportionality parameter $\alpha$. We assume $\alpha \leq 1$ where $\alpha = 0$ means independent firms and negative $\alpha$ means that each firm's security investment is detrimental to the other firm, and merely strengthens one's own firm. Thus, generalizing (1) from $\alpha = 0$ to general $\alpha$, the contest for firm $A$'s asset gives the probability

$$g_{Ak} = \frac{T_{Ak} + \alpha T_{Bk}}{t_{Ak} + T_{Ak} + \alpha(t_{Bk} + T_{Bk})} \tag{3}$$

that hacker $k$ gains the asset, $k = i,j$, where the attack on firm $A$ consists of $T_{Ak}$ directly from hacker $k$ and $\alpha T_{Bk}$ indirectly from hacker $k$ through firm $B$ and onto firm $A$. Analogously, the contest for firm $B$'s asset gives the probability

$$g_{Bk} = \frac{T_{Bk} + \alpha T_{Ak}}{t_{Bk} + T_{Bk} + \alpha(t_{Ak} + T_{Ak})} \tag{4}$$

that hacker $k$ gains the asset, $k = i,j$.

After hacker $i$'s attack in period 2, we assume in period 3 that firm $A$ shares information $s_A$ with firm $B$ with sharing effectiveness $\gamma$, and firm $B$ shares information $s_B$ with firm $A$ with sharing effectiveness $\gamma$. Receiving information from the other firm strengthens firm $A$'s defense from $t_{Aj}$ to

$t_{Aj} + \gamma s_B$, and strengthens firm $B$'s defense from $t_{Bj}$ to $t_{Bj} + \gamma s_A$, against hacker $j$. We thus replace the probabilities in (3) and (4) with

$$h_{Aj} = \frac{T_{Aj} + \alpha T_{Bj}}{t_{Aj} + \gamma s_B + T_{Aj} + \alpha(t_{Bj} + \gamma s_A + T_{Bj})}, \quad h_{Bj} = \frac{T_{Bj} + \alpha T_{Aj}}{t_{Bj} + \gamma s_A + T_{Bj} + \alpha(t_{Aj} + \gamma s_B + T_{Aj})} \tag{5}$$

respectively, where $t_{Aj} + \gamma s_B + \alpha(t_{Bj} + \gamma s_A)$ and $t_{Bj} + \gamma s_A + \alpha(t_{Aj} + \gamma s_B)$ are firm $A$'s and firm $B$'s, respectively, aggregate defenses against hacker $j$. When hacker $i$ shares information $S_i$ with hacker $j$, the effectiveness of hacker $i$'s sharing is a function of its attacking effort levels $T_{Ai} + T_{Bi}$. The reason is that when hacker $i$ exerts higher effort in attacking, e.g., more efforts on scanning and probing the firms before attacks, the information it collects and shares becomes more valuable to hacker $j$. We assume for simplicity linear effectiveness $\Gamma_i(T_{Ai} + T_{Bi})$, proportional to effort $T_{Ai} + T_{Bi}$, where the parameter $\Gamma_i$ is hacker $i$'s sharing effectiveness. Consequently, hacker $j$ can utilize the effectiveness $\Gamma_i(T_{Ai} + T_{Bi})$ multiplied with the amount $S_i$ that hacker $i$ shares, i.e., $\Gamma_i(T_{Ai} + T_{Bi})S_i$, scaled in the same denomination as hacker $j$'s effort $T_j$ in the second attack. Hacker $i$ cannot share more information than what has become available through its attacks, i.e., $0 \leq S_i \leq \Gamma_i(T_{Ai} + T_{Bi})$. Hence we replace the probabilities in (5) for hacker $j$ with

$$\begin{aligned} q_{Aj} &= \frac{T_{Aj} + \alpha T_{Bj} + \Gamma_i(T_{Ai} + T_{Bi})S_i}{t_{Aj} + \gamma s_B + T_{Aj} + \alpha(t_{Bj} + \gamma s_A + T_{Bj}) + \Gamma_i(T_{Ai} + T_{Bi})S_i}, \\ q_{Bj} &= \frac{T_{Bj} + \alpha T_{Aj} + \Gamma_i(T_{Ai} + T_{Bi})S_i}{t_{Bj} + \gamma s_A + T_{Bj} + \alpha(t_{Aj} + \gamma s_B + T_{Aj}) + \Gamma_i(T_{Ai} + T_{Bi})S_i} \end{aligned} \tag{6}$$

against firms $A$ and $B$ respectively, where $T_{Aj} + \alpha T_{Bj} + \Gamma_i(T_{Ai} + T_{Bi})S_i$ and $T_{Bj} + \alpha T_{Aj} + \Gamma_i(T_{Ai} + T_{Bi})S_i$ are hacker $j$'s aggregate attack against firms $A$ and $B$, respectively. After both hackers' attacks, the two hackers share their information with each other for mutual benefit, which is their second motivation. First, $\Gamma_i(T_{Ai} + T_{Bi})S_i$ expresses what hacker $j$ can utilize from hacker $i$. Second, $\Gamma_j(T_{Aj} + T_{Bj})S_j$ expresses what hacker $i$ can utilize from hacker $j$. The two hackers have different sharing effectiveness parameters $\Gamma_i$ and $\Gamma_j$ caused by differences in sharing competence, skills, motivations, beliefs, and information processing capacities. The sharing effectiveness $\Gamma_i$ also depends on how well hacker $i$ extracts information from its attacks $T_{Ai}$ and $T_{Bi}$, how effectively hacker $i$ shares information with hacker $j$, hacker $j$'s capability and willingness to use the information, and it scales $(T_{Ai} + T_{Bi})S_i$ relative to $T_{Bj} + \alpha T_{Aj}$. The two hackers' joint benefit is expressed by the product of these two expressions, i.e., $\Gamma_i(T_{Ai} + T_{Bi})S_i\Gamma_j(T_{Aj} + T_{Bj})S_j$. Hackers $i$ and $j$ earn a utility proportional to this joint benefit, with proportionality parameters $\Lambda_i$ and $\Lambda_j$, respectively. The parameters $\Lambda_i$ and $\Lambda_j$ are scaling parameters in the hackers' utility functions and reflect differences in the two hackers' ability to utilize and process joint sharing. They account only for mutual information sharing expressed with the product $S_iS_j$, in contrast to $\Gamma_i$ and $\Gamma_j$, which account only for one way information sharing. If $\Lambda_i = \Lambda_j = 0$, the two hackers are unable to utilize joint sharing. Upper limits exist to $\Lambda_i$ and $\Lambda_j$ so that information shared by the two hackers is not more valuable than if the same amount of information is generated by only one hacker. This gives

$$\Theta_i = \Lambda_i\Gamma_i(T_{Ai} + T_{Bi})S_i\Gamma_j(T_{Aj} + T_{Bj})S_j, \quad \Theta_j = \Lambda_j\Gamma_i(T_{Ai} + T_{Bi})S_i\Gamma_j(T_{Aj} + T_{Bj})S_j \tag{7}$$

to hackers $i$ and $j$, respectively.

Hacker $k$'s third motivation of information sharing for reputation gain is also obtained through $S_k$. Also here we scale proportional to effort $T_{Ak} + T_{Bk}$, yielding

$$\Psi_i = \Omega_i(T_{Ai} + T_{Bi})S_i, \quad \Psi_j = \Omega_j(T_{Aj} + T_{Bj})S_j \tag{8}$$

to hackers $i$ and $j$, respectively, where $\Omega_k$ is the reputation gain parameter which expresses hacker $k$'s capabilities of obtaining and marketing its reputation gain. The parameters $\Omega_i$ and $\Omega_j$ differ since the hackers generally gain reputation from the attack and information sharing differently.

We finally assume that hacker $k$ values firm $Q$'s asset as $V_k$, and that hacker $k$'s attack on firm $Q$ has unit cost $C_k$, $Q = A,B$, $k = i,j$. The two hackers' utilities are

$$\begin{aligned}
U_i &= g_{Ai}V_i + g_{Bi}V_i + \Theta_i + \Psi_i - C_iT_{Ai} - C_iT_{Bi} \\
&= \tfrac{T_{Ai}+\alpha T_{Bi}}{t_{Ai}+T_{Ai}+\alpha(t_{Bi}+T_{Bi})}V_i + \tfrac{T_{Bi}+\alpha T_{Ai}}{t_{Bi}+T_{Bi}+\alpha(t_{Ai}+T_{Ai})}V_i \\
&\quad +\Lambda_i\Gamma_i(T_{Ai}+T_{Bi})S_i\Gamma_j(T_{Aj}+T_{Bj})S_j + \Omega_i(T_{Ai}+T_{Bi})S_i - C_iT_{Ai} - C_iT_{Bi} \\
U_j &= q_{Aj}V_j + q_{Bj}V_j + \Theta_j + \Psi_j - C_jT_{Aj} - C_jT_{Bj} \\
&= \tfrac{T_{Aj}+\alpha T_{Bj}+\Gamma_i(T_{Ai}+T_{Bi})S_i}{t_{Aj}+\gamma s_B+T_{Aj}+\alpha(t_{Bj}+\gamma s_A+T_{Bj})+\Gamma_i(T_{Ai}+T_{Bi})S_i}V_j \\
&\quad + \tfrac{T_{Bj}+\alpha T_{Aj}+\Gamma_i(T_{Ai}+T_{Bi})S_i}{t_{Bj}+\gamma s_A+T_{Bj}+\alpha(t_{Aj}+\gamma s_B+T_{Aj})+\Gamma_i(T_{Ai}+T_{Bi})S_i}V_j \\
&\quad +\Lambda_j\Gamma_i(T_{Ai}+T_{Bi})S_i\Gamma_j(T_{Aj}+T_{Bj})S_j + \Omega_j(T_{Aj}+T_{Bj})S_j - C_jT_{Aj} - C_jT_{Bj}
\end{aligned} \tag{9}$$

In (9) each hacker has six terms in its utility. The first four correspond to each hacker's three motivations, and the two negative terms are the attack expenditures.

As in Gal-Or and Ghose [19] and Hausken [21], we assign leakage costs to the firms of information sharing. The transfer channels and usually broad domain within which the information transferred between firms exists give hackers larger room for maneuver. Players within or associated with the two firms may choose to leak shared information to criminals and hackers, or to agents with a conflict of interest with one or both firms. We consider the functional forms

$$\xi_A = \phi_1 s_A^2 - \phi_2 s_B^2 - \phi_3 s_A s_B, \quad \xi_B = \phi_1 s_B^2 - \phi_2 s_A^2 - \phi_3 s_A s_B, \quad \phi_1 \geq \phi_2 + \phi_3 \tag{10}$$

where $\phi_1 \geq 0$ is the inefficiency (unit cost) of own leakage, $\phi_2 \geq 0$ as the efficiency (unit benefit) of the other firm's leakage (since the first firm benefits from it), and $\phi_3 \geq 0$ as the efficiency (unit benefit) of joint leakage.

