Journal of Information Security, 2022, 13, 85-100
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

The Economics of Sharing Unclassified Cyber Threat Intelligence by Government Agencies and Departments

Josiah Dykstra[1], Lawrence A. Gordon[2], Martin P. Loeb[2], Lei Zhou[2]

[1]Cybersecurity Collaboration Center, National Security Agency, Fort Meade, MD, USA
[2]Robert H. Smith School of Business, University of Maryland, College Park, MD, USA
Email: josiah.dykstra@cyber.nsa.gov, lagordon@umd.edu, mploeb@umd.edu, lzhou@umd.edu

How to cite this paper: Dykstra, J., Gordon, L.A., Loeb, M.P. and Zhou, L. (2022) The Economics of Sharing Unclassified Cyber Threat Intelligence by Government Agencies and Departments. *Journal of Information Security*, **13**, 85-100.
https://doi.org/10.4236/jis.2022.133006

Received: February 12, 2022
Accepted: June 6, 2022
Published: June 9, 2022

Abstract

This paper extends the literature on the economics of sharing cybersecurity information by and among profit-seeking firms by modeling the case where a government agency or department publicly shares unclassified cyber threat information with all organizations. In prior cybersecurity information sharing models a common element was reciprocity—*i.e.*, firms receiving shared information are also asked to share their private cybersecurity information with all other firms (via an information sharing arrangement). In contrast, sharing of unclassified cyber threat intelligence (CTI) by a government agency or department is not based on reciprocal sharing by the recipient organizations. After considering the government's cost of preparing and disseminating CTI, as well as the benefits to the recipients of the CTI, we provide sufficient conditions for sharing of CTI to result in an increase in social welfare. Under a broad set of general conditions, sharing of CTI will increase social welfare gross of the costs to the government agency or department sharing the information. Thus, if the entity can keep the sharing costs low, sharing cybersecurity information will result in an increase in net social welfare.

Keywords

Cyber Threat Intelligence, Economics of Information Sharing

1. Introduction

The Internet was still in its infancy when well-intentioned users became aware of the presence of bad-intentioned users who saw the Internet as a means of various kinds of theft or harassment. One means to help counter the threat of bad actors on the Internet is for the well-intentioned users to share information concerning the presence of actual attacks, the nature of the attacks, methods to identify the penetration of attackers before the attacks could be carried out, and approaches to remediate successful attacks. Cyber Threat Intelligence (CTI) naturally became of interest to private for-profit and not-for-profit organizations as well as to government entities. The 911 terrorist attacks, along with the realization that approximately 85% of the nation's critical infrastructure are controlled by the private sector, accelerated the United States federal government's interest in facilitating information sharing throughout the economy.[1]

The sharing of cybersecurity-related information by and among private sector firms competing in a common market (via an Information Sharing Analysis Center [ISAC] or other information-sharing organization) is hindered by free-riding behavior and competition among the firms. In contrast, the sharing of CTI by a government agency or department (hereafter the term agency will often be used to refer to a government agency and/or department, such as the National Security Agency [NSA] or the Department of Homeland Security [DHS]) is not based on reciprocal sharing. Thus, in this latter setting, recipients of an agency's CTI are not considered to be free riding by accepting the agency's shared CTI. Furthermore, a government agency or department (e.g., NSA or DHS) does not measure its performance by profits or shareholder value and need not be concerned with a loss of profits to rival firms due to shared CTI. Hence, the incentive problems faced by private sector firms in considering sharing cybersecurity information are not directly pertinent to the government agency's consideration of sharing CTI.[2] Consequently, the economics of sharing CTI by government agencies requires a unique analysis.

Government agencies, in fulfilling their mission of securing the nation from cyber threats, collect and analyze a large quantity of cyber threat information. While a large portion of the collected cyber threat information is deemed as classified or controlled unclassified information, a portion of the information is unclassified and made publicly available. CTI may be classified if its disclosure would damage U.S. national security. For example, information about a foreign cyber threat may be classified if those facts could only be known using sensitive methods that would be compromised by disclosure. CTI that is controlled unclassified information is not classified, but the government believes should be exempt from public disclosure under the Freedom of Information Act. For example, if threat intelligence is associated with a particular intelligence agency it may be sensitive but unclassified. The cost of collecting the cyber threat information is sunk at the time of distributing the information. Once collected, the CTI is designated as classified, controlled unclassified information, or unclassi-

[1] See, for example, [1].

[2] This paper's focus is on the sharing of unclassified CTI. The sharing of classified CTI and controlled unclassified information (including For Official Use Only) raises other incentive issues. Sales [2], for example, notes that government agencies compete with other government agencies for policy influence and budget allocations giving rise to a free-rider problem in sharing (classified and controlled unclassified information) CTI with other government agencies.

fied for public consumption. The costs associated with determining which CTI should be designated as unclassified for public consumption, and preparing that CTI for dissemination to the public, are modest relative to the collection cost. These classification costs, however, are still substantial due to an extensive process associated with classifying, declassifying, or downgrading the classification CTI as unclassified (*i.e.*, the process involves many individuals at various levels of the organization[3]). Furthermore, if one takes into consideration the noise in such a process (as discussed by [4]), the ultimate costs could be quite high.

