JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–12
https://doi.org/10.1093/cybsec/tyad003
Research paper

Research paper

Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments

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

[1]Office of Innovation, National Security Agency, Ft. George G. Meade, MD 20755, USA and [2]Department of Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland, College Park, MD 20742, USA

*Correspondence address. 7699 Mowatt Lane, College Park, MD 20742, USA. Tel: +1-301-405-2209; E-mail: mploeb@umd.edu

†Although the authors are listed in alphabetical order, they wish it to be known that the four authors should be regarded as co-first authors.

Received 15 June 2022; revised 21 November 2022; accepted 14 February 2023

Abstract

The primary objective of the current study is to analytically examine the economic benefits an organization can obtain by receiving and processing cyber threat intelligence (CTI) shared by the US government. Our results show that the benefits from receiving CTI are closely associated with the difference between the threat level indicated by the CTI and the receiving organization's prior belief of the threat level. In addition, for the same difference between the threat levels indicated by the CTI and the organization's prior belief, our analyses show that the magnitude of adjustments to an organization's cybersecurity investments is inversely related to the organization's prior belief of the threat level. Thus, larger benefits can be obtained when the receiving organization's prior belief of a threat level is lower. Taken together, our results suggest that the common belief that it is optimal for a federal government agency or department to focus on sharing CTI related to vulnerabilities with the highest threat level is misguided. More generally, the benefits from CTI sharing can be improved if producers of CTI could develop a clearer understanding of the prior beliefs that organizations have concerning their threat level and focus on sharing CTI that is significantly different from those prior beliefs.

Key words: cyber threat intelligence, economics of information sharing, cybersecurity investment

Introduction

As cyber breaches grow ever more prevalent, cybersecurity becomes a day-to-day struggle for most organizations. Security experts have long argued that sharing cyber threat intelligence (CTI) is essential to defend against cyberattacks.[1] Industry-specific Information Sharing and Analysis Centers (ISACs) are nonprofit organizations introduced and promoted by President Clinton in ref. [2] in 1998 to facilitate information sharing related to cybersecurity. By 2019, the National Council of ISACs listed 21 member ISACs, including those for financial, automotive, energy, aviation, communications, and defense industrial base sectors. Information Sharing and Analysis Organizations (ISAOs) were initiated by President Obama's Executive Order (EO) 13691 [3] in 2015, which directed the Department of Homeland Security (DHS) to "strongly encourage the development and formation" of ISAOs.[2] Whereas ISACs are based on specific industries,

1 Based on a survey of IT practitioners whose organizations use threat intelligence as part of their cybersecurity program, the Ponemon Institute's report [1, p. 2] states that "Threat data feeds are important to an organization's cybersecurity strategy… Respondents believe an average of 50% of attacks can be stopped from intelligence threat feeds."

2 See ref. [4].

ISAOs are information-sharing groups that are not industry-specific. Despite the developments with ISACs and ISAOs, a survey of the literature by Pala and Zhuang [5] shows that organizations are reluctant to share cybersecurity-related information because they are concerned about privacy and civil liberties, legal liability, loss of trust and reputation (which could result in loss of market share), information leakage, and sharing costs (which impact profits). It should be noted, however, that Mermoud *et al.* [6] found that a positive attitude toward security information sharing and social/transactional reciprocity are positively associated with the frequency and/or intensity of security information sharing between ISAC members.

The demand for cyber intelligence has also created a prosperous commercial market. According to Gartner [7] research, "Different price points may be available for different tiers of service … Pricing for annual subscriptions can range from the low tens of thousands of dollars for basic services up to $500,000 or more for sophisticated offerings… ."

An estimate of the threat intelligence subscription costs is also given by TechTarget. In the company's buyer's guide to the security threat intelligence services, TechTarget states that "the cost of a data feed subscription varies from company to company but is in the range of roughly $1,500 to $10,000 per month, depending on the number of data feeds in the subscription. Some services require customers to buy their security devices along with a threat intelligence data feed subscription, which can add thousands of dollars to overall costs."[3,4]

The Cybersecurity and Infrastructure Security Agency (CISA), which is part of the DHS, is the lead US federal government agency for managing and reducing the risk of the nation's cyber and physical infrastructure. CISA notes that "… information sharing is essential to the protection of critical infrastructure and to furthering cybersecurity for the nation."[5] Government agencies and departments are in a unique position to share CTI. More to the point, government agencies and departments, such as the National Security Agency (NSA) and DHS, routinely collect a large volume of cyber threat information and possess exceptional expertise in cyber threat analysis. Unlike private companies, the government sharing of unclassified CTI to the public[6] is not profit motivated and therefore not inhibited by concerns of erosion of market share and loss of profits. Thus, reciprocal sharing of information is not an impediment to sharing unclassified CTI. Furthermore, confidentiality is not at issue in the case of a federal government agency or department sharing authorized unclassified information with the public (i.e. by definition, unclassified information does not require the designation of confidential).

In contrast to government agencies and departments sharing unclassified information, private sector firms belonging to an information-sharing organization are concerned with the confidentiality (i.e. privacy) issue associated with shared information. In addition, private sector firms are concerned with the fact that the costly sharing of information will not be reciprocated by competitor firms in the sharing organization (i.e. the free-rider problem is a fundamental concern to private sector organizations when participating in an information sharing organization). The free-rider problem does not, however, pose a problem in government agencies or departments as it does in private sector firms. Moreover, given that much of the information being shared by a government agency or department is already being collected for other purposes (e.g. national security), the unclassified portion of the information can be shared with the public at a nominal cost.

The above notwithstanding, according to the report by DHS Office of Inspector General [11], CTI sharing by the government agencies and departments in the Automated Indicator Sharing (AIS) program[7] is limited and ineffective. The problems with CTI sharing by the government are not limited to the AIS platform. Dykstra *et al.* [13] interviewed individuals/groups who receive CTI from NSA and found that the key challenges preventing the CTI recipients from more efficient use of the CTI are the time and resources involved in processing the received information, as well as issues associated with identifying the proper use of such information. Gartner [7] research expresses similar sentiments to ref. [13]. Based on a case study of two cybersecurity exercises focused on threat intelligence sharing, Brilingaite *et al.* [14] identified "… nine significant factors negatively impacting prioritization and execution of RIS (reporting and information-sharing) tasks due to overly focused attention on technical tasks, insufficient knowledge of information-sharing importance, standards and tools, and unclear benefits of these skills."

Unfortunately, little is known about the extent to which sharing CTI directly or indirectly prevents cyber incidents. In the 2020 SANS CTI industry survey, 82% of respondents believe that CTI provides value, but only 4.2% of the respondents measure its effectiveness [15]. In contrast to the negative findings regarding CTI sharing, anecdotal evidence of improved cybersecurity from CTI sharing has been documented [16].

There are many reasons why shared CTI may not result in the desired outcome. For example, the plethora of CTI available can impose significant processing costs for organizations that wish to use the information. When the volume of the CTI available exceeds an organization's capacity to fully process the CTI, information overload (or what some call information processing fatigue) can take place.[8] Furthermore, many CTI data feeds lack context about the threat and confidence levels in the intelligence, Thus, those charged with leading a firm's cybersecurity efforts need to identify the CTI relevant to their organizations, contextualize how the CTI can be used in their organization's cybersecurity scenarios, and figure out the best course of action based on the CTI. As a result of the issues noted above, CTI received by organizations is often inefficiently incorporated into an organization's cybersecurity decisions.

The primary objective of the current study is to analytically examine the economic benefits an organization can obtain by receiving and processing CTI, with a focus on unclassified CTI provided free of charge by a US government agency or department. We are particularly interested in identifying the conditions that increase the economic benefits an organization can obtain from receiving and processing CTI.

Our results show that the benefits derived from receiving and processing CTI by an organization are closely associated with the differ-

3 See ref. [8].

4 For a list of some of the top companies providing CTI solutions, see ref. [9].

5 See ref. [10].

6 The US federal government designates information as classified, unclassified for official use only, and unclassified. The focus of this study is only on unclassified information that is authorized for release to the public.

7 AIS, a CISA capability, enables the real-time exchange of machine-readable cyber threat indicators and defensive measures to help protect participants of the AIS community and ultimately reduce the prevalence of cyberattacks; see ref. [12].