Firm $Q$'s valuation of its asset as defended against hacker $k$ is $v_k$, and firm $Q$'s unit cost of defense against hacker $k$ is $c_k$, $Q = A,B$, $k = i,j$. Thus, the two firms' utilities are

$$\begin{aligned}
u_A &= v_i - g_{Ai}v_i - c_it_{Ai} + v_j - q_{Aj}v_j - c_jt_{Aj} - \xi_A \\
&= v_i - \tfrac{T_{Ai}+\alpha T_{Bi}}{t_{Ai}+T_{Ai}+\alpha(t_{Bi}+T_{Bi})}v_i - c_it_{Ai} + v_j \\
&\quad - \tfrac{T_{Aj}+\alpha T_{Bj}+\Gamma_i(T_{Ai}+T_{Bi})S_i}{t_{Aj}+\gamma s_B+T_{Aj}+\alpha(t_{Bj}+\gamma s_A+T_{Bj})+\Gamma_i(T_{Ai}+T_{Bi})S_i}v_j - c_jt_{Aj} - (\phi_1 s_A^2 - \phi_2 s_B^2 - \phi_3 s_A s_B) \\
u_B &= v_i - g_{Bi}v_i - c_it_{Bi} + v_j - q_{Bj}v_j - c_jt_{Bj} - \xi_B \\
&= v_i - \tfrac{T_{Bi}+\alpha T_{Ai}}{t_{Bi}+T_{Bi}+\alpha(t_{Ai}+T_{Ai})}v_i - c_it_{Bi} + v_j \\
&\quad - \tfrac{T_{Bj}+\alpha T_{Aj}+\Gamma_i(T_{Ai}+T_{Bi})S_i}{t_{Bj}+\gamma s_A+T_{Bj}+\alpha(t_{Aj}+\gamma s_B+T_{Aj})+\Gamma_i(T_{Ai}+T_{Bi})S_i}v_j - c_jt_{Bj} - (\phi_1 s_B^2 - \phi_2 s_A^2 - \phi_3 s_A s_B)
\end{aligned} \tag{11}$$

For each firm the two ratio terms correspond to defense against the hackers' first motivation of financial gain. These two negative ratio terms are subtracted from the firm's asset values. Two of the negative terms are the firm's defense expenditures. The final negative term is leakage costs of information sharing.

## 3. Analysis

This section provides the interior solution in Section 3.1, the corner solution when hacker $i$ is deterred in Section 3.2, the corner solution when hacker $j$ is deterred in Section 3.3, the corner solution

when hacker $i$ shares a maximum amount of information in Section 3.4, and some special cases of advantage for hackers $i$ and j in Section 3.5. Appendix A.1 solves the game with backward induction.

### *3.1. Interior Solution*

This subsection provides in Assumption 1 four assumptions for an interior solution, where all four players exert efforts and share information. Thereafter we present the related propositions. For an interior solution, where all four players exert efforts and share information, we assume the following:

$$\begin{aligned}\text{Assumption 1. (a) } \frac{2c_i}{v_i} > \frac{C_i}{V_i}; \text{(b)} \frac{2c_j}{v_j} > \frac{C_j}{V_j} + \frac{2\Omega_i c_j^2/v_j^2}{\Lambda_i\Gamma_i\Gamma_j S_j} - \frac{\Omega_j S_j}{V_j};\\ \text{(c) } \frac{2c_j}{v_j} > \sqrt{\frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}} \text{ and } \alpha \geq -1;\\ \text{(d) } \frac{\left(\frac{C_j}{V_j} - \frac{\Omega_j S_j}{V_j}\right)\left(\frac{8c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right) - 2\Lambda_j(1+\alpha)\frac{c_j}{v_j}\left(\frac{\Gamma_j S_j}{V_j} + \frac{\Omega_i c_j/v_j}{\Lambda_i\Gamma_i V_j}\right)}{8\left(4c_j^2/v_j^2 - (1+\alpha)\Lambda_j\Gamma_j S_j/V_j\right)c_j^2/v_j^2} > \gamma s\end{aligned} \tag{12}$$

Assumption 1a ensures that hacker $i$ is not deterred by the firms' defense in period 1, which would give a corner solution analyzed in Section 3.2. If hacker $i$'s unit attack cost $C_i$ relative to its valuation $V_i$ is less than twice that of the firms' unit defense cost $c_i$ relative to their valuation $v_i$, the firms' moderate defense $t_i$ is not perceived as overwhelming, and hacker $i$ attacks. Conversely, if hacker $i$ suffers high unit attack cost $C_i$ or has low valuation $V_i$, hacker $i$ is deterred by the overwhelming defense $t_i$ and does not attack, i.e., $T_i = 0$.

Assumption 1b ensures that hacker $j$ attacks with $T_j > 0$ in period 4, and is not deterred by the firms' defense $t_j$ in period 3, which would give a corner solution analyzed in Section 3.3. When $\Omega_i = \Omega_j = 0$, if the firms' unit defense cost $c_j$ relative to their valuation $v_j$ is larger than half that of hacker $j$'s unit attack cost $C_j$ relative to its valuation $V_j$, the firms' moderate defense $t_j$ is not perceived as overwhelming and deterrent, and hacker $j$ attacks. When $\Omega_i = 0$ and $\Omega_j > 0$, motivated by own reputation gain, hacker $j$ attacks even when $2c_j/v_j$ is lower. When $\Omega_i > 0$ and $\Omega_j = 0$, deterred by hacker $i$'s reputation gain, hacker $j$ requires higher $2c_j/v_j$ (i.e., more disadvantaged firms) in order to attack. Finally, if $\Omega_i = \Omega_j = 0$ and the firms enjoy low unit defense cost $c_j$ or have high valuation $v_j$, hacker $j$ is deterred by the overwhelming defense $t_j$ and does not attack, i.e., $T_i = 0$.

Assumption 1c is needed to ensure positive and finite information sharing $0 < S_i < \infty$ for hacker $i$, which also occurs when the firms' unit defense cost $c_j$ relative to their valuation $v_j$ is high, so that the firms can afford only moderate defense. Thus, hacker $i$ does not share information when sharing is not worthwhile assessed against the strength of the firms' defense. High interdependence $\alpha$ between the firms may prevent hacker $i$ from sharing information. More specifically, the size of $c_j/v_j$ to ensure $S_i > 0$ must be large if the interdependence $\alpha$ between the firms is large, hacker $j$ shares much information ($S_j$ is high), if hacker $j$ utilizes joint sharing ($\Lambda_j$ is high), if hacker $j$'s sharing effectiveness $\Gamma_j$ is high, and if hacker $j$'s valuation $V_j$ is low. This means that both hackers benefit from information sharing, and information sharing between the hackers is ensured when the firms are disadvantaged with a large $c_j/v_j$ so that the defense is not too large. $\alpha \geq -1$ is common in practice and prevents negative values under the root. See the corner solution in Section 3.4 when Assumption 1c is satisfied with a small margin.

Assumption 1d follows from $C_j > (\Omega_j + 2\Lambda_j\Gamma_i T_i S_i \Gamma_j)S_j$, which is needed in hacker $j$'s utility in (6) so that hacker $j$ experiences a cost of attacking, and more generally ensures that hacker $j$'s attack $T_j$ is positive. If hacker $j$'s unit cost $C_j$ is too low, hacker $j$ benefits so much from information sharing, expressed with $(\Omega_j + 2\Lambda_j\Gamma_i T_i S_i \Gamma_j)S_j$, that attack effort $T_j$ determined by $C_j$ is not needed, and would decrease hacker $j$'s utility because of the high expenditure $C_j T_j$. Assumption 1d is less likely satisfied

when $\gamma s$ is large, i.e., when the firms share much information and the sharing effectiveness $\gamma$ is large which prevents hacker j from attacking.

With these four assumptions, we present 10 propositions. First come 1. the interior solution and 2. mutual reaction between each firm's defense $t_i$ and hacker $i$'s attack $T_i$ in the first attack. Thereafter follow six propositions for the six independent variables in Table 1, i.e., 3. hacker $i$'s information sharing $S_i$, 4. hacker $i$'s effort $T_i$, 5. the firms' defense $t_i$ against hacker $i$, 6. the firms' defense $t_j$ against hacker $j$, 8. the firms' information sharing $s$, and 9. hacker $j$'s attack effort $T_j$. We supplement with 7. the firms' aggregate defense $t_j^{agg}$ and 10. hacker $j$'s aggregate attack $T_j^{agg}$.

**Proposition 1.** *When Assumption 1 is satisfied and $0 \leq S_i \leq 2\Gamma_i T_i$, the players' efforts and information sharing are*

$$\begin{aligned}
t_i &= \frac{C_i/V_i}{4c_i^2/v_i^2}, \quad T_i = \frac{1}{4c_i^2/v_i^2}\left(\frac{2c_i}{v_i} - \frac{C_i}{V_i}\right), \quad S_i = \frac{(1+\alpha)\left(\frac{2c_j}{v_j} - \frac{C_j}{V_j} + \frac{2\Omega_i c_j^2/v_j^2}{\Lambda_i\Gamma_i\Gamma_j S_j} + \frac{\Omega_j S_j}{V_j}\right)}{\frac{\Gamma_i}{c_i^2/v_i^2}\left(\frac{2c_i}{v_i} - \frac{C_i}{V_i}\right)\left(\frac{4c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right)}, \\
t_j &= \frac{\left(\frac{C_j}{V_j} - \frac{\Omega_j S_j}{V_j}\right)\left(\frac{8c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right) - 2\Lambda_j(1+\alpha)\frac{c_j}{v_j}\left(\frac{\Gamma_j S_j}{V_j} + \frac{\Omega_i c_j/v_j}{\Lambda_i\Gamma_i V_j}\right)}{8\left(4c_j^2/v_j^2 - (1+\alpha)\Lambda_j\Gamma_j S_j/V_j\right)c_j^2/v_j^2} - \gamma s, \\
s &= \frac{\gamma c_j}{2\phi_1 - \phi_3}, \quad T_j = \frac{2c_j/v_j - C_j/V_j + \Omega_j S_j/V_j}{8c_j^2/v_j^2} - \frac{\Omega_i}{4\Lambda_i\Gamma_i\Gamma_j S_j}
\end{aligned} \tag{13}$$

and the utilities follow from inserting into (9) and (11).