Before classifying information as unclassified for public consumption, government agencies carefully consider both the potential societal benefits associated with the wide dissemination of CTI as well as the possible costs.[4] The principal benefit of wide dissemination of CTI is associated with potential increased levels of cybersecurity and the savings in cybersecurity costs to the firms receiving the CTI. The primary cost of sharing CTI is the cost associated with the risk of malevolent actors using the publicly disseminated information to refine their cyber-attack strategies. Assuming that government agencies classification processes are effective in that they only publicly share CTI that provide insignificant benefit to malevolent actors, shared CTI allows firms to obtain greater cybersecurity without increasing their investment in cybersecurity and may also spur additional investments in cybersecurity.[5] Thus, by sharing unclassified CTI with the public, there is an expected increase in the nation's overall level of cybersecurity and a corresponding expected increase in the protection of the nation's economic and national security.[6]

From the perspective of a government agency seeking to maximize social welfare, they must consider expected losses from breaches that do not directly accrue to the private sector firms (e.g., externality costs borne by consumers). Hence, showing that information sharing would decrease the expected sum of the costs of cybersecurity breaches and the costs of all firms' cybersecurity investments (plus the agency's cost of preparation and dissemination of CTI) would not be sufficient to show an increase in social welfare. In this paper, we provide sufficient conditions for sharing of CTI by a government agency to result in an increase in the level of cybersecurity, and an increase in social welfare.

The remainder of this paper is organized as follows. In the second section of the paper, we discuss the related literature. We present our model in section three. Section four derives conditions under which expected social welfare is increased by a government agency's sharing of unclassified CTI. Section five discusses the implications of the findings from our analysis. We briefly summarize

[3] An overview of this process can be found in [3].

[4] Mohaisen *et al.* [5] discuss a range of risks associated information sharing.

[5] In our discussion of limitations in section six, we consider the case where malevolent actors receive the shared CTI.

[6] President Biden, as well as the last three Presidents of the United States (*i.e.*, Presidents Bush, Obama, and Trump) have all been concerned with the growing importance of cybersecurity to the nation's economic and national security.

our findings and conclusions, as well as discuss limitations, in section six.

2. Related Literature

The early economics literature concerned with information sharing examined costs and benefits in the context of sharing information unrelated to cybersecurity. For example, [6] [7] [8] [9] [10] examine the sharing of cost or demand information among rival firms.

The sharing of cybersecurity information only became an issue in the years after the development of the Internet. Hence, economic analysis specifically related to sharing of cybersecurity information began early in this millennium. The papers by Gordon *et al.* [11] and Gal-Or and Ghose [12] were among the first to specifically focus on the sharing of cybersecurity-related information sharing. These two papers examine the incentives for firms to share cybersecurity information via an information-sharing organization such as an Information Sharing Analysis Center (ISAC) and showed the potential gains to firms from sharing. The analyses of both [11] and [12] show, however, that without the appropriate incentives the free-rider problem may prevent the welfare benefits of information sharing to be realized.

The literature on the economics of sharing cybersecurity information was dormant for about ten years until a series of papers by Tosh *et al.* [13], Naghizadeh and Liu [14], Ezhei and Ladani [15], and Tosh *et al.* [16] again focused on the incentives for firms to share cybersecurity-related information via participation in an information-sharing organization. Mermoud *et al.* [17] confirmed behavioral issues associated with free-riding in the cybersecurity context. Their study used a questionnaire survey of the 462 total membership of a Swiss ISAC and attained a 62% response rate. More recently, [18] surveyed the cybersecurity information sharing literature, built a model to examine value creation based on the literature, and used a simulation to gain further insights.

The game-theoretic economics literature on cybersecurity information sharing provides insights concerning what drives private sector firms to share information and the associated welfare effects. This literature shows that information sharing can substitute for cybersecurity investment. That is, a firm's optimal investment in information security decreases as it receives information from another firm or from an information-sharing organization. Moreover, the game-theoretic literature highlights secondary and strategic ramifications of any actions by considering how other players (*i.e.*, attackers, competitors) will react to the action. The implications of the above insights for the CTI sharing decisions of a government agency or department (such as NSA or DHS) are, however, unclear at best. Utilizing a different stream of economics-based literature, the paper by Gordon *et al.* [19] applies real options analysis to the sharing of cybersecurity-related information. This paper provides insight that is directly relevant for a government agency or department. More specifically, to the extent that information shared reduces the risk associated with the receiving entity's real option to defer cybersecurity investments, the shared information has the potential effect of motivating the receiving entity to accelerate investments in cybersecurity. In other words, the sharing of CTI by a government agency may reduce the receiving entities' "wait" portion of the "wait and see" strategy for cybersecurity investments.

Laube and Böhme [20] perform an extensive survey of the theoretical and empirical literature on sharing of information cybersecurity-related information. One conclusion that they draw is that, in general, a firm's economic incentives lead them to share cybersecurity-related information to a lesser degree than is optimal from a social welfare maximization perspective.