8 Bawden and Robinson [17, p. 182–3] note that "There is no single generally accepted definition of information overload. The term is usually taken to represent a state of affairs where an individual's efficiency in using information in their work is hampered by the amount of relevant, and potentially useful, information available to them."

ence between the threat level suggested by the CTI and the receiving organization's prior belief concerning the threat level. For example, sharing CTI about the Conti ransomware may provide limited benefits if the cybersecurity community is already aware of the threat.[9] If, however, new details or context substantially updates public knowledge, then the CTI carries added value. In addition, the magnitude of adjustments to an organization's cybersecurity investments is inversely related to the organization's prior belief of the threat level. In other words, larger adjustments to cybersecurity investments will take place when the organization's prior belief of the threat level is lower. Taken together, our results suggest that the common belief that it is optimal for a federal government agency or department to focus on sharing CTI related to vulnerabilities with the highest threat level is misguided. More generally, the benefits from CTI sharing can be improved if producers of CTI could develop a clearer understanding of the prior beliefs that organizations have concerning their threat level and focus on sharing CTI that is significantly different from those prior beliefs.[10]

The major contributions of this paper are 2-fold. First, we provide new insights into the relationships among an organization's prior belief concerning the cyber threat level, the threat level indicated by government provided CTI, and an organization's cybersecurity investments. Second, this paper contributes to an understanding of how the difference between the threat level indicated by the CTI and the organization's prior belief affects benefits obtained from receiving and processing CTI.

The remainder of this paper will proceed as follows. In the next section, we provide a brief review of the prior literature on information sharing. In the third section of the paper, we provide an analysis of the benefits derived from a government agency or department sharing CTI, based on an economic model and information theory. In the third section of the paper, we also provide a numerical example to illustrate the findings from our analysis. The fourth section of the paper discusses the implications of our analysis. The fifth, and final, section of the paper provides some concluding comments.

Literature review

Early studies in the economics literature on information sharing focused on how information sharing could improve profits for private sector firms involved in information sharing arrangements [19, 20]. These papers addressed a variety of issues, including the type of information shared (e.g. product cost-related information and/or product demand-related information), the type of market competition (e.g. oligopoly, duopoly, etc.) in which the organizations sharing information operate, and whether the organizations sharing information sell products that are substitutes or complements. Issues related to the free-rider problem and the truth-telling problem have also been subjects of concern in the economics-based literature on information sharing [21].

Focus on the economics of sharing CTI information among private sector organizations did not take place until the beginning of the 21st century in response to the cyber threats and cybersecurity breaches emanating from the Internet.[11] Gordon *et al.* [24] and Gal-Or and Ghose [25] were among the earliest studies to address the cost–benefit aspects of sharing cybersecurity-related information. Both papers, however, found that, without additional economic incentives, the free-rider problem is a serious impediment to realizing the potential welfare benefits associated with information sharing among private sector firms.

More recent analytical papers investigate the incentives necessary to alleviate free-riding and encourage information sharing within information sharing organizations/platforms. Tosh *et al.* [26], for example, focus on incentive schemes that allow participants to share information anonymously. Naghizadeh and Liu [27] show how an imperfect public monitoring system can enhance truthful sharing of cyber threat and remediation information in an infinitely repeated game. Incorporating the incentives of both attackers and defenders, Ezhei and Ladani [28] use a two-stage sequential game to analyze benefits of a sharing organization when firms explicitly consider privacy costs. Gao and Zhong [29] and Hausken [30] also model both attackers and defenders using multistage game theoretic models. Gao and Zhong [29] demonstrate that the levels of investment by both defenders and attackers, as well as the level of sharing among defenders, depend on the type of competition (e.g. Cournot *vs* Bertrand competition) assumed. Hausken [30] analyzes information sharing among hackers who have to trade off between sharing information and launching costly attacks. Using an evolutionary game, Tosh *et al.* [31] propose a dynamic incentive structure through which a sharing organization can be self-sustained when it attracts a sufficient number of firms to share information.

Applying a real options analysis, Gordon *et al.* [32] find that sharing cybersecurity information could have the effect of incentivizing the receiving entity to accelerate investments in cybersecurity. Their findings arise from the fact that information sharing can reduce the risk associated with a firm's decision to invest in the current period, rather than exercising the real option to defer cybersecurity investments. The paper includes a hypothetical example that is used to illustrate their argument.

There have also been several review papers that explore various economic aspects of cybersecurity information sharing among various organizations (e.g. [5, 33, 34]). Laube and Böhme [33], for example, perform an extensive survey of theoretical and empirical literature and conclude that, in general, a firm's economic incentives lead them to share less cybersecurity information than is socially optimal. Pala and Zhuang [5] review 82 papers from technology, policy, and economic fields and identify the primary concerns in cybersecurity information sharing. These concerns include privacy and civil liberties, liability, loss of trust, loss of reputation, attracting more attacks, information leakage, and sharing costs.

The potential benefits derived from sharing cyber threat-related information have also been extensively discussed by the US federal government. As already mentioned in the Introduction, President Clinton's Presidential Decision Directive/NSC-63 [2] in 1998 was intended to facilitate information sharing among private sector and public sector organizations. However, the developments with the Internet in the mid-to-late 1990s, and the terrorists' attacks in the USA on 11 September 2001, combined to create a new sense of urgency concerning sharing CTI. Consequently, in 2004, President Bush issued Executive Order 13356 [35], which focused on threat-related information regarding terrorism. In 2012, the "National Strategy for Information Sharing and Safeguarding" [36] was published by The

9 Conti is a ransomware variant first observed in May 2020 and used in >400 attacks across the world. CISA issued an alert about Conti on 22 September 2021 [18].

10 Although the focus of this paper is on the US federal government as provider of CTI, the same argument would apply to commercial vendors that provide CTI. More will be said about private sector vendors that provide CTI later in the paper.

11 There is a large body of literature on the impact of cybersecurity breaches on the stock market value of firms (e.g. [22, 23]).

White House under President Obama. In 2013, President Obama issued Executive Order 13636 [37], in which Section 4, part (a), specifically states that: "It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats." Even with this acknowledgement for higher quality CTI, the goal remains elusive.

The Cybersecurity Information Sharing Act of 2015 [38] also focused on improving "… cybersecurity in the United States through enhanced sharing of information about cybersecurity threats…" In response to the Cybersecurity Information Sharing Act of 2015, in 2018, DHS established the CISA. CISA developed and maintains the AIS program, which is intended to facilitate the sharing of CTI among government and private sector entities.[12] In October 2016, the National Institute of Standards and Technology (NIST) issued its Special Publication 800–150 entitled "Guide to Cyber Threat Information Sharing," which "… provides guidance to help organizations exchange cyber threat information."[13,14]

Although recognizing the potential benefits from sharing cyber-related information among private sector firms (either directly as in the case of supply-chain partners or via an information sharing organization such as an ISAC), the literature on sharing cybersecurity-related information among private sector organizations continues to highlight the free-rider problem, as well as the concerns related to competition for market share and profits. Issues related to confidentiality (i.e. privacy) also remain as fundamental concerns among private sector organizations.[15] Despite these barriers, there are clearly many examples of successful information sharing among private sector organizations (e.g. see the IT-ISAC blog for a description of several success stories [41]).

Many of the barriers to information sharing among private sector organizations do not, however, apply to sharing unclassified CTI by the government. US federal government agencies and departments are not competing with private sector companies for customers. In addition, sharing CTI does not involve the risk of losing revenues due to the loss of trust or reputation as in the case of private companies. Hence, the US federal government is in a unique position to share a large volume of cybersecurity information at a nominal cost, providing it is already collecting such information to fulfill its organizational mission. The above notwithstanding, there is evidence to suggest that much of the information provided by federal government agencies and departments is either not used or used in an inefficient manner (e.g. see refs. [42] and [11]). In this regard, the report by the Office of Inspector General, which focused on evaluating DHS' progress in improving information sharing in accordance with the Information Sharing Act of 2015, noted that CISA "… made limited progress improving the overall quality of information it shares with AIS participants to effectively reduce cyber threats and protect against attacks" [11, p. 6].

The economics-based literature on sharing cyber-related information previously discussed examined sharing information among firms. Such sharing was sometimes facilitated by an information sharing organization that was organized with or without the support of the government. While the literature on sharing cyber information among firms includes several papers that incorporate an analytical economic model, there has been a paucity of economic modeling of information sharing between the government and firms in the private sector.[16] One exception is Laube and Böhme [44] who construct a principal–agent model to study security breach reporting to the government. Another exception is Dykstra *et al.* [42] who use an economic model to examine sufficient conditions for a government agency's sharing of CTI to private sector firms to increase social welfare. Unlike this paper, Dykstra *et al.* [42] do not examine of how the difference between the threat level indicated by the CTI and a recipient firm's prior belief affects benefits obtained from a government agency's shared CTI. To the best of our knowledge, our paper is the first to identify conditions when sharing CTI by a government agency is most beneficial.