**Proof.** Appendix A.1. □

**Proposition 2.** *Mutual reaction between each firm and hacker i in the first attack: For the first attack in isolation, hacker i's attack $T_i$ is inverse U-shaped in the defense $t_i$, and each firm's defense $t_i$ is inverse U-shaped in the attack $T_i$.*

**Proof.** Appendix A.2. □

Proposition 2 considers the non-equilibrium values of $t_i$ and $T_i$ relative to each other, in contrast to the unique equilibrium values of $t_i$ and $T_i$ in Proposition 1. Proposition 2 states that hacker $i$'s attack and each firm's defense are inverse U-shaped in each other. The amount of information uncovered by hacker $i$ is proportional to hacker $i$'s attack. Consequently, if hacker $i$ is disadvantaged relative to each firm, $C_i/V_i > c_i/v_i$, so that its attack $T_i$ is small compared with each firm's defense $t_i$, then little information is uncovered by hacker $i$ through the attack. This is reflected in hacker $i$'s sharing effectiveness $\Gamma_i(T_{Ai} + T_{Bi})$, which is $2\Gamma_i T_i$ in equilibrium, which is low when $T_i$ is low, and little information can be transferred to hacker $j$. As $T_i$ increases, more information is uncovered by hacker $i$ through the attack. If hacker $i$ and the firm are equally matched, $C_i/V_i \approx c_i/v_i$, both $T_i$ and $t_i$ are large, and hacker $i$ has large sharing effectiveness. If hacker $i$ is advantaged relative to the firm, $C_i/V_i < c_i/v_i$, so that its attack $T_i$ is large compared with each firm's defense $t_i$, then much information is uncovered by hacker $i$ through the attack.

**Proposition 3.** *Assume that Assumption 1 is satisfied and $0 \leq S_i \leq 2\Gamma_i T_i$. $\partial S_i/\partial\alpha > 0$, $\partial S_i/\partial(C_i/V_i) > 0$, $\partial S_i/\partial(C_j/V_j) < 0$, $\partial S_i/\partial\Lambda_i < 0$, $\partial S_i/\partial\Lambda_j > 0$, $\partial S_i/\partial\Gamma_i < 0$, $\partial S_i/\partial\Omega_i > 0$, $\partial S_i/\partial\Omega_j > 0$. When $C_i/V_i > c_i/v_i$, $\partial S_i/\partial(c_i/v_i) < 0$. When $C_i/V_i < c_i/v_i$, $\partial S_i/\partial(c_i/v_i) > 0$. When additionally $\Omega_i = 0$, $\partial S_i/\partial\Gamma_j > 0$, $\partial S_i/\partial S_j > 0$.*

**Proof.** $\frac{\partial S_i}{\partial\alpha} = \frac{S_i}{(1+\alpha)}\frac{4c_j^2}{v_j^2}/\left(\frac{4c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right)$. The other inequalities follow straightforwardly from differentiating $S_i$ in (13). □

Proposition 3 states, first, that hackers' information sharing $S_i$ increases in the interdependence $\alpha$ between the firms. When firms are interdependent, the hackers' attacks propagate more easily to the other firm not under direct attack. This causes larger aggregate attacks that enable hackers to compile more information and share more information with each other. Second, information sharing $S_i$ increases in hacker $i$'s ratio $C_i/V_i$ of unit cost to valuation. This is a substitution effect. When exerting effort $T_i$ becomes too costly relative to the valuation, hacker $i$ substitutes to information sharing instead, limited by $0 \leq S_i \leq 2\Gamma_i T_i$ since a small attack $T_i$ provides hacker $i$ with limited information. Third, when the firms are disadvantaged quantified as $C_i/V_i < c_i/v_i$, conversely, $S_i$ decreases in the firms' ratio $c_i/v_i$ of unit cost to valuation. This is also a substitution effect operating the other way since increasing $C_i/V_i$ and decreasing $c_i/v_i$ have the qualitatively same impact on $T_i$. However, when the firms are advantaged quantified as $C_i/V_i > c_i/v_i$, $S_i$ increases in $c_i/v_i$. Fourth, hacker $i$'s information sharing increases in both the hackers' reputation gain parameters $\Omega_i$ and $\Omega_j$, which motivate information sharing.

Fifth, and most interestingly, $S_i$ decreases in hacker $j$'s ratio $C_j/V_j$ of unit cost to valuation. This means that when hacker $j$ is disadvantaged with a large ratio $C_j/V_j$ of unit cost to valuation, and thus exerts low effort $T_j$, then hacker $i$ shares less information. Hacker $j$ would hope for the opposite, that hacker $i$ would compensate hacker $j$'s disadvantage of a high $C_j/V_j$, by sharing more information, but that is not the case. Instead, hacker $i$ uses hacker $j$'s high $C_j/V_j$ against hacker $j$, so that when hacker $j$ exerts lower effort $T_j$, then hacker $j$ will also be disadvantaged by receiving less information $S_i$. This follows since hacker $i$ does not expect hacker $j$ to use the shared information $S_i$ cost efficiently in a manner that benefits hacker $i$. This can also be interpreted so that hacker $i$ does not trust hacker $j$, or does not think hacker $j$ deserves to receive more information.

Except for this fifth point, when $\Omega_i = 0$ hackers $i$ and $j$ focus on their joint interests and support each other when sharing information. Thus, $S_i$ increases in hacker $j$'s sharing effectiveness $\Gamma_j$, decreases in hacker $i$'s sharing effectiveness $\Gamma_i$, increases in hacker $j$'s utilization $\Lambda_j$ of joint sharing, and increases in hacker $j$'s sharing $S_j$. Summing up, when $\Omega_i = 0$, the two hackers reinforce information sharing with each other, except that hacker $i$ shares less with hacker $j$ when hacker $j$ is unable to exert high attack effort $T_j$. When $\Omega_i > 0$, the dependence of $S_i$ on hacker $j$'s sharing effectiveness $\Gamma_j$ and hacker $j$'s sharing $S_j$ is mixed and has to be assessed in each individual case as the hackers search for individual reputation gain.

**Proposition 4.** *When Assumption 1 is satisfied and $0 \leq S_i \leq 2\Gamma_i T_i$, hacker i's effort $T_i$ and information sharing $S_i$ are strategic substitutes as impacted by $C_i/V_i$ and $c_i/v_i$.*

**Proof.** Follows from (13), where $\partial T_i/\partial(C_i/V_i) < 0$ and $\partial S_i/\partial(C_i/V_i) > 0$. When $C_i/V_i > c_i/v_i$, then $\partial T_i/\partial(c_i/v_i) > 0$ and $\partial S_i/\partial(c_i/v_i) < 0$. When $C_i/V_i < c_i/v_i$, then $\partial T_i/\partial(c_i/v_i) < 0$ and $\partial S_i/\partial(c_i/v_i) > 0$. □

Proposition 4 implies that hacker $i$ adjusts its attack effort $T_i$ and information sharing $S_i$ in opposite directions dependent on changes in $C_i/V_i$ and $c_i/v_i$ and limited by $0 \leq S_i \leq 2\Gamma_i T_i$. That is, if hacker $i$'s own unit cost to valuation ratio $C_i/V_i$ increases relative to the firms' unit cost to valuation ratio $c_i/v_i$, hacker $i$ chooses lower $T_i$ and higher $S_i$, and conversely if $C_i/V_i$ decreases relative to $c_i/v_i$. Hacker $i$'s attack $T_i$ increases in $c_i/v_i$ when hacker $i$ is disadvantaged ($C_i/V_i > c_i/v_i$), and decreases in $c_i/v_i$ when hacker $i$ is advantaged.

**Proposition 5.** *When Assumption 1 is satisfied and $0 \leq S_i \leq 2\Gamma_i T_i$, $\partial t_i/\partial(c_i/v_i) < 0$, $\partial t_i/\partial(C_i/V_i) > 0$.*

**Proof.** Follows from differentiating $t_i$ in (13). □

Proposition 5 states that the firms' defense $t_i$ against hacker $i$ intuitively decreases in their own ratio $c_i/v_i$ of unit cost to valuation, since defense becomes more costly (high $c_i$) and/or less desirable

(low $v_i$). For the opposite reason, and thus also intuitively, the firms' defense $t_i$ against hacker $i$ increases in hacker $i$'s ratio $C_i/V_i$ of unit cost to valuation, which comparatively corresponds to increasing $c_i/v_i$.

**Proposition 6.** *When Assumption 1 is satisfied and* $0 \leq S_i \leq 2\Gamma_i T_i$, $\partial t_j/\partial\alpha < 0$, $\partial t_j/\partial\gamma < 0$, $\partial t_j/\partial(C_j/V_j) > 0$, $\partial t_j/\partial\Gamma_j < 0$, $\partial t_j/\partial\Lambda_j < 0$, $\partial t_j/\partial\Omega_i < 0$, $\partial t_j/\partial\Omega_j < 0$. *When additionally* $\Omega_j = 0$, $\partial t_j/\partial S_j < 0$.

**Proof.** Follows from differentiating $t_j$ in (13). □

Proposition 6 states that the firms' defense $t_j$ decreases in their interdependence $\alpha$. One possible explanation is that when attacks propagate more easily between firms, each firm may prefer the other firm to incur the defense burden. Mathematically for $t_j$, in (13) terms with $\alpha$ are subtracted in the numerator, and in (A5) $T_iS_i$ which increases in $\alpha$ is subtracted in the numerator, causing lower $t_j$. Further, the firms' defense $t_j$ against hacker $j$ increases in $C_j/V_j$, regardless of whether the firms are disadvantaged or not, and decreases in hacker $j$'s sharing effectiveness $\Gamma_j$ and utilization $\Lambda_j$ of joint sharing. The defense $t_j$ decreases in information sharing $S_j$ when $\Omega_j = 0$. Furthermore, the firms defend less as the reputation gain parameters $\Omega_i$ and $\Omega_j$ increase, which may be controversial, as discussed in Section 5.

**Proposition 7.** *When Assumption 1 is satisfied and* $0 \leq S_i \leq 2\Gamma_i T_i$, *except for* $\partial t_j^{agg}/\partial\alpha$ *which can be negative or positive, the firms' aggregate defense* $t_j^{agg} = (1+\alpha)(t_j + \gamma s)$ *has equivalent derivatives as in Proposition 6 for* $t_j$, *i.e.,* $\partial t_j^{agg}/\partial z = \partial t_j/\partial z$, *where* $z = C_j/V_j$, $z = \Gamma_j$, $z = \Lambda_j$, $z = \Omega_i$, $z = \Omega_j$ *and* $z = S_j < 0$.