The papers reviewed above, apart from [19], focused on profit-maximizing firms' decisions to share information with rival firms directly or indirectly (via a trade organization or an information-sharing organization). These papers modeled a firm's sharing decision according to the effect of the decision on the firm's profits. Firms seeking to maximize profits (or shareholder value) must consider how sharing cybersecurity information with their competitors will affect their position in the marketplace. For example, competitors seeking to increase their market share may leak shared information to diminish the reputation of the firm sharing information. However, as shown by [12], conditions may exist such that firms with a strong competitive advantage in the marketplace have an incentive to avoid sharing cybersecurity-related information. In contrast, a government agency or department does not measure its performance by profits or shareholder value. Thus, it need not be concerned with a loss of profits to rival firms. Hence, the incentive problems faced by private sector firms in considering sharing cybersecurity information are not directly pertinent to government agencies' consideration of sharing CTI.

The review paper by He *et al.* [21] discusses the costs and benefits of information sharing arrangements (e.g., ISACS) that involve government participation/sponsorship. In their Table I (p. 222), they list the types of costs, categorized as being incurred as either prior to a cybersecurity attack or after an attack. In their Table II (p. 223), they categorize benefits, all of which accrue to the entity based on the type of information the entity has received and on whether such information reduces the loss from breaches and the reduction of the entity's costs of defending against cyber-attacks. Looking at the summary of costs and benefits given by [21], one notices that all of the benefits are received by the entity with no direct benefits reaped by the Government.

The Sales [2] paper is relevant to the current study because it indicates that one should explicitly consider the government agency's objective function and how there may be a conflict (*i.e.*, a divergence of preferences) between the agency and individual decision-makers within the agency. In considering incentives to share CTI in a government setting, one should consider separately the incentives to share controlled unclassified information and unclassified CTI (*i.e.*, CTI made publicly available). Employing a logical narrative reflective of the articles found in law journals and making use of concepts from the economics of public choice literature, [2] focuses implicitly on a government agency's incentive to share CTI that is controlled unclassified information and addresses the question of why intelligence agencies are reluctant to share such information. The author claims that public policy directives have not resulted in the desired increase in information sharing because the policymakers have failed to consider "the iron law of agency self-interest." According to [2], agencies are interested in maximizing their influence over executive branch senior policymakers and in maintaining or increasing their agency's autonomy. By sharing information with another agency, that agency may get credit for a substantial part of the work of the agency that produced the information. This reduces the relative influence of the government agency and, with a lag, can result in a decreased budget for the agency (it also decreases the government agency's incentive to produce valuable threat information in the first place). Also, sharing information may result in another government agency expanding its operations to the turf of the agency producing the information, resulting in a loss of agency autonomy. Furthermore, institutional culture reinforces the idea that an individual analyst has more to lose than to gain from sharing information. That is, the risk of hurting an analyst's career advancement due to sharing information may be greater than the potential gain to an analyst's career from sharing such information. Thus, organizational problems lead many analysts to be excessively risk-averse to sharing CTI that is controlled unclassified information.

3. The Model

Let us now turn our attention to the sharing of unclassified CTI and present a model to investigate the welfare benefit of a government agency's sharing of such CTI. Consider an economy composed of n identical firms and a consumer sector. Following [22], each firm wishes to protect a single information set by weighing the expected benefits from investments in cybersecurity versus the costs of the investment. Let x represent the firm's monetary expenditures on cybersecurity and L_p represent the firm's loss if their information set is breached. We assume the effectiveness of a firm's cybersecurity expenditures in reducing the probability of the firm's information set being breached depends on the CTI that the firm has received from the government agency or department.[7]

Assume that the quantity of (unclassified) CTI shared with all firms can be represented by a non-negative real number denoted as y. Similar to the [11] formulation, the probability that a firm's information set is breached is represented by the security breach probability function $P(x,y)$, where P is a continuously twice differentiable function that decreases in the firm's cybersecurity expenditures at a decreasing rate and, for positive levels of cybersecurity expenditures, is non-increasing in the quantity of CTI shared by the government

[7] This formulation is similar to that of [11], where cybersecurity information received was information shared from by members of an information sharing organization.

agency. That is, $P_1(x,y)<0$, $P_{11}(x,y)>0$, and $P_2(x,y)\le 0$, where $P_1(x,y)=\frac{\partial P(x,y)}{\partial x}$, $P_{11}(x,y)=\frac{\partial P(x,y)}{\partial x^2}$, and $P_2(x,y)=\frac{\partial P(x,y)}{\partial y}$.

For a given amount of shared CTI, each firm selects the cybersecurity expenditure level to minimize its total expected cybersecurity costs, which equals its expected costs from breach plus the firm's cybersecurity expenditures.[8] That is, each firm selects *x*(*y*) as shown in Equation (1):

$$x(y)=\left\{P(\underline{x},y)L_p+\underline{x}\right\}. \tag{1}$$

Given the assumed properties of the security breach probability function, *x*(*y*) uniquely minimizes the expression in brackets in Equation (1). Hence, as one would naturally expect.