According to a survey by the Ponemon Institute [45, p. 9] of IT practitioners whose organizations use threat intelligence as part of their cybersecurity program, only 17% of respondents consider ISAC/ISAO as the primary source of CTI for their organizations, and only 15–18% of respondents indicate a government sharing program as the primary source. This may, in part, be due to information overload and resource constraints (e.g. related to processing capacity) of the organizations (especially small- and medium-size organizations) receiving the threat information provided by commercial vendors and the government. In the 2021 Poneman Institute survey [1], 56% of the respondents agree that "threat feeds provide threat data that is often too voluminous and/or complex to provide timely and actionable intelligence." In this regard, Schick *et al.* [46, p. 206] argue that information overload occurs for "… an individual when the information processing demands on time … to perform interactions and internal calculations exceed the supply or capacity of time available … for such processing." Anderson and Palma [47] formally model information congestion in an advertising scenario and propose incentive schemes to improve social welfare.

The literature reviewed above indicates that the potential benefits of sharing government-collected CTI are widely acknowledged. Nevertheless, while a significant proportion of recipients of government-supplied CTI find some benefits from having received the CTI, the literature also clearly indicates that impediments exist (e.g. information overload and resource constraints) that prevent receiving organizations from realizing the full potential benefits of CTI sharing. However, even without directly addressing these impediments, there are ways of analytically examining methods for improving the economic benefits associated with government agencies or departments sharing unclassified CTI. Accordingly, in the following section of this paper, we provide an economic model and analysis that identifies conditions when sharing CTI by a federal government agency or department is most beneficial.

Assessing the benefits of CTI

Generic model

Assume an organization has intelligence on the cyber threat level related to a security vulnerability.[17] We denote the threat intelligence as p, where $0 < p \leq 1$ represents the best estimate of the probability

12 For a detailed description of CISA, see ref. [39].

13 The NIST publication provides an excellent discussion of the benefits and challenges associated with information sharing [40].

14 The above are just a few of a very long list of the US federal government publications concerned with sharing CTI.

15 The GDPR (General Data Protection Regulation), which is a regulation in the European Union and the European Economic Area, is a clear manifestation of the need for private sector organizations to be concerned about the privacy of data, whether or not the information is shared.

16 Although there is an extensive literature on CTI modeling (e.g. [43]), the models presented are not analytical economic models.

17 For simplicity, we assume that a threat is related to one and only one vulnerability.

that a hacker will initiate a cyberattack exploiting the vulnerability. An organization can decrease the chance of the attack being successful by investing in cybersecurity activities that reduce the vulnerability. We adopt a similar setting to Gordon and Loeb [48] and denote the productivity function of cybersecurity investments reducing a vulnerability as $s(z, v)$, where $v \in (0, 1)$ represents the inherent probability that a cyberattack exploiting the vulnerability will be successful if an organization does not make any investment to reduce the vulnerability, i.e. $s\ (0, v) = v$. The organization will choose z, the amount of cybersecurity investments it makes to reduce the vulnerability. Following Gordon and Loeb [48], we assume that investment in cybersecurity decreases the chance that a cyberattack will be successful, but at a decreasing rate, i.e. $s_z = \frac{\partial s}{\partial z} < 0$ and $s_{zz} = \frac{\partial^2 s}{\partial z^2} > 0$.[18] In this setting, the probability of an organization being breached due to a vulnerability is the product of the probability that an attack will take place and the probability that the attack will be successful, i.e. $p \cdot s(z, v)$.[19]

Before receiving and processing any CTI, an organization has its own belief of the threat level (i.e. the probability that a hacker will engage in a cyberattack exploiting a given vulnerability of the organization). Such belief may be formed from analyzing the organization's own past experiences, receiving intelligence from ISACs/ISAOs or in the news media, and/or purchasing intelligence services from commercial vendors. We denote the organization's prior belief before receiving CTI shared by the government as $\tilde{p}$, i.e. the organization believes the probability that a hacker will attack a given vulnerability is $\tilde{p}$. Based on the prior belief, the organization would invest in cybersecurity activities defending the vulnerability, and hence minimize the total expected cybersecurity costs. Formally stated, the organization will solve the following minimization problem:

$$\min_z \left[\tilde{p} \cdot s\,(z, v)\, L + z\right] \text{ s.t. } z \geq 0, \tag{1}$$

where L is the amount of loss the organization will suffer, assuming a cyber breach were to occur.

If the organization receives and processes intelligence on a vulnerability, it will update its belief of the threat level regarding the vulnerability from $\tilde{p}$ to p, and adjust its investment level accordingly.[20] In other words, the organization will solve the following minimization problem instead:

$$\min_z \left[p \cdot s\,(z, v)\, L + z\right] \text{ s.t. } z \geq 0 \tag{2}$$

Notice that the optimal investment in reducing the vulnerability depends on the CTI the organization receives and processes. Let the optimal investment in reducing a given vulnerability before the organization processes the CTI on that vulnerability shared by the government be $\tilde{z}$ and the optimal investment in reducing the same vulnerability after the organization processes the intelligence shared by the government be z^*. The optimal investments, $\tilde{z}$ and z^*, are functions of the threat levels, which can be written as

$$\tilde{z}\ (\tilde{p}) = \operatorname{argmin}\left[\tilde{p} \cdot s\,(z, v)\, L + z\right], \tag{3}$$

$$z^*\ (p) = \operatorname{argmin}\left[p \cdot s\,(z, v)\, L + z\right]. \tag{4}$$

We now introduce **Lemma 1**, which describes how the optimal investment changes with respect to the intelligence on threat level.

Lemma 1

The optimal amount to invest in reducing a vulnerability increases in the probability that an organization believes a hacker will exploit the vulnerability, i.e. $z^*(p)$ increases in p. In the special case where $p = 0$, the optimal investment amount is 0.[21]

Proof:

For the minimization problem $z^* = \operatorname{argmin}[\mathrm{p} \cdot \mathrm{s}(\mathrm{z}, \mathrm{v})\mathrm{L} + \mathrm{z}]$, the below first-order condition needs to be satisfied:

$$p \cdot s_z\left(z^*\right) L + 1 = 0. \tag{5}$$

Based on Equation (5), we can calculate the derivative of the optimal z with respect to p as follows:

$$z_p^* = \frac{dz^*}{dp} = -\frac{s_z\,(z^*)}{s_{zz}\,(z^*)\,p} = \frac{1}{s_{zz}\,(z^*)\,p^2 L}. \tag{6}$$

Given that $s_{zz} > 0$, we have

$$z_p^* > 0. \tag{7}$$

When $p = 0$, $p \cdot s(z, v)L = 0$, the organization's total expected costs related to cybersecurity $p \cdot s(z, v)L + z$ is minimized when $z = 0$. ■ □

Lemma 1 shows that an organization will invest more in reducing a vulnerability if it believes that an attack targeting that vulnerability is more likely to happen. However, the CTI that reveals a lower threat level than the organization previously thought would lead the organization to reduce the investment needed to address this vulnerability. A closer examination of Equation (6) also reveals that the changes in investment level will be larger if the investment has higher productivity and lower diminishing return. Overall, z_p^* represents how sensitive the optimal investment is to changes in an organization's belief of the threat level.

We further analyze the changes in the optimal amount to invest to reduce a vulnerability in Proposition 1.

Proposition 1

For three broad classes of productivity functions described in Gordon and Loeb [48],[22] the optimal amount to invest in reducing a vulnerability increases in the threat level at a decreasing rate. That is, if $s(z, v)$ takes any of the following functional forms: $s^I\ (z, v) = \frac{v}{(\alpha z+1)^\beta}$, $s^{II}\ (z, v) = v^{\alpha z+1}$, or $s^{III}\ (z, v) = ve^{\alpha z(v-1)}$, where $\alpha > 0$ and $\beta \geq 1$, then z_p^* decreases in p.[23]

Proof:

It can be easily shown that □

for $s^I\ (z, v) = \frac{v}{(\alpha z+1)^\beta}$, $\frac{dz_p^*}{dp} = -\frac{\beta(\alpha\beta v L p)^{1/(1+\beta)}}{p^2\alpha(1+\beta)^2} < 0$;

for $s^{II}\ (z, v) = v^{\alpha z+1}$, $\frac{dz_p^*}{dp} = \frac{1}{p^2\alpha ln(v)} < 0$, since $v < 1$;

for $s^{III}\ (z, v) = ve^{\alpha z(v-1)}$, $\frac{dz_p^*}{dp} = \frac{1}{p^2\alpha(v-1)} < 0$, since $v < 1$. ■

(Appendix A provides derivations of the above derivatives.)