**Proof.** Follows from (13) and Proposition 6 where $\partial t_j/\partial\alpha < 0$. □

Proposition 7 illustrates how the firms strike a balance or tradeoff between defense $t_j$ and information sharing $\gamma s$, and earns a reinforced defense through $\alpha$. If defense becomes costly or undesirable for some reason, the firms substitute to information sharing, and vice versa.

**Proposition 8.** *When Assumption 1 is satisfied and* $0 \leq S_i \leq 2\Gamma_i T_i$, $\partial s/\partial\gamma > 0$, $\partial s/\partial c_j > 0$, $\partial s/\partial\phi_1 < 0$, $\partial s/\partial\phi_3 > 0$.

**Proof.** Follows from differentiating $s$ in (13). $2\phi_1 > \phi_3$ since $\phi_1 \geq \phi_2 + \phi_3$. □

Proposition 8 states that the firms' information sharing $s$ increases in their sharing effectiveness $\gamma$, since sharing then becomes more useful for the firms, and increases in their unit defense cost $c_j$ against hacker $j$, since defense then becomes more costly making it beneficial to substitute into information sharing instead. Further, $s$ decreases in each firm's unit cost $\phi_1$ of own information leakage, and increases in the unit benefit $\phi_3$ of joint leakage.

Comparing large sharing effectiveness $\gamma > 0$ with zero sharing effectiveness $\gamma = 0$ enables comparing between the firms' strategies when they share information vis-à-vis when they do not. The most useful insight from the subtraction of $\gamma s$ in the expression for $t_j$ in (13) is that large sharing effectiveness enables firms to rely on information sharing as directly useful in defending against hackers, which in turn enables firms to cut back on their security defense $t_j$.

**Proposition 9.** *When Assumption 1 is satisfied and* $0 \leq S_i \leq 2\Gamma_i T_i$, $\partial T_j/\partial\alpha = 0$. $\partial T_j/\partial(C_j/V_j) < 0$, $\partial T_j/\partial\Omega_i < 0$, $\partial T_j/\partial\Omega_j > 0$, $\partial T_j/\partial S_j > 0$, $\partial T_j/\partial\Gamma_i > 0$, $\partial T_j/\partial\Gamma_j > 0$, $\partial T_j/\partial\Lambda_i > 0$. *When additionally* $\frac{c_j}{v_j} < \frac{C_j}{V_j} - \frac{\Omega_j S_j}{V_j}$, $\partial T_j/\partial(c_j/v_j) > 0$.

**Proof.** Follows from differentiating $T_j$ in (13). □

Proposition 9 states that hacker $j$'s attack effort $T_j$ decreases in $C_j/V_j$, increases in its reputation gain parameter $\Omega_j$, decreases in hacker $i$'s reputation gain parameter $\Omega_i$, and increases in its information sharing $S_j$, hacker $i$'s utilization $\Lambda_i$ of joint sharing, and both sharing effectiveness parameters $\Gamma_i$ and $\Gamma_j$. Further, hacker $j$'s attack effort $T_j$ increases in the firms' ratio $c_j/v_j$ when the firms are advantaged with a low $c_j/v_j$. In this event hacker $j$ is disadvantaged and takes advantage of increasing $c_j/v_j$ by attacking more. Conversely, high $c_j/v_j$ means that hacker $j$ is advantaged and a large attack is not needed against disadvantaged firms.

**Proposition 10.** *When Assumption 1 is satisfied and $0 \leq S_i \leq 2\Gamma_i T_i$, hacker $j$'s aggregate attack $T_j^{agg} = (1+\alpha)T_j + 2\Gamma_i T_i S_i$ increases in the firms' interdependence $\alpha$, i.e., $\partial T_j^{agg}/\partial\alpha > 0$.*

**Proof.** Follows from (13) and $\partial S_i/\partial\alpha > 0$ in Proposition 3. □

Comparing Propositions 10 and 7 suggests that hacker $j$'s aggregate attack $T_j^{agg}$, directed toward each firm and channeled through $\alpha$ to the other firm, increases in the firms' interdependence $\alpha$, whereas the firms' aggregate defense $t_j^{agg}$, furnished by own defense $t_j$ and reinforced by information sharing from the other firm, either decreases or increases in the firms' interdependence $\alpha$. Interdependence between firms is a potential liability firms should be conscious about. It causes attacks against firms to propagate to other firms, and may possibly cause firms to defend less.

### *3.2. Corner Solution When Hacker i Is Deterred*

**Proposition 11.** *When Assumption 1a is not satisfied and $0 \leq S_i \leq 2\Gamma_i T_i$, the firms choose $t_i = V_i/C_i + \varepsilon$, where $\varepsilon$ is arbitrarily small but positive, causing $T_i = S_i = 0$.*

**Proof.** Appendix A.3. □

That Assumption 1a is not satisfied means that hacker $i$ is disadvantaged, which means that hacker $i$'s unit attack cost $C_i$ relative to its valuation $V_i$ is larger than twice that of the firms' unit defense cost $c_i$ relative to its valuation $v_i$. With such a disadvantaged hacker $i$, the firms choose their defense $t_j$ slightly above that level which makes hacker $i$ indifferent between attacking and not attacking. This deters hacker $i$ ($T_i = S_i = 0$). The game between the firms and hacker $j$ in periods 3 and 4 is thus without information sharing, with $t_j + \gamma s$ and $T_j$ as $t_i$ and $T_i$ in (13).

### *3.3. Corner Solution When Hacker j Is Deterred*

**Proposition 12.** When Assumption 1b is not satisfied and $0 \leq S_i \leq 2\Gamma_i T_i$, the firm chooses $t_j = V_j/C_j + \gamma s + \varepsilon$, where $\varepsilon$is arbitrarily small but positive, causing $T_j = S_i = S_j = 0$.

**Proof.** Appendix A.4. □

That Assumption 1b is not satisfied means that hacker $j$ is disadvantaged, which when $\Omega_i = \Omega_j = 0$ means that hacker $j$'s $C_j/V_j$ is larger than twice that of the firms' $c_j/v_j$. The firm then deters hacker $j$ ($T_j = S_j = 0$). Hacker $j$'s unwillingness to attack in period 4 has ripple effects to period 1. Hacker $i$ realizes that nothing is gained by sharing information with hacker $j$. Hacker $i$ thus chooses not to share information, $S_i = 0$. The game between the firms and hacker $i$ in periods 1 and 2 is thus without information sharing between the two hackers, with $t_i$ and $T_i$ as in (13).

### *3.4. Corner Solution When Hacker i Shares a Maximum Amount of Information*

**Proposition 13.** *When Assumption 1b is satisfied and* $0 \leq S_i \leq 2\Gamma_i T_i$*, and Assumption 1c is satisfied with a small margin, hacker i shares a maximum amount of information with hacker j, i.e.,* $S_i = 2\Gamma_i T_i$.

**Proof.** When $\frac{2c_j}{v_j} = \sqrt{\frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}} + \varepsilon > \frac{C_j}{V_j} - \frac{2\Omega_i c_j^2/v_j^2}{\Lambda_i\Gamma_i\Gamma_j S_j} - \frac{\Omega_j S_j}{V_j}$, the interior solution for $S_i$ in (13) applies with positive numerator and small positive denominator. As $\varepsilon$ decreases towards zero, the denominator decreases towards zero causing $S_i$ to increase towards infinity. As $\varepsilon$ becomes negative, the interior solution for $S_i$ in (13) no longer applies and hacker $i$ shares a maximum amount of information with hacker $j$, i.e., $S_i = 2\Gamma_i T_i$. □

Proposition 13 assumes that the firms' ratio $c_j/v_j$ of unit defense cost relative to their valuation is intermediate. That is, $c_j/v_j$ is not so low that hacker $j$ is deterred (Proposition 12), and not so high that the interior solution applies. Instead, driven by hacker $j$'s large information sharing $S_j$ relative to its valuation $V_j$, hacker $j$'s large sharing effectiveness $\Gamma_i$, and hacker $j$'s large utilization $\Lambda_j$ of joint sharing, both hackers benefit substantially from hacker $i$'s sharing and hacker $i$ thus shares information maximally. In this solution $T_i$ follows from solving $\partial U_i/\partial T_i = 0$ in (A8) when $S_i = S_{imax}$ (not shown because it is a voluminous solution of a third order equation in $T_i$), $t_j$ follows from (A5), $T_j$ follows from (A1), and $t_i$ follows from using (A3) to differentiate firm $A$'s period 1 utility with respect to $t_{Ai}$ and setting $t_i = t_{Bi} = t_{Ai}$.

### *3.5. Some Special Cases of Advantage for Hackers i and j*

Assume $\Omega_i = \Omega_j = 0$, $\Lambda_i = \Lambda_j = c_i = v_i = c_j = v_j = V_i = V_j = \alpha = \gamma = \phi_2 = \phi_3 = 1$, $\phi_1 = 3$, $\Gamma_i = \Gamma_j = 4$ and $S_j = 0.25$ which gives $S_i = S_j$ when $C_i = C_j$, see row 2 in Table 2.

**Table 2.** Values of variables for various parameter values.

| | $t_i$ | $T_i$ | $S_i$ | $t_j$ | $s$ | $T_j$ | $U_i$ | $U_j$ | $U_i + U_j$ | $u$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $C_i = C_j = 1$ | 0.25 | 0.25 | 0.25 | 0.208 | 0.2 | 0.125 | 0.625 | 0.832 | 1.457 | 0.523 |
| $C_i = 1, C_j = 3/2$ | 0.25 | 0.25 | 0.125 | 0.354 | 0.2 | 0.0625 | 0.531 | 0.349 | 0.881 | 0.603 |
| $C_i = 3/2, C_j = 1$ | 0.375 | 0.125 | 0.5 | 0.208 | 0.2 | 0.125 | 0.25 | 0.832 | 1.082 | 0.648 |

Row 3 assumes that hacker $i$ is 2/3 more advantaged than hacker $j$ in terms of unit cost divided by valuation, i.e., $C_i = 1$ and $C_j = 3/2$. The advantaged hacker $i$ shares less, $S_i = 0.125$, causing hacker $j$ to attack less. Both hackers earn lower expected utilities and the firms earn higher expected utility. Conversely, row 4 assumes that hacker $j$ is 2/3 more advantaged, i.e., $C_i = 3/2$ and $C_j = 1$. Then the disadvantaged hacker $i$ shares more, $S_i = 0.5$, causing higher expected utility to the advantaged hacker $j$. Comparing the bottom two rows in Table 2, the hackers' collective expected utility $U_i + U_j$ is largest when they benefit from more substantial mutual information sharing. Hence with these strong assumptions hacker $j$ should be the advantaged hacker from the two hackers' collective viewpoint of view. Intuitively, the firms prefer the hackers to be disadvantaged with large unit costs $C_i$ or $C_j$.