CTI sharing cannot leave any firm worse off.[9] That is:

$$P\big(x(y),y\big)L_p+x(y)\le P\big(x(0),0\big)L_p+x(0). \tag{2}$$

For the case where (2) holds as a strict Inequality, each firm's expected total cybersecurity costs (*i.e.*, their expected losses from a breach plus their expenditures on cybersecurity prevention) will be less when the CTI is provided than when it is not. Since the welfare of each firm increases when their expected total cybersecurity costs decrease, the welfare of all firms increases when the government agency shares unclassified CTI. Yet, for this case, there are two reasons why such sharing does not necessarily lead to an increase in total social welfare. The first reason is that total social welfare is decreased by the cost to the government agency of classifying and disseminating unclassified CTI. Hence, if those costs are sufficiently large, sharing unclassified CTI will cause total expected welfare to decline. The second reason that total social welfare may decline as it is decreased by the externality costs of cybersecurity breaches that are borne by consumers.[10] These externality costs, while difficult to measure, can be substantial and include monetary and non-pecuniary costs consumers bear in dealing with identity theft.

The total externality costs suffered by all consumers from a single cybersecurity breach is denoted as L_e, so that the externality costs suffered from the expected number of cybersecurity breaches is $n\cdot P\big(x(y),y\big)\cdot L_e$. For simplicity, the government agency's cost of classifying and disseminating unclassified y units of CTI is assumed to be equal to $c\cdot y$ (*i.e.*, c is the constant variable cost of classifying and disseminating a unit of CTI). The government agency's objec-

[8] For simplicity, we assume that the probability of a firm suffering a cybersecurity breach does not depend on whether other firms suffer a breach. Since all firms are motivated to select the same level, *x*(*y*), of cybersecurity expenditures, the probability of cybersecurity breaches occurring follow a binomial distribution with $b(n,p)=b\big(n,P\big(x(y),y\big)\big)$. Thus, the expected number of breaches in the economy will be $n\cdot P\big(x(y),y\big)$.

[9] This result (*i.e.*, Equation (2)) is formally proven in the Appendix as part of the proof of our first proposition.

[10] For simplicity, we do not consider the externalities of a firm's cybersecurity breach imposed on other firms.

tive, therefore, is viewed as the minimization of total expected social costs, denoted $E\left[SC(y)\right]$, with respect to *y*, the quantity of information the agency shares. The total expected value of social costs, $E\left[SC(y)\right]$, can be written as:

$$E\left[SC(y)\right]=n\left\{P\left(x(y),y\right)\cdot L_p+x(y)+P\left(x(y),y\right)\cdot L_e\right\}+c\cdot y, \tag{3}$$

where the term $n\cdot\left[P\left(x(y),y\right)\cdot L_p+x(y)\right]$ represents the sum of expected cybersecurity costs for all *n* firms.

The government agency's problem, therefore, is to select *y* to minimize

$$E\left[SC(y)\right]=n\left[P\left(x(y),y\right)\cdot L_p+x(y)\right]+n\cdot P\left(x(y),y\right)\cdot L_e+c\cdot y\,. \tag{4}$$

Let L represent the sum of the losses of a cybersecurity breach to a firm and the loss of a cybersecurity breach to all consumers, that is $L=L_p+L_e$, then (4) can be written as:

$$E\left[SC(y)\right]=n\left[P\left(x(y),y\right)\cdot L+x(y)\right]+c\cdot y\,. \tag{5}$$

Having presented the basic model, we now examine the conditions under which sharing CTI is beneficial. For CTI sharing to be beneficial, the expected social costs with sharing must be less than the expected social costs without sharing.

4. When Sharing CTI Is Beneficial

Sharing of unclassified CTI by a government agency or department influences each firm's marginal productivity of cybersecurity investments and, hence, the firm's level of cybersecurity investments, $x(y)$. The level, *y*, of sharing of CTI can have one of three effects on each firm's selected level of cybersecurity investments and the resulting probability of a cybersecurity breach. Firstly, the CTI shared could increase the firm's marginal productivity of investments, leading the firm to increase its cybersecurity investments and thereby causing the probability of a cybersecurity breach to decrease. Secondly, the CTI shared could have no effect on the firm's marginal productivity of investments resulting in the firm level of cybersecurity investments remaining the same. Even though sharing would have no effect on the cybersecurity level of investment for this case, the probability of a cybersecurity breach could decrease since, by having received information on existing threats firms could employ their existing cybersecurity assets more effectively. This is the underlying reasoning behind the assumption that $P(x,y)$ is non-increasing in *y*. Thirdly, the CTI shared could substitute for some of each firm's investment in cybersecurity (especially their purchases of CTI from private firms) and cause each firm's investment in cybersecurity to decline. However, the resulting change in the probability of a breach would then be indeterminate and depend on the specific functional form of $P(x,y)$. Therefore, even when the government sharing of CTI leads to a decline in each firm's level of cybersecurity expenditures, the probability of cybersecurity breach could decline.

The following proposition shows that whenever CTI sharing leads to a reduction in the probability of security breaches sharing CTI will increase social welfare for sufficiently small sharing costs. That is the proposition provides a sufficient condition for the sharing of CTI to meet the cost/benefit test. (The proofs of propositions are shown in the Appendix.)