Proposition 1 shows that, for the above three broad classes of productivity functions of cybersecurity investments, when an orga-

18 Our setting is different from that of Gordon and Loeb [48]. Gordon and Loeb [48] refer the probability that a breach will take place as vulnerability (i.e. they incorporate threat into their notion of vulnerability). We separate the probability of a breach into the threat p (the probability that a hacker will engage in an attack) and the vulnerability v (the chance that an attack will be successful).

19 In essence, $s(z, v)$ represents the revised vulnerability after investment z.

20 For simplicity, we use p to represent both the threat level indicated in the shared CTI and the organization's posterior belief. A more general scenario is that after receiving CTI shared by the government, the organization's belief will move away from its prior and toward, but not necessarily completely all the way to, the threat level indicated by the CTI. That is, the organization's posterior probability of a threat may be modeled as $p^{\text{Posterior}} = \tilde{p} + \theta(p - \tilde{p})$, for $0 < \theta \leq 1$. By assuming $\theta = 1$, the analysis is less cumbersome without affecting our results qualitatively.

21 Note that given $z^* \geq 0$, we run into a corner solution where $z^* = 0$ for very small p. Our discussion focuses on the interior solutions where $z^* > 0$.

22 The Gordon–Loeb model of cybersecurity investment has been widely studied (e.g. [49]).

23 Appendix B provides a sufficient condition that generalizes Proposition 1.

nization's prior belief of threat level on a vulnerability is higher, it will increase its investment level less aggressively in responding to a CTI that increases the threat level. This is because the organization has invested a greater amount when it believes the threat level is higher and further investments produce a smaller reduction of the vulnerability. As a result, the reduction in expected loss from a cyber breach is also smaller when an organization's prior belief of threat level is high. Contrary to the notion that CTI providers should focus on alerting organizations about cyber threats with the highest threat levels, prioritizing sharing CTIs on vulnerabilities that organizations have a prior belief of low threat level may induce larger increases in cyber investment and result in greater improvement of security level.

The benefits an organization obtains from receiving CTI on a vulnerability are not limited to improved cybersecurity level. Having better CTI can also result in a reduction in total expected cybersecurity costs related to a vulnerability, which is the sum of the expected loss from cyber breach and cybersecurity investment. We denote the benefits obtained by an organization from receiving and processing the threat intelligence on a vulnerability as G, where

$$G = [p \cdot s(\tilde{z}, v) L + \tilde{z}] - [p \cdot s(z^*, v) L + z^*]. \quad (8)$$

Notice that when $p = \tilde{p}$, $z^* = \tilde{z}$, an organization does not need to take any actions and receives no benefit from receiving and processing the intelligence if the CTI is identical to its prior belief, i.e. $G = 0$ if $p = \tilde{p}$.

Proposition 2

G increases in $p - \tilde{p}$ when $p > \tilde{p}$, and G increases in $\tilde{p} - p$ when $p < \tilde{p}$.[24]

Proof:

Let $\delta = p - \tilde{p}$ and $G = [p \cdot s(\tilde{z}, v)L + \tilde{z}] - [p \cdot s(z^*, v)L + z^*]$, we can rewrite G as

$$G = [p \cdot s(\tilde{z}(p - \delta), v) L + \tilde{z}(p - \delta)] - [p \cdot s(z^*(p), v) L + z^*(p)],$$

$$\frac{dG}{d\delta} = -p \cdot s_z(\tilde{z}, v) \tilde{z}_p L - \tilde{z}_p = -\tilde{z}_p [p \cdot s_z(\tilde{z}, v) L + 1]. \quad (9)$$

Combining Equation (9) with Equations (5) and (6), it follows that

$$\frac{dG}{d\delta} = -\tilde{z}_p \cdot \delta \cdot s_z(\tilde{z}, v) L = -\frac{\delta \cdot s_z(\tilde{z}, v)}{s_{zz}(\tilde{z}, v)(p - \delta)^2}. \quad (10)$$

Given that $s_z < 0$ and $s_{zz} > 0$, we have $\frac{dG}{d\delta} > 0$ when $\delta > 0$, and $\frac{dG}{d\delta} < 0$ when $\delta < 0$. Hence, G increases in $p - \tilde{p}$ when $p > \tilde{p}$, and G increases in $\tilde{p} - p$ when $p < \tilde{p}$. ■ □

Proposition 2 shows that the benefit obtained from receiving and processing CTI for a vulnerability depends on the difference between the threat level indicated by the CTI and an organization's prior belief. As indicated in Lemma 1, if the CTI indicates that the threat level is lower than the organization's prior belief, the organization will decrease the investment level. This would result in a higher chance that a breach will take place, but the organization will save on cybersecurity expenditure and reduce the total cybersecurity related costs. In other words, an organization will always benefit from updating its prior belief to the CTI shared by the government, regardless of whether the CTI increases or decreases the organization's belief of threat level. The magnitude of the benefits depends on how different the CTI is from an organization's prior belief concerning cyber threats.

A closer examination of Equation (10) and Equation (6) reveals that the marginal benefit from receiving and processing CTI ($\frac{dG}{d\delta}$) can also be written as

$$\frac{dG}{d\delta} = \frac{\delta \cdot \tilde{z}_p}{\tilde{p}}. \quad (11)$$

This suggests that the marginal benefit from receiving and processing CTI increases with the sensitivity of optimal cyber investments to the threat level and decreases with the prior belief of threat level. Recall that Proposition 1 shows that the optimal cybersecurity investment increases with the threat level at a decreasing rate. Equation (11) implies that, for the same difference between the threat level in the CTI and the prior belief by the receiving organization, the benefits tend to be smaller when the receiving organization's prior belief indicates a higher threat level. In other words, CTI sharing tends to be the most beneficial when the receiving organization had very little (in the extreme, no) prior awareness about a threat.[25]

Comparison to results from information theory

The benefit from receiving CTI analyzed in Proposition 2 is closely related to the concept of Kullback–Leibler Divergence in information theory [50]. The Kullback–Leibler Divergence, also referred as the relative information entropy, measures the information gained by revising one's beliefs from a prior probability distribution to a posterior probability distribution. In the situation where an organization revises its belief of the threat level from $\tilde{p}$ to p, the Kullback–Leibler Divergence D_{KL} can be formally written as

$$D_{KL}(p\tilde{p}) = p \log \frac{p}{\tilde{p}} + (1 - p) \log \frac{(1 - p)}{(1 - \tilde{p})}. \quad (12)$$

Note that $D_{KL} > 0$ for any $p \neq \tilde{p}$. Similar to G, D_{KL} increases in $p - \tilde{p}$ when $p > \tilde{p}$ and increases in $\tilde{p} - p$ when $p < \tilde{p}$.

Note that D_{KL} is symmetric, i.e. the information gained calculated using the Kullback–Leibler Divergence depends only on the relative levels of threat indicated in the CTI and prior belief. To see this, notice that $D_{KL}(p\tilde{p}) = D_{KL}(1 - p1 - \tilde{p})$. In order words, updating posterior belief $p = 0.9$ from prior belief $\tilde{p} = 0.1$ will result in same relative information entropy as updating posterior belief $p = 0.1$ from prior belief $\tilde{p} = 0.9$. This is because the calculation of Kullback–Leibler Divergence in the CTI sharing scenario measures only the changes in CTI but does not consider how an organization would adjust the optimal cybersecurity investments based on the CTI shared. Due to the diminishing return of cybersecurity investments, difference in CTI does not translate uniformly to difference in the organization's cybersecurity investment. More specifically, organizations with prior belief that indicates a lower threat level enjoy higher marginal benefits from their further cybersecurity investments, hence will receive higher economic benefits from CTI shared by the government departments and agencies. As a result, the economic benefits from receiving CTI are not symmetric as the Kullback–Leibler Divergence. In the domain of CTI sharing, the decision-making process has been focusing on the CTI to induce the biggest revision of beliefs. Our results show that CTI provides should explicitly take the changes in investment into consideration to maximize the benefits of CTI sharing.