## 4. Policy and Managerial Implications

First, our analysis reveals that the first hacker shares less information when the second hacker can be expected to attack inefficiently. Hence if hackers believe that their attacks may not be followed up by subsequent attacks, they may share less information.

Second, unit costs of effort and asset valuations are influential in the analysis. Firms cannot do too much about their own asset valuations since their utility flows from the valuations, but they can acquire defense technology to decrease their own unit effort costs. Firms can further seek to design their defenses so that the available attack technology incurs a high unit attack cost. Large firms may

have the expertise to lobby lawmakers to hamper the availability or forbid certain attack technologies, e.g., spyware. Firms may also seek to decrease the hackers' valuations of their assets so that the assets becomes less usable or not usable elsewhere, e.g., that the assets get destroyed upon procurement or that law enforcement gets enabled to interfere with hackers' successful exploitation of hacked information assets.

Third, especially large firms may possess the ability to impact public and hacker opinion e.g., so that sharing information acquired by hacking causes lower or negative reputation. For example, some communities have successfully handled graffiti tagging by shaming perpetrators into other activities, which may be tried for hacking.

Fourth, that the first hacker's reputation gain deters the second hacker's attack causes a dilemma for the firms. Firms prefer hackers not earn a reputation gain. However, if one hacker's reputation can deter other hackers, that may be preferable for the firms if they have found a way to handle the reputed hacker.

Fifth, one may attempt to decrease the hackers' sharing effectiveness parameters and utilization of joint sharing. To the extent hackers meet online, these online sites can be attempted surveyed or hacked by firms and law enforcement making it more difficult for hackers to share information without being noticed, or planting incorrect information about the firms making it costly for hackers to distinguish between correct and incorrect information. To the extent hackers meet offline, e.g., Internet cafes or various gathering places, these places can be placed under surveillance to prevent hackers from feeling safe from supervision.

Sixth, that hackers' information sharing increases in the interdependence between firms is a vulnerability firms should be conscious about.

Seventh, the corner solution where the advantaged firm deters a disadvantaged hacker confirms for the firms that their defense strategy work, and may continue to work if the first hacker does not share information with the second hacker.

Eighth, the corner solution where the first hacker shares information maximally may be handled by the firms by attempting to hinder hackers from sharing information.

Ninth, if a hacker's attack can be reduced, information sharing increases since attack and information sharing are strategic substitutes. Understanding this relationship may enable combating one or the other.

Tenth, our analysis suggests the need to heighten 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 firms' vulnerabilities.

## 5. Limitations and Future Research

One challenge for a complex model such as the one in this paper is that the requirements for a reality check of the results are higher. Although many of the results are plausible, some may be interpreted as indicative, and others may need further scrutiny, especially if they sound counterintuitive.

Let us interpret Proposition 3 about hacker $i$'s information sharing $S_i$, Proposition 6 about the firms' defense $t_j$ against hacker $j$, and Proposition 9 about hacker $j$'s attack $T_j$. The three expressions for $S_i$, $t_j$, and $T_j$ are the most complicated in (13), with many functional dependencies. Proposition 3 seems largely intuitive. For example, as hacker $i$'s ratio $C_i/V_i$ of unit cost to valuation increases, hacker $i$ can be expected to cut back on hacking and substitute into alternatives, which in the current model means information sharing. Propositions 6 and 9 suggest many ways in which the firms' defense $t_j$ and hacker $j$'s attack $T_j$ may increase or decrease. These results may need further scrutiny since increases or decreases in defense or attack may be due to how two opposing players are advantaged or disadvantaged relative to each other. In this regard, Proposition 2 states that hacker $i$'s attack and each firm's defense are inverse U-shaped in each other. The inverse $U$ shape follows since a player may

exert high effort when opponents are similarly matched expressed as similar unit effort costs relative to valuation, and may exert low effort when opponents are differently matched. Being differently matched means either advantaged or disadvantaged. When advantaged, the player exerts low effort since the opponent is merely a nuisance not worth paying too much attention to. Thus, a cost benefit analysis suggests low effort. When disadvantaged, the player exerts low effort since the opponent's effort is so overwhelmingly large that the player's effort does not make much difference. Thus, a cost benefit analysis again suggests low effort. It seems theoretically possible that the complex model captures only one side of the story for the various findings in Propositions 6 and 9, and that future research should check how firms defend against advantaged versus disadvantaged hackers due to firms being advantaged versus disadvantaged. The inverse $U$ shape has also been found in earlier research. For example, Hausken [20,21] finds that information sharing and security investment for two firms are inverse U-shaped in the aggregate attack.

The finding in Proposition 6 that firms defend less as the hackers' reputation gain parameters $\Omega_i$ and $\Omega_j$ increase, may be controversial for the same reason of this inverse $U$ shape. For example, larger $\Omega_j$ causes larger attack $T_j$ for hacker $j$ (Proposition 9). Whether the firms react to the increased attack with larger or smaller defense $t_j$ may depend on weighing benefits and costs related to being advantaged versus disadvantaged.

Logical implications of complex models benefit from a reality test. In the earlier sections we have tried to indicate whether results seem intuitive or plausible. Complex models may uncover hidden, hitherto unknown, and sometimes bizarre relations, and reveal new insight. However, it is also possible that if the results of modeling are counterintuitive or do not match with experience, the model may be insufficiently expressive in various respects. That is, some results may constitute spurious effects and fail a reality test despite flowing from the model. Thus, Levins [50] and Levins and Lewontin [51] suggest, regarding modeling, that "truth is the intersection of multiple lies". This work proceeds in the right direction. Future research should extend game theoretical modeling of complex strategic scenarios between defenders and attackers for cybersecurity. Particular focus may be devoted to reputation gain, interdependence, and being advantaged versus disadvantaged.

We have considered a scenario with two hackers and two firms, which are interpreted to be sufficiently unitary. The literature, e.g., about duopoly versus oligopoly, reveals that much insight is often obtained by considering a limited number of players. Generalizing to $n$ hackers and $N$ firms, to scrutinize the system's scalability, is interesting but analytically challenging. We reasonably assume that many of the qualitative insights of the model carry through to scenarios with more than two hackers. One difference is that firms facing more than two hackers are subject to an opposition that may share information in more sophisticated manners.

The chosen four period defense and attack scenario is one of the simplest that seems possible and realistic. The phenomenon inevitably involves the time dimension where players react to each other through time. Information has to be obtained before it can be shared. Future research, with four or more than four players, should consider alternative defense and attack scenarios, and alternative sequences and manners in which players choose strategies and share in formation.

Other extensions are to different kinds of security investment, and distinguishing between different kinds of information that hackers can share. Information is multidimensional. Security breaches occur at low and high levels of sophistication, and variation is large regarding methods, success of earlier attacks, identities of hackers, and secrets about research, development, future plans, trade, capacities, personnel dispositions, etc. Future research may also consider case studies, assess how the model confirms with empirics, and apply various forms of performance evaluation.

## 6. Conclusions

We consider two firms under cyber attack by two hackers who share information with each other about the firms' vulnerabilities and security breaches. We analyze a game where, first, the firms defend against hacking. Second, the first hacker chooses whether or not to attack, and if it attacks

it chooses how much information to share with a second hacker. Third, the firms defend against subsequent attacks and share information with each other about the first hacker's attack. Fourth, the second hacker attacks the firms and shares information with the first hacker. Each hacker has a triple motivation of financial gain, information exchange as a basis for future superior attacks, and reputation gain. The firms choose optimal defenses, which are costly and consist in investing in information technology security to ensure protection. The firms also choose optimal information sharing and incur leakage costs. 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 firms' vulnerabilities, but synergies of joint sharing also provide incentives to provide information. 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 costly attacks.

We find that the first hacker's attack and each firm's defense are inverse U-shaped in each other. A disadvantaged player refrains from exerting effort due to weakness, and an advantaged player refrains from exerting effort due to strength, causing the largest efforts to be exerted when the hacker and firm are equally matched.

Driven by the substitution effect, the first hacker shares more information and attacks less if its unit cost of attack increases relative to its valuation. When the second hacker is disadvantaged with a high unit cost relative to its valuation, it receives less information from the first hacker, which does not expect the shared information to be used efficiently. As the hackers' reputation gain parameters increase, both hackers share more information.

The second hacker's attack increases in its own reputation gain parameter, and decreases in the first hacker's reputation gain parameter. Although the second hacker is motivated by its own reputation, it is deterred by the first hacker's reputation gain. The second hacker's attack increases in both sharing effectiveness parameters and in the first hacker's utilization of joint sharing, which illustrates the benefits of joint sharing and attack.

As firms' information sharing effectiveness increases, they substitute from defense to information sharing which also increases in the firms' unit defense cost, decreases in each firm's unit cost of own information leakage, and increases in the unit benefit of joint leakage. This shows how firms' information sharing furnishes a solid foundation for firms' aggregate defense and enable them to cut back on their regular defense not based on information sharing.

Increasing interdependence between firms has multiple impacts. It causes hackers' attacks to propagate to the firm not attacked directly, which enables obtaining more information, which enables more information sharing between hackers. Firms need to be conscious about such enhanced aggregate attacks. Firms' defense gets additionally reinforced by information sharing between firms.

We consider three corner solutions. The first two involve deterrence when players move sequentially and the first moving advantaged players, i.e., the firms, choose a strategy that suffices to deter the subsequent disadvantaged player, i.e., the first and the second hacker. First, the firms deter the first hacker when the first hacker is disadvantaged. The deterrence defense is proportional to the first hacker's valuation and inverse proportional to the first hacker's unit attack cost. Second, and with the same logic, the firms deter the second hacker when the second hacker is disadvantaged. Furthermore, when the second hacker is deterred in period 4, the first hacker does not share information in period 2. Third, a corner solution exists where the first hacker shares a maximum amount of information. This occurs when the second hacker shares much information relative to its valuation, has large sharing effectiveness and large utilization of joint sharing, so that both hackers benefit substantially from joint sharing.