Proposition 1: Suppose sharing $y > 0$ CTI leads firms to select $x(y)$ such that $P(x(0),0) > P(x(y),y)$. Then, for sufficiently small $c > 0$, $E[SC(y)] < E[SC(0)]$.

While Proposition 1 gives a sufficient condition for CTI sharing to be welfare enhancing, it remains to be shown that the conditions of the proposition do not hold vacuously. To do so we consider two broad classes of security breach probability functions. The two broad classes of security breach probability functions are natural modifications of the two classes specified in the Gordon-Loeb Model [22], which are widely used in the literature (e.g., [23] [24] [25] [26] [27]). The two classes of security breach probability functions in [22], modified to include the CTI sharing variable, are given below:

$$P^I(x,y) = v \big/ \left[\alpha x(y+1)+1\right]^\beta, \tag{6}$$

where $\alpha > 0$ and $\beta \geq 1$ are productivity measures; and

$$P^{II}(x,y) = v^{\alpha x(y+1)+1}, \tag{7}$$

where $\alpha > 0$ is a productivity measure.

The following proposition shows that for security breach probability functions belonging to either of the two broad classes specified in Equations (6) and (7), a positive amount of shared CTI leads to a decrease in the probability of a breach and hence to an increase is social welfare when sharing cost are sufficiently small.

Proposition 2: For security breach probability function $P^I(x,y) = v \big/ \left[\alpha x(y+1)+1\right]^\beta$ and security breach probability function $P^{II}(x,y) = v^{\alpha x(y+1)+1}$, sharing CTI by the government agency decreases the probability of a security breach, *i.e.*, $P^I[x(y),y] < P^I[x(0),0]$ and $P^{II}[x(y),y] < P^{II}[x(0),0]$ for $y > 0$. Hence, for sufficiently small $c > 0$, CTI sharing by the government increases the expected social welfare.

Given that the breadth of the two classes of security breach probability functions, P^I and P^{II}, Proposition 2 provides some reassurance that when the costs of providing CTI are sufficiently small, social welfare is increased by sharing of CTI[11].

Observation: Based on the first-order condition of minimizing the total expected cybersecurity costs $P_1(x,y)L+1=0$, we have $P_{11}(x,y)L\partial x + P_{12}(x,y)L\partial y = 0$. Therefore, $\partial x/\partial y = -P_{12}(x,y)/P_{11}(x,y) < 0$ if and only if $P_{12}(x,y) > 0$. In other words, an organization will decrease its own

[11] A third broad class of security breach probability functions is provided in footnote 18 of [22]. One can easily demonstrate that Proposition 2 extends to security breach probability functions belonging to this additional class (modified to include the sharing variable). Thus, for this third class, CTI sharing leads to a reduction in the probability of a cybersecurity breach and an increase in social welfare.

cybersecurity investment if $P_{12}(x,y)>0$. For both $P^{I}(x,y)=v\big/\left[\alpha x(y+1)+1\right]^{\beta}$, and $P^{II}(x,y)=v^{\alpha x(y+1)+1}$, $P_{12}(x,y)>0$. Therefore, receiving CTI shared by the government agency reduces the organization's investment in cybersecurity, but increases the level of cybersecurity.

5. Implications

The model and the analysis presented in this paper demonstrate the positive role agencies such as NSA can have in increasing social welfare by publicly sharing CTI. ISACs and other cybersecurity information sharing organizations depend on the reciprocal sharing of information by members of the sharing organization, but this is not the case with sharing of information collected by a government agency and distributed freely to the public. The benefits of sharing cybersecurity information by organizations such as an ISAC are dependent on the willingness of the organization's members to share (at least some of) their privately held cybersecurity information. To show the potential benefits of sharing by such organizations, earlier papers either assumed that the organization's members would freely provide truthful cybersecurity information or assumed that incentive systems could be provided to motivate the sharing while not specifying the cost or feasibility of such an incentive system. In contrast, our analysis shows that CTI sharing by government agencies or departments will be beneficial under a wide range of general conditions without assuming that recipients of CTI share any of their privately held cybersecurity information or that incentives motivating such behavior could be provided. The sharing of cybersecurity information by government agencies or departments does not ask recipients to take actions (e.g., sharing information about successful breaches) that could possibly hurt the organization in the marketplace via the recipient's rivals. As a result, sharing CTI by government agencies or departments provides a large information sharing advantage relative to sharing organizations in terms of providing social welfare improvements.

Our analysis showed that for the broad classes of security probability functions examined, sharing CTI will benefit society if the government agency can keep their sharing costs sufficiently low. In our model, the shared CTI allowed recipient organizations to achieve the level of cybersecurity they had without the shared CTI at a reduced cost and will select cybersecurity investment levels that result in a decrease in the probability of a security breach. Hence, sharing of CTI should lead to an increase in social welfare gross of the government agency's cost of sharing the CTI. For these results to apply to government agents sharing CTI, the CTI shared must have value to the recipients as a substitute for some of the recipients' costly cybersecurity activities.