24 We choose to state the proposition in the current way to facilitate later discussion of the results. We can further show that G is a convex function of $p - \tilde{p}$, which achieves its minimum level when $p = \tilde{p}$. The proof is provided in Appendix C.

25 An analogy can be found in the public health domain. Significant improvements in public health can be achieved by informing people of the basic health risks and hygiene practices, which can be more cost-effective in improving the population's life expectancy than investing in advanced health care targeting terminal diseases.

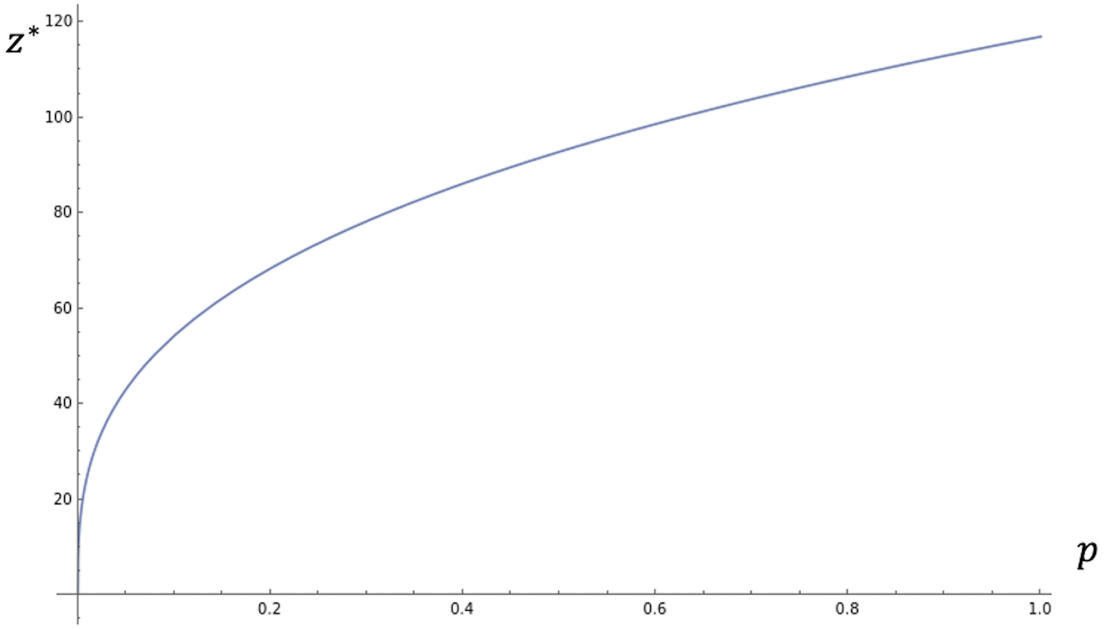

Figure 1: The optimal investment *vs* threat level.

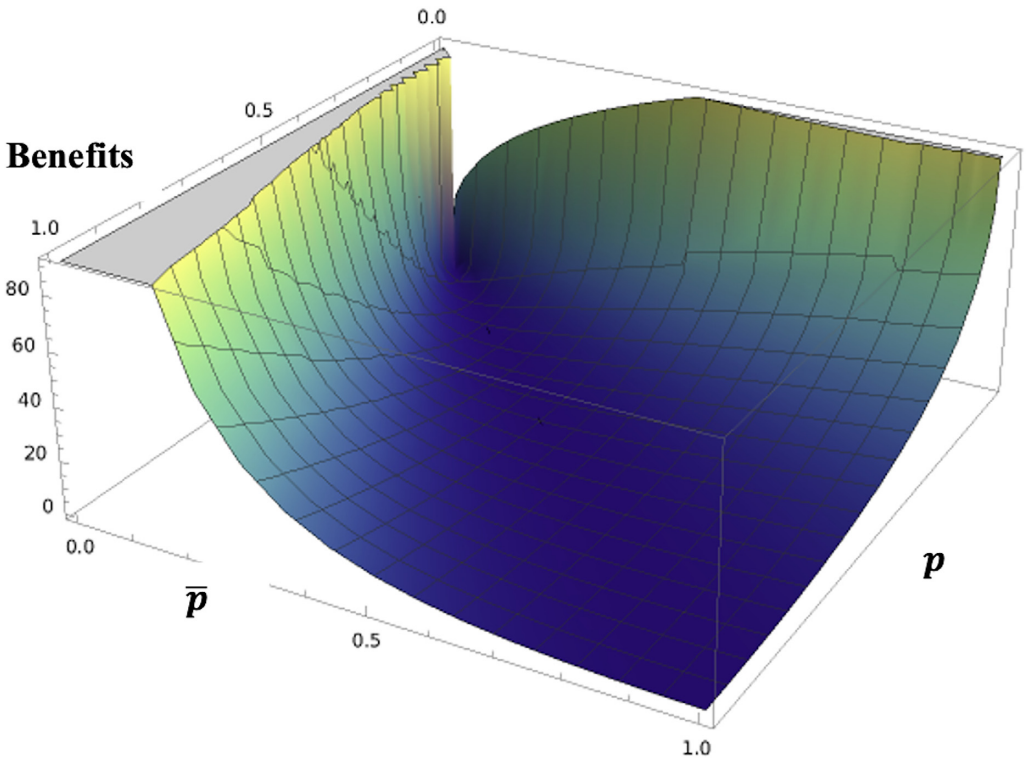

Figure 2: Benefits obtained from intelligence on threat level (p) based on prior belief of threat level ($\bar{p}$).

Numerical example

To further illustrate the results of our analyses, we present a numerical example. For security breach productivity function $s^I(z,v) = \frac{v}{(\alpha z+1)^\beta}$, where $v = 0.8$, $\alpha = 1$, $\beta = 2$, and L = \$1,000,000, we plot the optimal investment $z^*(p) = \sqrt[3]{1{,}600{,}000p} - 1$ as a function of the threat level p in Fig. 1. As indicated in Proposition 1, z^* increases in the threat level at a decreasing rate.

We also plot the benefits, G, from receiving and processing CTI with respect to the prior belief of the threat level, $\bar{p}$, and the threat level indicted in the CTI, p, in Fig. 2. As predicted in our Proposition 2, an organization receives larger benefits from processing CTI as the difference between p and $\bar{p}$ increases.

Notice that the benefits obtained from receiving and processing CTI are not symmetric. In Table 1, we calculate the benefits obtained from receiving and processing CTI, when $\bar{p} = 1, 0.1, \ldots, 1$, and when $p - \bar{p} = -1, -0.9, \ldots, 0.9, 1$. Our calculations show that when $\bar{p} = 0.1$ and $p - \bar{p} = 0.5$ (i.e. $p = 0.6$), the benefit is \$69.18, and when $\bar{p} = 0.9$ and $p - \bar{p} = -0.5$ (i.e. $p = 0.4$), the benefit is only \$14.30. Also notice that the benefits are the greatest when the CTI indicates a threat that the organization was not aware of (i.e. when $\bar{p} = 0$) and decrease as the organization had greater awareness of a threat prior to receiving the CTI. This asymmetry in the benefits is a result of diminishing returns of cybersecurity investments.

Using the same probabilities indicated by the prior and posterior beliefs, we also calculate the Kullback–Leibler Divergence when prior belief $\bar{p} = 0.1, 0.2, \ldots, 0.9$, and when $p - \bar{p} = -0.8, -0.7, \ldots, 0.7, 0.8$. The results are shown in Table 2.[26] Observe that the information gained when $\bar{p} = 0.1$ and $p - \bar{p} = 0.5$ (i.e. $p = 0.6$) is the same as the information gained when $\bar{p} = 0.9$ and $p - \bar{p} = -0.5$ (i.e. $p = 0.4$). Although the information theory approach does not provide the financial economic benefits, it provides an alternative way of viewing the fact that the information value (i.e. entropy) increases in the difference between the threat level indicated by the CTI and an organization's prior belief of the threat level.