**Acknowledgments:** We thank two anonymous reviewers of this journal for useful comments. No sources of funding exist.

**Conflicts of Interest:** The author declares no conflict of interest.

## Appendix A

*Appendix A.1. Interior Solution*

We solve the symmetric game with backward induction starting with period 4. Differentiating hacker $j$'s utility $U_j$ in (9) with respect to $T_{Aj}$, and thereafter setting $T_j = T_{Aj} = T_{Bj}$ and analogously for all variables and parameters, equating with zero and solving, gives

$$\begin{aligned} &\frac{\partial U_j}{\partial T_{Aj}} = \frac{(1+\alpha)^2(t_j+\gamma s)V_j}{\left((1+\alpha)(T_j+t_j+\gamma s)+2\Gamma_i T_i S_i\right)^2} + (\Omega_j + 2\Lambda_j\Gamma_i T_i S_i \Gamma_j)S_j - C_j = 0 \Rightarrow \\ T_j = &\begin{cases} \sqrt{\frac{(t_j+\gamma s)V_j}{C_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j}} - \frac{2\Gamma_i T_i S_i}{1+\alpha} - t_j - \gamma s \\ \quad when\, C_j > (\Omega_j + 2\Lambda_j\Gamma_i T_i S_i \Gamma_j)S_j \, and \, \sqrt{\frac{(t_j+\gamma s)V_j}{C_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j}} > \frac{2\Gamma_i T_i S_i}{1+\alpha} + t_j + \gamma s \\ 0 \, otherwise \end{cases} \end{aligned} \tag{A1}$$

where hacker $j$ assumes that firms $A$ and $B$ behave equivalently in equilibrium. The second order condition is always satisfied as negative;

$$\frac{\partial^2 U_j}{\partial {T_{Aj}}^2} = \frac{-2(1+\alpha)(1+\alpha^2)(t_j+\gamma s)V_j}{\left((1+\alpha)(T_j+t_j+\gamma s)+2\Gamma_i T_i S_i\right)^3} \tag{A2}$$

Without loss of generality we consider firm $A$ in period 3, and replace $t_j$ and $s$ in (A1) with $t_{Aj}$ and $s_A$, respectively, since firm $A$'s optimization is based on taking firm $B$'s behavior as given. Inserting $T_{Aj} = T_{Bj} = T_j$ in (A1) into (11) gives firm $A$'s period 3 utility

$$\begin{aligned} u_A = &v_i - \frac{T_{Ai}+\alpha T_{Bi}}{t_{Ai}+T_{Ai}+\alpha(t_{Bi}+T_{Bi})}v_i - c_i t_{Ai} \\ &+ \frac{\sqrt{(t_{Aj}+\gamma s_A)}\sqrt{C_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j}}{\sqrt{V_j}}v_j - c_j t_{Aj} - (\phi_1 s_A^2 - \phi_2 s_B^2 - \phi_3 s_A s_B) \end{aligned} \tag{A3}$$

Differentiating $u_A$ in (A3) with respect to $t_{Aj}$ and $s_A$, and equating with zero gives

$$\begin{aligned} \frac{\partial u_A}{\partial t_{Aj}} &= \frac{v_j\sqrt{C_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j}}{2\sqrt{t_{Aj}+\gamma s_A}\sqrt{V_j}} - c_j = 0 \\ \frac{\partial u_A}{\partial s_A} &= \frac{\gamma v_j\sqrt{C_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j}}{2\sqrt{(t_{Aj}+\gamma s_A)}\sqrt{V_j}} - 2\phi_1 s_A + \phi_3 s_B = 0 \end{aligned} \tag{A4}$$

Inserting $T_i = T_{Ai} = T_{Bi}$, $t_i = t_{Ai} = t_{Bi}$, $t_j = t_{Aj} = t_{Bj}$, $s = s_A = s_B$, and equivalent parameters into (A4) and solving yields

$$\begin{aligned} s = &\begin{cases} \frac{\gamma c_j}{2\phi_1-\phi_3} \, when \, \frac{C_j/V_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j/V_j}{4c_j^2/v_j^2} > \gamma s \\ 0 \, otherwise \end{cases} \\ t_j = &\begin{cases} \frac{C_j/V_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j/V_j}{4c_j^2/v_j^2} - \gamma s \, when \, \frac{C_j/V_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j/V_j}{4c_j^2/v_j^2} > \gamma s \\ 0 \, otherwise \end{cases} \end{aligned} \tag{A5}$$

The second order conditions are always satisfied as negative, and the Hessian matrix is negative semi-definite, i.e.,

$$\begin{aligned}
\frac{\partial^2 u_A}{\partial t_{Aj}^2} &= -\frac{v_j\sqrt{C_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j}}{4(t_{Aj}+\gamma s_A)^{3/2}\sqrt{V_j}} \\
\frac{\partial^2 u_A}{\partial s_A^2} &= -\frac{\gamma^2 v_j\sqrt{C_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j}}{4(t_{Aj}+\gamma s_A)^{3/2}\sqrt{V_j}} \\
\frac{\partial^2 u_A}{\partial t_{Aj}\partial s_A} &= \frac{\partial^2 u_A}{\partial s_A\partial t_{Aj}} = -\frac{\gamma v_j\sqrt{C_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j}}{4(t_{Aj}+\gamma s_A)^{3/2}\sqrt{V_j}} \\
|H| &= \begin{vmatrix} \frac{\partial^2 u_A}{\partial t_{Aj}^2} & \frac{\partial^2 u_A}{\partial t_{Aj}\partial s_A} \\ \frac{\partial^2 u_A}{\partial s_A\partial t_{Aj}} & \frac{\partial^2 u_A}{\partial s_A^2} \end{vmatrix} = \frac{\partial^2 u_A}{\partial t_{Aj}^2}\frac{\partial^2 u_A}{\partial s_A^2} - \frac{\partial^2 u_A}{\partial t_{Aj}\partial s_A}\frac{\partial^2 u_A}{\partial s_A\partial t_{Aj}} = 0
\end{aligned} \tag{A6}$$

Inserting $T_j$ in (A1) and $t_j$ in (A5) into (9), and setting $T_i = T_{Ai} = T_{Bi}$ and $t_i = t_{Ai} = t_{Bi}$, gives hacker $i$'s period 2 utility

$$U_i = 2T_i\left[\frac{V_i}{t_i+T_i} + \Lambda_i\Gamma_i S_i\Gamma_j\left(\frac{1}{c_j/v_j} - \frac{4\Gamma_i T_i S_i}{1+\alpha} - \frac{C_j/V_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j/V_j}{2c_j^2/v_j^2}\right)S_j + \Omega_i S_i - C_i\right] \tag{A7}$$

Differentiating $U_i$ in (A7) with respect to $T_i$ and $S_i$, and equating with zero, gives

$$\begin{aligned}
\frac{\partial U_i}{\partial T_i} &= 2S_i\Lambda_i\Gamma_i\Gamma_j\left(\frac{1}{c_j/v_j} - \frac{8\Gamma_i T_i S_i}{1+\alpha} - \frac{C_j/V_j-(\Omega_j+4\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j/V_j}{2c_j^2/v_j^2}\right)S_j \\
&\quad + \frac{2V_i}{t_i+T_i} - \frac{2T_i V_i}{(t_i+T_i)^2} + 2\Omega_i S_i - 2C_i = 0, \\
\frac{\partial U_i}{\partial S_i} &= 2T_i\left[\Lambda_i\Gamma_i\Gamma_j\left(\frac{1}{c_j/v_j} - \frac{8\Gamma_i T_i S_i}{1+\alpha} - \frac{C_j/V_j-(\Omega_j+4\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j/V_j}{2c_j^2/v_j^2}\right)S_j + \Omega_i\right] = 0
\end{aligned} \tag{A8}$$

which are solved to yield

$$\begin{aligned}
T_i &= \begin{cases} \sqrt{t_i}(\sqrt{V_i/C_i} - \sqrt{t_i})\ when\ \frac{V_i}{C_i} > t_i \\ 0\ otherwise \end{cases} \\
S_i &= \begin{cases} \dfrac{(1+\alpha)\left(2c_j/v_j - C_j/V_j + \frac{2\Omega_i c_j^2/v_j^2}{\Lambda_i\Gamma_i\Gamma_j S_j} + \frac{\Omega_j S_j}{V_j}\right)}{4T_i\Gamma_i\left(4c_j^2/v_j^2 - (1+\alpha)\Lambda_j\Gamma_j S_j/V_j\right)} \\ \quad when\ \frac{2c_j}{v_j} > \frac{C_j}{V_j} - \frac{2\Omega_i c_j^2/v_j^2}{\Lambda_i\Gamma_i\Gamma_j S_j} - \frac{\Omega_j S_j}{V_j}\ and\ \frac{2c_j}{v_j} > \sqrt{\frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}}\quad and\ \frac{V_i}{C_i} > t_i \\ 0\ otherwise \end{cases}
\end{aligned} \tag{A9}$$

Assuming $0 \le S_i \le 2\Gamma_i T_i$. When (A9) yields $S_i > 2\Gamma_i T_i$, inserting $S_i = 2\Gamma_i T_i$ into the first equation in (A8) gives a fifth order equation in $T_i$ which we do not solve.