6. Concluding Remarks

Two key features of information sharing by a government agency or department distinguish the setting from the setting in which cybersecurity information is voluntarily provided by members of an information sharing organization and distributed to its membership. The two features are: 1) the absence of a free-rider problem, and 2) the absence of competition in the marketplace of the information provider (the government agency or department) with the recipients of the shared information. Due to these differences, the analysis differs from the analyses of membership-based cybersecurity information sharing organizations (e.g., the ISACs).

In contrast to the two-way arrangements where sharing can only work if firms are both providers and recipients of information, this paper examined the costs and benefits of a one-way sharing arrangement. Specifically, we examined CTI sharing in which a government agency or department is the provider of unclassified CTI, and those receiving the CTI act only as information recipients. In this context, the government agency balances cost and benefits in terms of the minimization of expected social costs or equivalently maximizing expected social welfare. Social costs consider the benefits derived by the information recipients (e.g., firms and consumers) from the shared information, as well as the government's cost of producing and distributing CTI.

Earlier models of cybersecurity sharing (e.g., [11] [12]) looked only at the total profits of the firms in the sharing organization. The analysis in this paper also considers expected losses from cybersecurity breaches to consumers. Thus, in the CTI context, a government agency's sharing of CTI that benefits all firms is neither a sufficient nor a necessary condition for the sharing of information to be beneficial. The potential benefit to consumers, in the form of a reduction in expected (externality) losses to consumers from reducing the probability of a successful breach, need not be considered by information sharing organizations focused solely on the welfare (*i.e.*, profits) of its members. In contrast, government agencies like NSA or DHS should consider this externality in making the decision regarding the sharing of CTI. That is, the reduction in the externality cost is a benefit of sharing that adds weight to the benefit side of the cost/benefit decision to share CTI.

In our model, where firms can always disregard the CTI information they receive, receiving CTI can only decrease or leave unchanged, a firm's expected cybersecurity costs (which equals their costs of cybersecurity investments plus their expected losses from a cybersecurity breach). It is possible that after receiving CTI, it may be best for each firm to reduce their cybersecurity investments without increasing the probability of a cybersecurity breach. In that case, total social costs decrease, provided that the government agency's cost of preparing and disseminating the CTI is less than the combined cost savings in cybersecurity investments by the firms receiving the CTI. Assuming the government's cost of preparing and disseminating the CTI is relatively low, an increase in social welfare should occur.

Overall, our analysis showed that there are benefits of CTI sharing by government agencies and departments. By keeping the costs of sharing the CTI sufficiently low, society will benefit from the sharing of CTI.

While we believe our economic analysis of government sharing of CTI provides new insights, the analysis is subject to limitations. Perhaps the most significant limitation of our analysis is our assumption that the information being shared by a government agency or department provide insignificant benefits to malevolent actors. The potential use of CTI by malicious actors is considered by government agencies and departments in their cost-value consideration between tipping off an adversary compared with the strengthening of broad defense. As a result, in deciding what and how to share information, government agencies and departments sometimes decide that the information is too sensitive to release to the public at a particular moment. In such a case, they limit distribution to a smaller, trusted group. This is not to say, however, that screening by government agencies and departments is perfect and that some information that is useful to malicious actors is never publicly shared. When bad actors receive CTI, the probability of a breech occurring may increase. In that case, shared CTI may have countervailing effects—decreasing the probability of a breach due to resulting increased defenses by the good recipients of the CTI and increasing the probability of a breach due to malevolent actions of the bad recipients. As long as the overall breach probability decreases, sharing CTI would be welfare increasing for sufficiently low sharing costs (*i.e.*, the sufficient condition presented would remain valid).

As with all economic models, our results are sensitive to the assumptions underlying our model. In order to show that our sufficient condition for sharing CTI to be welfare increasing does not hold vacuously, we presented two general classes of security breach probability functions such that positive amounts of shared CTI lead to a decrease in the probability of a breach. It is an open question as to how restrictive is the condition that positive amounts of shared CTI lead to a decrease in the probability of a breach. More to the point, there may be plausible security probability breach functions for which this condition does not hold. More generally, the characteristics of security breach probability functions are not observed and determining the nature of these functions remain open to empirical research. In any case, the model and analysis presented should open up avenues for further economic research into the sharing of CTI by government agencies and departments.

Acknowledgements

The authors thank two anonymous reviewers for their helpful comments. Drs. Gordon, Loeb, and Zhou thank UMD's Smith School of Business and the National Security Agency for financial support associated with this research. The views and conclusions expressed in this paper are those of the authors, and do not necessarily represent those of the Department of Defense or U.S. Federal Government.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Department of Homeland Security (DHS) (2007 October) National Strategy for Information Sharing. https://www.dhs.gov/sites/default/files/publications/10_0924_NSI_National-Strategy-Information-Sharing.pdf

[2] Sales, N.A. (2009) Share and Share Alike: Intelligence Agencies and Information Sharing. *The George Washington Law Review*, **78**, 279.