Implications

As discussed earlier in this paper, the US federal government routinely collects CTI. Unlike profit-seeking firms belonging to a private sector information sharing organization, the federal government is not concerned about competing in the marketplace, and reciprocity of information sharing is not the reason for sharing information with private sector organizations. In addition, since the unclassified information is not confidential (by definition) and assuming that any CTI being shared would be collected by the government irrespective of the information sharing, the government is able to share a large volume of unclassified CTI at nominal cost. If a receiving organization has unlimited capacity to receive and process such CTI, federal government departments and agencies can share all its unclassified CTI without further concern. However, the processing capability of many receiving organizations is likely to be limited by either technology, human capital capabilities, and/or some other resource constraint.[27] Thus, many organizations may not be able to process all the CTI shared by the government. That is, sharing large volumes of complex CTI may congest the processing capacity of many receiving organizations and cause information overload and/or confusion. As a result, many receiving organizations may not be able to efficiently incorporate the CTI into their strategy for addressing cybersecurity threats.

Using an economics-based model, plus an analysis based on information theory, this paper identifies ways for improving the economic benefits that organizations can obtain from receiving and processing CTI from government agencies and departments on a given vulnerability. Our analysis, which was illustrated via a numerical example, suggests that the economic benefits an organization can obtain from government provided CTI are an increasing function of the difference between the CTI and the receiving organization's prior belief of the threat level. In addition, the economic benefit from the CTI is inversely related to the receiving organization's prior belief of the threat level.[28] Thus, federal government agencies and departments could improve the benefits derived from their CTI sharing by identifying CTI that is most different from the receiving organizations' prior beliefs about cyber threats, as well as prioritizing sharing CTI associated with cyber threats that are believed by the recipients to be of a low threat level. These findings are contrary to the common perception that government agencies and departments should focus on sharing CTI simply because it is associated with the highest threat level to organizations.

Of course, for a government agency or department to take actions in line with the above findings, it would need to assess the CTI that is already available to those organizations receiving its CTI. In other words, the government organization providing CTI would be well served to assess the quantity and quality of the information already available to most organizations via the news media and commercial firms that provide CTI at a moderate cost. Although such an assessment would likely be noisy, it should be possible to categorize CTI to facilitate the above recommendation. For example, unclassified CTI could be categorized as follows: (1) readily available in the public domain at a nominal cost to all organizations, (2) available in the public domain, but at a low to moderate cost (e.g. via inexpensive commercial services), (3) available at a high cost (e.g. subscribing to costly commercial services), and (4) information that is obtained by the government as a result of its unique ability to gather such information and therefore not otherwise available to organizations (regardless of their resources). The above suggestion does, however, raise the issue of whether a government agency or department could segment unclassified CTI in a manner that would facilitate a clear differentiation in the potential use of the CTI among different users (e.g. small firms with limited budgets for cybersecurity-related activities as opposed to large firms with large budgets for cybersecurity-related activities) without providing any sort of advantage to one group over another group of potential users of the CTI.

Our results are not limited to CTI shared by the government agencies and departments. For example, any producer of CTI could increase the value of their CTI feeds by accessing the prior beliefs of those receiving the CTI and identifying the CTI that is most different from those prior beliefs. Of course, commercial producers of CTI are unlikely to be able to share the information at a nominal cost as is the case with a government agency or department because the CTI is not already being collected to fulfill the government mission. Thus, in the case of a commercial producer of CTI, the cost–benefit considerations are more complicated. It is worth noting, however, that the producers of CTI (whether a government organization or a profit-seeking private sector company) need feedback from the consumers of the CTI concerning their beliefs regarding the current level of cyber threat and the type of CTI that would be helpful to them. Although feedback is rare in most threat information sharing arrangements, reliable feedback could go a long way toward enhancing the economic benefits of CTI sharing by a government agency or department.

Concluding comments

Cybersecurity risks and cyber incidents have become a critical concern to all organizations in today's interconnected digital world. Indeed, the threat of cyberattacks is considered one of the critical national and economic risk factors confronting a nation and its economy. For example, in 2013, President Obama (in Executive Order

26 We omit the cases when p or $\bar{p}$ is 0 or 1 because the Kullback–Leibler Divergence approaches infinity in these cases.

27 A variety of resource constraints are particularly common among small- and medium-size private sector firms.

28 Although beyond the scope of this paper, updating prior beliefs about cyber threats can be addresses from a Bayesian statistics perspective.

Table 1: Benefits: obtained from receiving and processing CTI that indicates threat level p when the prior belief of threat level is $\bar{p}$.

$p-\bar{p}$	Prior belief ($\bar{p}$)										
	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
−1											$115.96
−0.9										$111.92	$41.38
−0.8									$107.58	$37.77	$26.06
−0.7								$102.85	$33.93	$22.87	$17.06
−0.6							$97.65	$29.84	$19.55	$14.30	$11.09
−0.5						$91.83	$25.44	$16.09	$11.49	$8.75	$6.95
−0.4					$85.18	$20.68	$12.49	$8.66	$6.45	$5.04	$4.08
−0.3				$77.30	$15.52	$8.80	$5.86	$4.26	$3.26	$2.59	$2.12
−0.2			$67.40	$9.91	$5.12	$3.24	$2.27	$1.69	$1.32	$1.06	$0.88
−0.1		$53.29	$4.07	$1.80	$1.05	$0.70	$0.50	$0.38	$0.30	$0.25	$0.21
0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
0.1	$79919.57	$5.98	$2.25	$1.23	$0.79	$0.56	$0.42	$0.33	$0.26	$0.22	
0.2	$159898.40	$18.27	$7.53	$4.30	$2.84	$2.04	$1.55	$1.22	$1.00		
0.3	$239883.55	$33.60	$14.65	$8.62	$5.81	$4.23	$3.25	$2.59			
0.4	$319871.73	$50.76	$23.02	$13.87	$9.49	$6.99	$5.41				
0.5	$399861.75	$69.18	$32.32	$19.83	$13.74	$10.22					
0.6	$479853.03	$88.52	$42.33	$26.36	$18.46						
0.7	$559845.23	$108.58	$52.91	$33.35							
0.8	$639838.13	$129.20	$63.96								
0.9	$719831.61	$150.29									
1.0	$799825.56										

Table 2: Information: gained (Kullback–Leibler Divergence) from revising from prior belief ($\bar{p}$) to posterior belief (p).

$p-\bar{p}$	Prior belief ($\bar{p}$)								
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
−0.8									1.758
−0.7								1.146	1.363
−0.6							0.794	0.832	1.033
−0.5						0.551	0.534	0.583	0.751
−0.4					0.368	0.335	0.339	0.382	0.511
−0.3				0.226	0.193	0.184	0.192	0.223	0.311
−0.2			0.116	0.092	0.082	0.081	0.087	0.105	0.154
−0.1		0.037	0.026	0.022	0.020	0.020	0.023	0.028	0.044
0	0	0	0	0	0	0	0	0	0
0.1	0.044	0.028	0.023	0.020	0.020	0.022	0.026	0.037	
0.2	0.154	0.105	0.087	0.081	0.082	0.092	0.116		
0.3	0.311	0.223	0.192	0.184	0.193	0.226			
0.4	0.511	0.382	0.339	0.335	0.368				
0.5	0.751	0.583	0.534	0.551					
0.6	1.033	0.832	0.794						
0.7	1.363	1.146							
0.8	1.758								

13636 [37]) noted the importance of cyber threats to the national and economic security of the USA. In 2011 and 2018, the Securities and Exchange Commission (SEC) also highlighted the importance of cyber threats by issuing disclosure guidance for its registrants concerning cybersecurity risks and cyber incidents [51, 52].

US federal government departments and agencies (e.g. CIA, FBI, DHS, NSA) gather and publicly share large amounts of unclassified CTI to help protect the national and economic security of the USA. The primary focus of this paper has been on identifying ways of increasing the economic benefits that private sector organizations can obtain from receiving and processing CTI shared by the US federal government. Contrary to the common perception that these benefits are an increasing function of the level of cyber threat, our analysis shows that the greatest benefits are obtained when the difference between CTI and the prior beliefs concerning the cyber threat by the organization receiving the CTI is greatest. Furthermore, for the same difference between CTI and a receiving organization's prior belief about a cyber threat level, a receiving organization's adjustment in cybersecurity investments is inversely related to its prior belief of a cyber threat level. These findings are contrary to the common belief that it is optimal for a federal government agency or department to focus on sharing CTI related to vulnerabilities with the highest threat level.

The above findings were primarily derived based on economics-based models. However, we also show that similar insights could be obtained through the lens of information theory in terms of infor-

mation entropy. A numerical example was also provided to reinforce our findings.