Inserting $T_i$ and $S_i$ in (A9) into (A3), and inserting $T_{Ai} = T_{Bi} = T_i$ and $t_{Ai} = t_{Bi} = t_i$ due to symmetry, gives firm $A$'s period 1 utility

$$u_A = \frac{v_i\sqrt{t_i}}{\sqrt{V_i/C_i}} - c_i t_i + \frac{\sqrt{(t_{Aj}+\gamma s_A)}\sqrt{C_j-(\Omega_j+2\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j}}{\sqrt{V_j}}v_j - c_j t_{Aj} - (\phi_1 s_A^2 - \phi_2 s_B^2 - \phi_3 s_A s_B) \tag{A10}$$

where $T_i S_i$ and $t_{Aj}$ do not depend on $t_i$. Differentiating $u_A$ in (A10) with respect to $t_i$, equating with zero and solving, gives

$$\frac{\partial u}{\partial t_i} = \frac{v_i}{2\sqrt{t_i V_i/C_i}} - c_i = 0 \Rightarrow t_i = \begin{cases} \frac{C_i/V_i}{4c_i^2/v_i^2}\ when\ \frac{C_i}{V_i} < \frac{2c_i}{v_i} \\ 0\ otherwise \end{cases} \tag{A11}$$

which is inserted into (A9) to yield

$$T_i = \begin{cases} \frac{1}{4c_i^2/v_i^2}\left(\frac{2c_i}{v_i} - \frac{C_i}{V_i}\right) \textit{ when } \frac{C_i}{V_i} < \frac{2c_i}{v_i} \\ 0 \textit{ otherwise} \end{cases}$$

$$S_i = \begin{cases} \frac{(1+\alpha)\left(\frac{2c_j}{v_j} - \frac{C_j}{V_j} + \frac{2\Omega_i c_j^2/v_j^2}{\Lambda_i\Gamma_i\Gamma_j S_j} + \frac{\Omega_j S_j}{V_j}\right)}{\frac{\Gamma_i}{c_i^2/v_i^2}\left(\frac{2c_i}{v_i} - \frac{C_i}{V_i}\right)\left(\frac{4c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right)} \\ \quad \textit{when } \frac{2c_j}{v_j} > \frac{C_j}{V_j} - \frac{2\Omega_i c_j^2/v_j^2}{\Lambda_i\Gamma_i\Gamma_j S_j} - \frac{\Omega_j S_j}{V_j} \textit{ and } \frac{2c_j}{v_j} > \sqrt{\frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}} \\ \quad \textit{and } \frac{C_i}{V_i} < \frac{2c_i}{v_i} \\ 0 \textit{ otherwise} \end{cases} \tag{A12}$$

The second order conditions and Hessian matrix are

$$\begin{aligned} \frac{\partial^2 U_i}{\partial T_i^2} &= -\frac{4S_i^2\Lambda_i\Gamma_i^2\Gamma_j}{(1+\alpha)c_j^2/v_j^2}\left(\frac{4c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right)S_j - \frac{4t_i V_i}{(t_i+T_i)^3} \\ \frac{\partial^2 U_i}{\partial S_i^2} &= -\frac{4T_i^2\Lambda_i\Gamma_i^2\Gamma_j}{(1+\alpha)c_j^2/v_j^2}\left(\frac{4c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right)S_j \\ \frac{\partial^2 U_i}{\partial T_i\partial S_i} &= \frac{\partial^2 U_i}{\partial S_i\partial T_i} = 2\Lambda_i\Gamma_i\Gamma_j\left(\frac{1}{c_j/v_j} - \frac{8\Gamma_i T_i S_i}{1+\alpha} - \frac{C_j/V_j - (\Omega_j + 4\Lambda_j\Gamma_i T_i S_i\Gamma_j)S_j/V_j}{2c_j^2/v_j^2}\right)S_j \\ &\quad - \frac{4T_i S_i\Lambda_i\Gamma_i^2\Gamma_j}{(1+\alpha)c_j^2/v_j^2}\left(\frac{4c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right)S_j + 2\Omega_i S_i \\ |H| &= \begin{vmatrix} \frac{\partial^2 U_i}{\partial T_i^2} & \frac{\partial^2 U_i}{\partial T_i\partial S_i} \\ \frac{\partial^2 U_i}{\partial S_i\partial T_i} & \frac{\partial^2 U_i}{\partial S_i^2} \end{vmatrix} = \frac{\partial^2 U_i}{\partial T_i^2}\frac{\partial^2 U_i}{\partial S_i^2} - \frac{\partial^2 U_i}{\partial T_i\partial S_i}\frac{\partial^2 U_i}{\partial S_i\partial T_i} \geq 0 \end{aligned} \tag{A13}$$

Inserting the values for $t_i$ in (A11) and $T_i$ and $S_i$ in (A12) into (A13) gives

$$|H| = \frac{2C_i S_j(2c_i/v_i - C_i/V_i)^2\Gamma_i^2\Gamma_j\Lambda_i(4c_j^2/v_j^2 - (1+\alpha)\Lambda_j\Gamma_j S_j/V_j)}{(1+\alpha)(c_i^3/v_i^3)c_j^2/v_j^2} \geq 0 \tag{A14}$$

The Hessian matrix is negative semi-definite when $\frac{2c_j}{v_j} > \sqrt{\frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}}$.
Inserting (A12) into (A5) gives

$$s = \begin{cases} \frac{\gamma c_j}{2\phi_1 - \phi_3} \textit{ when } \frac{\left(\frac{C_j}{V_j} - \frac{\Omega_j S_j}{V_j}\right)\left(\frac{8c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right) - 2\Lambda_j(1+\alpha)\frac{c_j}{v_j}\left(\frac{\Gamma_j S_j}{V_j} + \frac{\Omega_i c_j/v_j}{\Lambda_i\Gamma_i V_j}\right)}{8\left(4c_j^2/v_j^2 - (1+\alpha)\Lambda_j\Gamma_j S_j/V_j\right)c_j^2/v_j^2} > \gamma s \\ 0 \textit{ otherwise} \end{cases}$$

$$t_j = \begin{cases} \frac{\left(\frac{C_j}{V_j} - \frac{\Omega_j S_j}{V_j}\right)\left(\frac{8c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right) - 2\Lambda_j(1+\alpha)\frac{c_j}{v_j}\left(\frac{\Gamma_j S_j}{V_j} + \frac{\Omega_i c_j/v_j}{\Lambda_i\Gamma_i V_j}\right)}{8\left(4c_j^2/v_j^2 - (1+\alpha)\Lambda_j\Gamma_j S_j/V_j\right)c_j^2/v_j^2} - \gamma s \\ \quad \textit{when } \frac{2c_j}{v_j} > \frac{C_j}{V_j} - \frac{2\Omega_i c_j^2/v_j^2}{\Lambda_i\Gamma_i\Gamma_j S_j} - \frac{\Omega_j S_j}{V_j} \textit{ and } \frac{2c_j}{v_j} > \sqrt{\frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}} \quad \textit{and } \frac{C_i}{V_i} < \frac{2c_i}{v_i} \\ \quad \textit{and } \frac{\left(\frac{C_j}{V_j} - \frac{\Omega_j S_j}{V_j}\right)\left(\frac{8c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j\Gamma_j S_j}{V_j}\right) - 2\Lambda_j(1+\alpha)\frac{c_j}{v_j}\left(\frac{\Gamma_j S_j}{V_j} + \frac{\Omega_i c_j/v_j}{\Lambda_i\Gamma_i V_j}\right)}{8\left(4c_j^2/v_j^2 - (1+\alpha)\Lambda_j\Gamma_j S_j/V_j\right)c_j^2/v_j^2} > \gamma s \\ 0 \textit{ otherwise} \end{cases} \tag{A15}$$

Inserting (A12) and (A15) into (A1) gives

$$T_j = \begin{cases} \frac{2c_j/v_j - C_j/V_j + \Omega_j S_j/V_j}{8c_j^2/v_j^2} - \frac{\Omega_i}{4\Lambda_i \Gamma_i \Gamma_j S_j} \\ \quad when\ \frac{2c_j}{v_j} > \frac{C_j}{V_j} + \frac{2\Omega_i c_j^2/v_j^2}{\Lambda_i \Gamma_i \Gamma_j S_j} - \frac{\Omega_j S_j}{V_j}\ and\ \frac{2c_j}{v_j} > \sqrt{\frac{(1+\alpha)\Lambda_j \Gamma_j S_j}{V_j}}\quad and\ \frac{C_i}{V_i} < \frac{2c_i}{v_i} \\ \quad and\ \frac{\left(\frac{C_j}{V_j} - \frac{\Omega_j S_j}{V_j}\right)\left(\frac{8c_j^2}{v_j^2} - \frac{(1+\alpha)\Lambda_j \Gamma_j S_j}{V_j}\right) - 2\Lambda_j(1+\alpha)\frac{c_j}{v_j}\left(\frac{\Gamma_j S_j}{V_j} + \frac{\Omega_i c_j/v_j}{\Lambda_i \Gamma_i V_j}\right)}{8\left(4c_j^2/v_j^2 - (1+\alpha)\Lambda_j \Gamma_j S_j/V_j\right)c_j^2/v_j^2} > \gamma s \\ 0\ otherwise \end{cases} \tag{A16}$$

*Appendix A.2. Mutual Reaction between Hacker i and Each Firm in the First Attack*

Differentiating (2) gives

$$\begin{aligned} \frac{\partial U_i^{first}}{\partial T_{Ai}} &= \frac{t_{Ai} V_i}{(T_{Ai}+t_{Ai})^2} - C_i = 0 \Rightarrow T_{Ai} = T_i = \begin{cases} \left(\sqrt{\frac{V_i}{C_i}} - \sqrt{t_i}\right)\sqrt{t_i}\ when\ t_i < \frac{V_i}{C_i} \\ 0\ otherwise \end{cases}, \\ \frac{\partial T_i}{\partial t_i} &= \frac{1}{2}\sqrt{\frac{V_i}{C_i t_i}} - 1, \frac{\partial^2 T_i}{\partial t_i^2} = -\frac{\sqrt{V_i}}{2t_i^{3/2}\sqrt{C_i}} \\ \frac{\partial u^{first}}{\partial t_{Ai}} &= \frac{T_{Ai} v_i}{(T_{Ai}+t_{Ai})^2} - c_i = 0 \Rightarrow t_{Ai} = t_i = \begin{cases} \left(\sqrt{\frac{v_i}{c_i}} - \sqrt{T_i}\right)\sqrt{T_i}\ when\ T_i < \frac{v_i}{c_i} \\ 0\ otherwise \end{cases}, \\ \frac{\partial t_i}{\partial T_i} &= \frac{1}{2}\sqrt{\frac{v_i}{c_i T_i}} - 1, \frac{\partial^2 t_i}{\partial T_i^2} = -\frac{\sqrt{v_i}}{2T_i^{3/2}\sqrt{c_i}} \end{aligned} \tag{A17}$$

where $\partial T_i/\partial t_i > 0$ when $t_i < V_i/4C_i$, $\partial T_i/\partial t_i < 0$ when $V_i/C_i > t_i > V_i/4C_i$, $\partial t_i/\partial T_i > 0$ when $T_i < v_i/4c_i$, $\partial t_i/\partial T_i < 0$ when $v_i/c_i > T_i > v_i/4c_i$.