[3] Exec. Order No. 13526, 3 C.F.R. 707-731 (2010, January 5). https://www.govinfo.gov/content/pkg/FR-2010-01-05/pdf/E9-31418.pdf

[4] Kahneman, D., Sibony, O. and Sunstein, C.R. (2021) Noise: A Flaw in Human Judgment. Little, Brown. https://doi.org/10.53776/playbooks-judgment

[5] Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K. and Njilla, L. (2017) Rethinking Information Sharing for Threat Intelligence. *Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies*, San Jose, 14 October 2017, Article No. 6. https://doi.org/10.1145/3132465.3132468

[6] Clarke, R.N. (1983) Collusion and the Incentives for Information Sharing. *The Bell Journal of Economics*, **14**, 383-394. https://doi.org/10.2307/3003640

[7] Gal-Or, E. (1985) Information Sharing in Oligopoly. *Econometrica*, **53**, 329-343. https://doi.org/10.2307/1911239

[8] Kirby, A.J. (1988) Trade Associations as Information Exchange Mechanisms. Trade Associations as Information Exchange Mechanisms. *RAND Journal of Economics*, **19**, 138-146.

[9] Vives, X. (1990) Trade Association Disclosure Rules, Incentives to Share Information, and Welfare. *RAND Journal of Economics*, **21**, 409-430.

[10] Ziv, A. (1993) Information Sharing in Oligopoly: The Truth-Telling Problem. *RAND Journal of Economics*, **24**, 455-465.

[11] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003) Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, **22**, 461-485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

[12] Gal-Or, E. and Ghose, A. (2005) The Economic Incentives for Sharing Security Information. *Information Systems Research*, **16**, 186-208. https://doi.org/10.1287/isre.1050.0053

[13] Tosh, D.K., Molloy, M., Sengupta, S., Kamhoua, C.A. and Kwiat, K.A. (2015) Cyberinvestment and Cyber-Information Exchange Decision Modeling. 2015 *IEEE* 17*th International Conference on High Performance Computing and Communications*, 2015 *IEEE* 7*th International Symposium on Cyberspace Safety and Security*, and 2015 *IEEE* 12*th International Conference on Embedded Software and Systems*, New York, 24-26 August 2015, 1219-1224. https://doi.org/10.1109/HPCC-CSS-ICESS.2015.264

[14] Naghizadeh, P. and Liu, M. (2016) Inter-Temporal Incentives in Security Information Sharing Agreements. 2016 *Information Theory and Applications Workshop* La Jolla, 31 January-5 February 2016, 1-8. https://doi.org/10.1109/ITA.2016.7888179

[15] Ezhei, M. and Ladani, B.T. (2017) Information Sharing vs. Privacy: A Game Theoretic Analysis. *Expert Systems with Applications*, **88**, 327-337. https://doi.org/10.1016/j.eswa.2017.06.042

[16] Tosh, D.K., Shetty, S., Sengupta, S., Kesan, J.P. and Kamhoua, C.A. (2017) Risk Management Using Cyber-Threat Information Sharing and Cyber-Insurance. *International Conference on Game Theory for Networks*, Knoxville, 9 May 2017,

154-164. https://doi.org/10.1007/978-3-319-67540-4_14

[17] Mermoud, A., Keupp, M.M., Huguenin, K., Palmié, M. and Percia, D.D. (2019) To Share or Not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing. *Journal of Cybersecurity*, **5**, tyz006. https://doi.org/10.1093/cybsec/tyz006

[18] Rashid, Z., Noor, U. and Altmann, J. (2021) Economic Model for Evaluating the Value Creation through Information Sharing within the Cybersecurity Information Sharing Ecosystem. *Future Generation Computer Systems*, **124**, 436-466. https://doi.org/10.1016/j.future.2021.05.033

[19] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015) The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective. *Journal of Accounting and Public Policy*, **34**, 509-519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

[20] Laube, S. and Böhme, R. (2017) Strategic Aspects of Cyber Risk Information Sharing. *ACM Computing Surveys*, **50**, Article No. 77. https://doi.org/10.1145/3124398

[21] He, M., Devine, L. and Zhuang, J. (2018) Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach. *Risk Analysis*, **38**, 215-225. https://doi.org/10.1111/risa.12878

[22] Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)*, **5**, 438-457. https://doi.org/10.1145/581271.581274

[23] Matsuura, K. (2009) Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. In: Johnson, M.E., Ed., *Managing Information Risk and the Economics of Security*, Springer, Boston, 99-119. https://doi.org/10.1007/978-0-387-09762-6_5

[24] Tatsumi, K.I. and Goto, M. (2010) Optimal Timing of Information Security Investment: A Real Options Approach. In Moore, T., Pym, D. and Ioannidis, C., Eds., *Economics of Information Security and Privacy*, Springer, Boston, 211-228. https://doi.org/10.1007/978-1-4419-6967-5_11

[25] Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2014) Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security,* **6**, 24-30. https://doi.org/10.4236/jis.2015.61003

[26] Naldi, M. and Flamini, M. (2017) Calibration of the Gordon-Loeb Models for the Probability of Security Breaches. 2017 *UKSim-AMSS* 19*th International Conference on Computer Modelling & Simulation* (*UKSim*), Cambridge, 5-7 April 2017, 135-140. https://doi.org/10.1109/UKSim.2017.18