As with any research based on analytical models, the results of our analysis are conditioned on the validity of the assumptions underlying the models. In this regard, these assumptions include the following. First, it is assumed that the free-rider concern that is prevalent when private sector organizations share information is not a fundamental concern to a government agency or department that shares CTI. Second, our analysis assumes that the government is already gathering the CTI for national security purposes, and therefore sharing the unclassified portion of this CTI could be done at a minimal (i.e. non-consequential) cost. Third, our analysis assumes that the recent findings by Dykstra *et al.* [13] and DHS Office of Inspector General Report [11], concerning the fact that the CTI shared by the government is perceived to be of limited use, provide an accurate picture of the situation (at least to a large number of organizations receiving the CTI). Of course, information overload and/or resource constraints are likely part of the reason CTI is not efficiently incorporated into cybersecurity decisions by many organizations. In addition, many of the factors identified by Brilingaite *et al.* [14] are also likely to be part of the reason why CTI is not efficiently incorporated into cybersecurity decisions by organizations. Fourth, we assume all organizations have the same prior beliefs. Of course, different organizations will have different prior beliefs, and this point is especially true in terms of large *vs* small- and medium-size organizations.

The above assumptions have limitations and are issues worthy of further investigation. These limitations notwithstanding, we believe the analysis contained in this paper provides new insights into information sharing where the focus is on CTI-related information shared by government agencies and departments.

Acknowledgements

We thank several NSA experts for their valuable insights. 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 any other agency or department of the US federal government.

Author contributions

Each of the authors (Josiah Dykstra, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou) contributed to all aspects of the research reported in this paper as well as to all aspects of preparing the paper for publication (i.e., in the paper's conceptualization, formal analysis, funding acquisition, formal analysis, writing, editing, and visualization).

Conflict of interest statement

The authors do not have any conflicts of interest.

Funding

This work was supported by the US Department of Defense [H98 230-19-D-0003].

References

1. Ponemon Institute. The state of threat feed effectiveness in the United States and United Kingdom, 2021. https://www.ponemon.org/userfiles/filemanager/9u0j2syx272onj9dkfpj/ (8 March 2023, date last accessed).
2. Clinton WJ. Presidential Decision Directive 63/NSC, 22 May 1998. https://irp.fas.org/offdocs/pdd/pdd-63.pdf (18 February 2023, date last accessed).
3. Obama BH. Executive Order 13691. Promoting private sector cybersecurity information sharing, 13 February 2015. https://www.govinfo.gov/content/pkg/DCPD-201500098/pdf/DCPD-201500098.pdf (18 February 2023, date last accessed).
4. Vijayan J. What is an ISAC or ISAO? How these cyber threat information sharing organizations improve security, 26 July 2022. https://www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html (18 February 2023, date last accessed).
5. Pala A, Zhuang J. Information sharing in cybersecurity: a review. *Decis Anal* 2019;**16**:172–96.
6. Mermoud A, Keupp MM, Huguenin K. *et al.* To share or not to share: a behavioral perspective on human participation in security information sharing. *J Cybersecur* 2019;**5**:tyz006.
7. Gartner. Executive perspectives on cyber threat intelligence: understanding the options, the value, and the market, 2019.
8. Tittel E. Five criteria for purchasing from threat intelligence providers, 2017. https://www.techtarget.com/searchsecurity/feature/Five-criteria-for-purchasing-threat-intelligence-services (18 February 2023, date last accessed).
9. Threat Technology. Threat intelligence: top companies providing threat intelligence solutions. https://threat.technology/threat-intelligence-top-companies-providing-threat-intelligence-solutions/ (18 February 2023, date last accessed).
10. CISA. *Information sharing and awareness*. https://www.cisa.gov/information-sharing-and-awareness (18 February 2023, date last accessed).
11. Office of Inspector General (OIG), Department of Homeland Security. DHS made limited progress to improve information sharing under the Cybersecurity Act in calendar year 2017 and 2018, September 2020. https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-74-Sep20.pdf (18 February 2023, date last accessed).
12. CISA. *Automated indicator sharing*. https://www.cisa.gov/ais (18 February 2023, date last accessed).
13. Dykstra J, Fante M, Donahue P. *et al.* Lessons from using the I-Corps methodology to understand cyber threat intelligence sharing. In: *12th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 19)*, 2019. https://www.usenix.org/system/files/cset19-paper_dykstra.pdf (8 March 2023, date last accessed).
14. Brilingaite A, Bukauskas L, Juozapavičius A. *et al.* Overcoming information challenges in cyber defense exercises. *J Cybersecur* 2022;**8**:1–9.
15. Lee RM. SANS cyber threat intelligence (CTI) survey. SANS Institute: Rockville, MD, 2020. https://threatconnect.com/wp-content/uploads/Survey_CTI-2020_ThreatConnect.pdf (18 February 2023, date last accessed).
16. Turetsky DS, Nussbaum BH, Tatar U. *Success stories in cybersecurity information sharing*. University of Albany, New York, NY, 2020. https://www.albany.edu/sscis (18 February 2023, date last accessed).
17. Bawden D, Robinson L. The dark side of information: overload, anxiety and other paradoxes and pathologies. *J Inf Sci* 2009;**35**:180–91.
18. CISA. Alert (AA21-265A) Conti Ransomware, 22 September 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-265a (18 February 2023, date last accessed).
19. Clarke RN. Collusion and the incentives for information sharing. *Bell J Econ* 1983;**14**:383–94.
20. Vives X. Trade association disclosure rules, incentives to share information, and welfare. *Rand J Econ* 1990;**21**:409–30.
21. Ziv A. Information sharing in oligopoly: the truth-telling problem. *Rand J Econ* 1993;**24**:455–65.
22. Gordon LA, Loeb MP, Zhou L. The impact of information security breaches: has there been a downward shift in costs? *J Comput Secur* 2011;**19**:33–56.
23. Spanos G, Angelis L. The impact of information security events to the stock market: a systematic literature review. *Comput Secur* 2016;**58**:216–29.
24. Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer systems security: an economic analysis. *J Account Public Policy* 2003;**22**:461–85.

25. Gal-Or E, Ghose A. The economic incentives for sharing security information. *Inf Syst Res* 2005;**16**:186–208.
26. Tosh DK, Molloy M, Sengupta S. *et al.* Cyber-investment and cyber-information exchange decision modeling. In: *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems 2015*. New York, NY, 2015, pp. 1219–24.
27. Naghizadeh P, Liu M. Inter-temporal incentives in security information sharing agreements. In: *Workshops at the Thirtieth AAAI Conference on Artificial Intelligence*, La Jolla, CA, March 2016, pp. 1–8.
28. Ezhei M, Ladani BT. Information sharing vs. privacy: a game theoretic analysis. *Expert Syst Appl* 2017;**88**:327–37.
29. Gao X, Zhong W. Economic incentives in security information sharing: the effects of market structures. *Inf Technol Manag* 2016;**17**: 361–77.
30. Hausken K. Security investment, hacking, and information sharing between firms and between hackers. *Games* 2017;**8**:23.
31. Tosh DK, Shetty S, Sengupta S. *et al.* Risk management using cyber-threat information sharing and cyber-insurance. In: *International Conference on Game Theory for Networks*, pp. 154–64. Cham: Springer, May, 2017.
32. Gordon LA, Loeb MP, Lucyshyn W. *et al.* The impact of information sharing on cybersecurity underinvestment: a real options perspective. *J Account Public Policy* 2015;**34**:509–19.
33. Laube S, Böhme R. Strategic aspects of cyber risk information sharing. *ACM Comput Surv (CSUR)* 2017;**50**:1–36.
34. Rashid Z, Noor U, Altmann J. Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. *Fut Gener Comput Sys* 2021;**124**: 436–66.
35. Bush GW. Executive Order 13356. Strengthening the sharing of terrorism information to protect Americans. 27 August 2004. https://www.govinfo.gov/content/pkg/WCPD-2004-08-30/pdf/WCPD-2004-08-30-Pg1704.pdf (8 March 2023, date last accessed).
36. The White House. National strategy for information sharing and safeguarding, December 2012. https://www.dhs.gov/sites/default/files/publications/15_1026_NSI_National-Strategy-Information-Sharing-Safeguarding.pdf (18 February 2023, date last accessed).
37. Obama BH. Executive Order 13636. *Improving Critical Infrastructure Cybersecurity*. 12 February 2013. https://www.govinfo.gov/content/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf (18 February 2023, date last accessed).
38. Cybersecurity Act of 2015. https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf (18 February 2023, date last accessed).
39. CISA. https://www.cisa.gov/about-cisa (18 February 2023, date last accessed).
40. National Institute of Standards and Technology (NIST). *Guide to Cyber Threat Information Sharing, NIST Special Publication 800-150*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf (18 February 2023, date last accessed).
41. IT-ISAC. Successes in information sharing, 8 July 2019. https://www.it-isac.org/post/manage-your-blog-from-your-live-site (18 February 2023, date last accessed).
42. Dykstra J, Gordon LA, Loeb MP. *et al.* The economics of sharing unclassified cyber threat intelligence by government agencies and departments. *J Inf Secur* 2022;**13**:85–100.
43. Xiong W, Lagerström R. Threat modeling—a systematic literature review. *Comput Secur* 2019;**84**:53–69.
44. Laube S, Böhme R. The economics of mandatory security breach reporting to authorities. *J Cybersecur* 2016;**2**:29–41.
45. Ponemon Institute. The value of threat intelligence: annual study of North American & United Kingdom companies, 2019. https://stratejm.com/wp-content/uploads/2019/08/2019_Ponemon_Institute-Value_of_Threat_Intelligence_Research_Report_from_Anomali.pdf (8 March 2023, date last accessed).
46. Schick AG, Gordon LA, Haka S. Information overload: a temporal approach. *Account Organ Soc* 1990;**15**:199–220.
47. Anderson SP, De Palma A. Information congestion. *Rand J Econ* 2009;**40**:688–709.
48. Gordon LA, Loeb MP. The economics of information security investment. *ACM Trans Inf Syst Secur (TISSEC)* 2002;**5**:438–57.
49. Matsuura K. Productivity space of information security in an extension of the Gordon-Loeb's investment model. In: Johnson ME (ed.), *Managing Information Risk and the Economics of Security*, Boston, MA: Springer, 2009, 99–119.
50. Kullback S, Leibler RA. On information and sufficiency. *Ann Math Stat* 1951;**22**:79–86. 10.1214/aoms/1177729694
51. Securities and Exchange Commission. CF Disclosure Guidance: Topic No. 2, 13 October 2011. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (18 February 2023, date last accessed).
52. Securities and Exchange Commission. Commission Statement and guidance on public company cybersecurity disclosure, 26 February 2018. https://www.sec.gov/rules/interp/2018/33-10459.pdf (18 February 2023, date last accessed).