*Appendix A.3. Corner Solution When Hacker i Is Deterred*

$T_i = T_{Ai} = T_{Bi} = 0$ causes $S_i = 0$ according to $U_i$ in (9). Inserting $T_i = S_i = 0$, and $S_j = 0$ since hacker $j$ does not gain from information sharing, into (A9) and solving gives $t_i = V_i/C_i$. When hacker $i$ is deterred, inserting $T_i = S_i = S_j = 0$ into (A5) and (A1) gives

$$t_j = \frac{C_j/V_j}{4c_j^2/v_j^2} - \gamma s, \quad s = \frac{\gamma c_j}{2\phi_1 - \phi_3}, \quad T_j = \begin{cases} \frac{1}{4c_j^2/v_j^2}\left(\frac{2c_j}{v_j} - \frac{C_j}{V_j}\right)\ when\ \frac{2c_j}{v_j} > \frac{C_j}{V_j} \\ 0\ otherwise \end{cases} \tag{A18}$$

which is the same solution as for $t_i$ and $T_i$ in (13) except that we now have $t_j + \gamma s$ instead of $t_i$ because of information sharing.

*Appendix A.4. Corner Solution When Hacker j Is Deterred*

Deterring hacker $j$ means inserting $T_j = 0$ into (A1) and solving

$$\sqrt{\frac{(t_j + \gamma s)V_j}{C_j - (\Omega_j + 2\Lambda_j \Gamma_i T_i S_i \Gamma_j)S_j}} - \frac{2\Gamma_i T_i S_i}{1+\alpha} - t_j - \gamma s = 0 \tag{A19}$$

with respect to $t_j$. When hacker $j$ is deterred, hacker $i$ gains nothing by sharing information causing $S_i = 0$. Accordingly we assume that hacker $j$ does not share information either, $S_j = 0$. Inserting into (A19) yields $t_j = V_j/C_j - \gamma s$.

## References

1. Kampanakis, P. Security automation and threat information-sharing options. *IEEE Secur. Priv.* **2014**, *12*, 42–51. [CrossRef]

2. Novshek, W.; Sonnenschein, H. Fulfilled expectations cournot duopoly with information acquisition and release. *Bell J. Econ.* **1982**, *13*, 214–218. [CrossRef]
3. Gal-Or, E. Information sharing in oligopoly. *Econometrica* **1985**, *53*, 329–343. [CrossRef]
4. Shapiro, C. Exchange of cost information in oligopoly. *Rev. Econ. Stud.* **1986**, *53*, 433–446. [CrossRef]
5. Kirby, A.J. Trade associations as information exchange mechanisms. *RAND J. Econ.* **1988**, *19*, 138–146. [CrossRef]
6. Vives, X. Trade association disclosure rules, incentives to share information, and welfare. *RAND J. Econ.* **1990**, *21*, 409–430. [CrossRef]
7. Cremonini, M.; Nizovtsev, D. Risks and benefits of signaling information system characteristics to strategic attackers. *J. Manag. Inf. Syst.* **2009**, *26*, 241–274. [CrossRef]
8. Fultz, N.; Grossklags, J. Blue versus red: Towards a model of distributed security attacks. In Proceedings of the Thirteenth International Conference Financial Cryptography and Data Security, Accra Beach, Barbados, 23–26 February 2009; Springer: Christ Church, Barbados, 2009.; pp. 167–183.
9. Herley, C. Small world: Collisions among attackers in a finite population. In Proceedings of the 12th Workshop on the Economics of Information Security (WEIS), Washington, DC, USA, 11–12 June 2013.
10. Lin, Y. The institutionalization of hacking practices. *Ubiquity* **2003**, *2003*. [CrossRef]
11. Sarvari, H.; Abozinadah, E.; Mbaziira, A.; Mccoy, D. Constructing and analyzing criminal networks. In Proceedings of the IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 17–18 May 2014; pp. 84–91.
12. August, T.; Niculescu, M.F.; Shin, H. Cloud implications on software network structure and security risks. *Inf. Syst. Res.* **2014**, *25*, 489–510. [CrossRef]
13. Dey, D.; Lahiri, A.; Zhang, G. Quality competition and market segmentation in the security software market. *MIS Q.* **2014**, *38*, 589–606.
14. Dey, D.; Lahiri, A.; Zhang, G. Hacker behavior, network effects, and the security software market. *J. Manag. Inf. Syst.* **2012**, *29*, 77–108. [CrossRef]
15. Galbreth, M.; Shor, M. The impact of malicious agents on the enterprise software industry. *MIS Q.* **2010**, *34*, 595–612.
16. Chul Ho, L.; Xianjun, G.; Raghunathan, S. Contracting information security in the presence of double moral hazard. *Inf. Syst. Res.* **2013**, *24*, 295–311.
17. Ransbotham, S.; Mitra, S. Choice and chance: A conceptual model of paths to information security compromise. *Inf. Syst. Res.* **2009**, *20*, 121–139. [CrossRef]
18. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W. Sharing information on computer systems security: An economic analysis. *J. Account. Public Policy* **2003**, *22*, 461–485. [CrossRef]
19. Gal-Or, E.; Ghose, A. The economic incentives for sharing security information. *Inf. Syst. Res.* **2005**, *16*, 186–208. [CrossRef]
20. Hausken, K. Security investment and information sharing for defenders and attackers of information assets and networks. In *Information Assurance, Security and Privacy Services, Handbooks in Information Systems*; Rao, H.R., Upadhyaya, S.J., Eds.; Emerald Group Pub Ltd.: Bingley, UK, 2009; Volume 4, pp. 503–534.
21. Hausken, K. Information sharing among firms and cyber attacks. *J. Account. Public Policy* **2007**, *26*, 639–688. [CrossRef]
22. Gao, X.; Zhong, W.; Mei, S. A game-theoretic analysis of information sharing and security investment for complementary firms. *J. Oper. Res. Soc.* **2014**, *65*, 1682–1691. [CrossRef]
23. Liu, D.; Ji, Y.; Mookerjee, V. Knowledge sharing and investment decisions in information security. *Decis. Support Syst.* **2011**, *52*, 95–107. [CrossRef]
24. Mallinder, J.; Drabwell, P. Cyber security: A critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber attack. *J. Bus. Contin. Emerg. Plan.* **2013**, *7*, 103–111.
25. Choras, M. Comprehensive approach to information sharing for increased network security and survivability. *Cybern. Syst.* **2013**, *44*, 550–568. [CrossRef]
26. Tamjidyamcholo, A.; Bin Baba, M.S.; Tamjid, H.; Gholipour, R. Information security—Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Comput. Educ.* **2013**, *68*, 223–232. [CrossRef]

27. Rocha Flores, W.; Antonsen, E.; Ekstedt, M. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Comput. Secur.* **2014**, *43*, 90–110. [CrossRef]
28. Tamjidyamcholo, A.; Bin Baba, M.S.; Shuib, N.L.M.; Rohani, V.A. Evaluation model for knowledge sharing in information security professional virtual community. *Comput. Secur.* **2014**, *43*, 19–34. [CrossRef]
29. Png, I.P.L.; Wang, Q.-H. Information security: Facilitating user precautions vis-à-vis enforcement against attackers. *J. Manag. Inf. Syst.* **2009**, *26*, 97–121. [CrossRef]
30. Choi, J.P.; Fershtman, C.; Gandal, N. Network security: Vulnerabilities and disclosure policy. *J. Ind. Econ.* **2010**, *58*, 868–894. [CrossRef]
31. Nizovtsev, D.; Thursby, M. To disclose or not? An analysis of software user behavior. *Inf. Econ. Policy* **2007**, *19*, 43–64. [CrossRef]
32. Arora, A.; Krishnan, R.; Telang, R.; Yang, Y. An empirical analysis of software vendors' patch release behavior: Impact of vulnerability disclosure. *Inf. Syst. Res.* **2010**, *21*, 115–132. [CrossRef]
33. Temizkan, O.; Kumar, R.L.; Park, S.; Subramaniam, C. Patch release behaviors of software vendors in response to vulnerabilities: An empirical analysis. *J. Manag. Inf. Syst.* **2012**, *28*, 305–338. [CrossRef]
34. Cavusoglu, H.; Mishra, B.; Raghunathan, S. The value of intrusion detection systems in information technology security architecture. *Inf. Syst. Res.* **2005**, *16*, 28–46. [CrossRef]
35. Moore, T.; Clayton, R.; Anderson, R. The economics of online crime. *J. Econ. Perspect.* **2009**, *23*, 3–20. [CrossRef]
36. Skopik, F.; Settanni, G.; Fiedler, R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Comput. Secur.* **2016**, *60*, 154–176. [CrossRef]
37. Hausken, K. A strategic analysis of information sharing among cyber attackers. *J. Inf. Syst. Technol. Manag.* **2015**, *12*, 245–270. [CrossRef]
38. Hausken, K. Information sharing among cyber hackers in successive attacks. *Int. Game Theory Rev.* **2017**, *19*. [CrossRef]
39. Raymond, E.S. *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*; O'Reilly Media: Sebastopol, CA, USA, 2008.
40. Ritchie, C. *A Look at the Security of the Open Source Development Model*; Technical Report; Oregon State University: Corvallis, OR, USA, 2000.
41. Brunker, M. Hackers: Knights-Errant or Knaves? NBCNews. 1998. Available online: http://msnbc.msn.com/id/3078783 (accessed on 24 May 2017).
42. Simon, H. *The Sciences of the Artificial*; MIT Press: Cambridge, MA, USA, 1969.
43. Hirshleifer, J. Anarchy and its breakdown. *J. Political Econ.* **1995**, *103*, 26–52. [CrossRef]
44. Tullock, G. The welfare costs of tariffs, monopolies, and theft. *West. Econ. J.* **1967**, *5*, 224–232. [CrossRef]
45. Salop, S.C.; Scheffman, D.T. Raising rivals' costs. *Am. Econ. Rev.* **1983**, *73*, 267–271.
46. Hausken, K. Production and conflict models versus rent-seeking models. *Public Choice* **2005**, *123*, 59–93. [CrossRef]
47. Tullock, G. Efficient rent-seeking. In *Toward a Theory of the Rent-Seeking Society*; Buchanan, J.M., Tollison, R.D., Tullock, G., Eds.; Texas A. & M. University Press: College Station, TX, USA, 1980; pp. 97–112.
48. Kunreuther, H.; Heal, G. Interdependent security. *J. Risk Uncertain.* **2003**, *26*, 231–249. [CrossRef]
49. Hausken, K. Income, interdependence, and substitution effects affecting incentives for security investment. *J. Account. Public Policy* **2006**, *25*, 629–665. [CrossRef]
50. Levins, R. The strategy of model building in population biology. *Am. Sci.* **1966**, *54*, 421–431.
51. Levins, R.; Lewontin, R. *The Dialectical Biologist*; Harvard University Press: Cambridge, MA, USA, 1985.