[27] Wang, S.S. (2019) Integrated Framework for Information Security Investment and Cyber Insurance. *Pacific-Basin Finance Journal*, **57**, Article ID: 101173. https://doi.org/10.1016/j.pacfin.2019.101173

Appendix

Proof of Proposition 1:

Suppose $P(x(0),0) > P(x(y),y)$. We need to show that there exists $c > 0$ such that:

$$E\left[SC(y)\right] < E\left[SC(0)\right]] \tag{A1}$$

From Equation (3), Inequality (A1) may be rewritten as

$$\begin{aligned} &n\left\{P(x(y),y)\cdot L_p + x(y) + P(x(y),y)\cdot L_e\right\} + c\cdot y \\ &> n\left\{P(x(0),0)\cdot L_p + x(0) + P(x(0),0)\cdot L_e\right\} \end{aligned} \tag{A2}$$

By rearranging the terms in (A2), one can see that we need to show that for sufficiently small $c > 0$,

$$c < \frac{n}{y}\cdot T, \tag{A3}$$

where

$$\begin{aligned} T = {} &P(x(0),0)\cdot L_p + x(0) + P(x(0),0)\cdot L_e \\ &-\left[P(x(y),y)\cdot L_p + x(y) + P(x(y),y)\cdot L_e\right]. \end{aligned} \tag{A4}$$

If $T > 0$, then Inequality (A3) holds for sufficiently small $c > 0$. Thus, to complete the proof we need to show $T > 0$. Again, rearranging terms, Equation (A4) can be written as:

$$\begin{aligned} T = {} &\left[P(x(0),0)\cdot L_p + x(0)\right] - \left[P(x(y),y)\cdot L_p + x(y)\right] \\ &+\left[P(x(0),0)\cdot L_e - P(x(y),y)\cdot L_e\right]. \end{aligned} \tag{A5}$$

Given that the proposition assumes $P(x(0),0) > P(x(y),y)$, the third term in brackets in (A5) is positive. Thus, to show that T is positive, we need only show:

$$P(x(0),0)\cdot L_p + x(0) \ge P(x(y),y)\cdot L_p + x(y). \tag{A6}$$

Since increasing the level of shared CTI is assumed to decrease or have no effect on the probability of cybersecurity breach (*i.e.*, $P_2(x(y),y) \le 0$), we have:

$$P(x(0),0)\cdot L_p + x(0) \ge P(x(0),y)\cdot L_p + x(0), \tag{A7}$$

and from the definition of $x(y)$ as given in Equation (1), we have:

$$P(x(0),y)\cdot L_p + x(0) \ge P(x(y),y)\cdot L_p + x(y). \tag{A8}$$

By combining Inequalities (A7) and (A8), we have demonstrated Inequality (A6), thereby completing the proof.■

Proof of Proposition 2:

The first-order condition for x to solve the minimization specified in Equation (1) is $P_1(x,y)L + 1 = 0$. Thus, for $P^{I}(x,y) = \frac{v}{\left[\alpha x(y+1)+1\right]^{\beta}}$ the first-order condition yields:

$$\frac{\partial P^{I}\left(x,y\right)}{\partial x}=-\frac{v\beta\alpha\left(y+1\right)}{\left[\alpha x\left(y+1\right)+1\right]^{\beta+1}}=-\frac{1}{L}. \tag{A9}$$

Hence, we have

$$x\left(y\right)=\frac{\left[Lv\beta\alpha\left(y+1\right)\right]^{\frac{1}{\beta+1}}-1}{\alpha\left(y+1\right)}, \tag{10}$$

and

$$P^{I}\left[x\left(y\right),y\right]=\frac{v}{\left[Lv\beta\alpha\left(y+1\right)\right]^{\frac{\beta}{\beta+1}}}. \tag{A11}$$

Thus, it follows that for $y>0$, $P^{I}\left[x\left(y\right),y\right]<P^{I}\left[x\left(0\right),0\right]$.

For $P^{II}\left(x,y\right)$ the first order condition yields:

$$\frac{\partial P^{II}\left(x,y\right)}{\partial x}=\alpha\left(y+1\right)\ln\ln v\cdot v^{\alpha x\left(y+1\right)+1}=-\frac{1}{L}. \tag{A12}$$

Hence, we have

$$x\left(y\right)=\frac{\ln\ln\left[\frac{-1}{\alpha\left(y+1\right)vL\ln\ln v}\right]}{\alpha\left(y+1\right)\ln\ln v}, \tag{A13}$$

and

$$P^{II}\left[x\left(y\right),y\right]=v^{\frac{\ln\ln\left[\frac{-1}{\alpha\left(y+1\right)L\ln\ln v}\right]}{\ln\ln v}}. \tag{A14}$$

Consequently, for $y>0$, $P^{II}\left[x\left(y\right),y\right]<P^{II}\left[x\left(0\right),0\right]$. Hence, by Proposition 1, we have that for sufficiently small $c>0$, $E\left[SC\left(y\right)\right]<E\left[SC\left(0\right)\right]$.■