Appendix A: Proof of Proposition 1

Case 1: $s^I(z,v) = \frac{v}{(\alpha z+1)^\beta}$

The first derivative of $s^I(z,v)$ *w.r.t.* z is
$s_z^I(z) = -\frac{v\alpha\beta}{(\alpha z+1)^{\beta+1}}$.
From Equation (5), it follows that
$-\frac{v\alpha\beta pL}{(\alpha z^*+1)^{\beta+1}} + 1 = 0$.
Hence,

$$(\alpha z^* + 1)^{\beta+1} = v\alpha\beta pL,$$

$z^* = \frac{1}{\alpha}\cdot[(v\alpha\beta pL)^{\frac{1}{\beta+1}} - 1]$.
Taking the first derivative of z^* *w.r.t.* p, we have
$z_p^* = \frac{vpL}{\beta+1}(v\alpha\beta pL)^{\frac{1}{\beta+1}-1}$.
It follows that the second derivate of z^* *w.r.t.* p is
$\frac{dz_p^*}{dp} = \frac{v\beta L}{\beta+1}\cdot(\frac{1}{\beta+1}-1)\cdot v\alpha\beta L\cdot(v\alpha\beta pL)^{\frac{1}{\beta+1}-2} = -\frac{\beta(\alpha\beta vLp)^{1/(1+\beta)}}{p^2\alpha(1+\beta)^2} < 0$..

Case 2: $s^{II}(z,v) = v^{\alpha z+1}$

The first derivative of $s^{II}(z,v)$ *w.r.t.* z is
$s_z^{II}(z) = v^{\alpha z+1}\,\alpha\ln(v)$.
The second derivative of $s^{II}(z,v)$ *w.r.t.* z is
$s_{zz}^{II}(z) = v^{\alpha z+1}\,\alpha^2\ln^2(v)$.
From Equation (6), it follows that
$z_p^* = -\frac{1}{p\alpha\ln(v)}$.
Hence, the second derivative of z^* *w.r.t.* p is
$\frac{dz_p^*}{dp} = \frac{1}{p^2\alpha\ln(v)}$.
Given that $v < 1$, we have $\frac{dz_p^*}{dp} < 0$.

Case 3: $s^{III}(z,v) = ve^{\alpha z(v-1)}$

The first derivative of $s^I(z,v)$ *w.r.t.* z is
$s_z^{III}(z) = \alpha(v-1)ve^{\alpha z(v-1)}$.
From Equation (5), it follows that
$\alpha(v-1)ve^{\alpha z^*(v-1)}pL + 1 = 0$.
Hence,

$$e^{\alpha z^*(v-1)} = -1/\alpha(v-1)vpL\,.$$

$z^* = \frac{1}{\alpha(v-1)}\ln[-1/\alpha(v-1)vpL]$.
Take the first derivative of z^* *w.r.t.* p, we have
$z_p^* = -\frac{1}{\alpha(v-1)p}$.
It follows that the second derivate of z^* *w.r.t.* p can be written as
$\frac{dz_p^*}{dp} = \frac{1}{p^2\alpha(v-1)}$.
Given that $v < 1$, we have $\frac{dz_p^*}{dp} < 0$. ■

Appendix B: A Sufficient Condition to Generalize Proposition 1

Claim: A sufficient condition for z_p^* to decrease in p is that $2s_{zz}^2 - s_z \cdot s_{zzz} > 0$, where s_z, s_{zz} are as previously defined and s_{zzz} is the third derivative of $s(z)$ *w.r.t. z*.

Proof:

From Equation (6), it follows that

$$\begin{aligned}\frac{dz_p^*}{dp} &= \frac{d\left[-\frac{s_z(z^*)}{s_{zz}(z^*)p}\right]}{dp} \\ &= -\frac{s_{zz}^2(z^*)\,z_p^* p - s_z(z^*)\left[s_{zzz}(z^*)\,z_p^* p + s_{zz}(z^*)\right]}{[s_{zz}(z^*)\,p]^2} \\ &= -\frac{\left[s_{zz}^2(z^*) - s_z(z^*)\,s_{zzz}(z^*)\right]z_p^* p - s_z(z^*)\,s_{zz}(z^*)}{[s_{zz}(z^*)\,p]^2}. \end{aligned} \tag{B1}$$

Combining Equations (6) and (B1), we have

$$\begin{aligned}\frac{dz_p^*}{dp} &= -\frac{\left[s_{zz}^2(z^*) - s_z(z^*)\,s_{zzz}(z^*)\right]\cdot\left[-\frac{s_z(z^*)}{s_{zz}(z^*)p}\right]\cdot p - s_z(z^*)\,s_{zz}(z^*)}{[s_{zz}(z^*)\,p]^2} \\ &= \frac{s_z(z^*)}{s_{zz}(z^*)}\cdot\frac{\left[s_{zz}^2(z^*) - s_z(z^*)\,s_{zzz}(z^*)\right] + s_{zz}^2(z^*)}{[s_{zz}(z^*)\,p]^2} \\ &= \frac{s_z(z^*)}{s_{zz}(z^*)}\cdot\frac{2s_{zz}^2(z^*) - s_z(z^*)\,s_{zzz}(z^*)}{[s_{zz}(z^*)\,p]^2}. \end{aligned} \tag{B2}$$

Given $s_z < 0$ and $s_{zz} > 0$, if $2s_{zz}^2 - s_z \cdot s_{zzz} > 0$, we have $\frac{dz_p^*}{dp} < 0$. ■

It can be verified that all three functional forms of $s(z)$ discussed in Proposition 1 satisfy this sufficient condition.

Appendix C: Proof of G's Convexity in $p - \bar{p}$

Claim: G is convex in $p - \bar{p}$

Proof:

Let $\delta = p - \bar{p}$, then $G = [p \cdot s(\tilde{z}, v)L + \tilde{z}] - [p \cdot s(z^*, v)L + z^*]$ can also be rewritten as:

$$G = \left[(\bar{p}+\delta)\cdot s\left(\tilde{z}\left(\bar{p}\right), v\right)L + \tilde{z}\left(\bar{p}\right)\right] - \left[(\bar{p}+\delta)\cdot s\left(z^*\left(\bar{p}+\delta\right), v\right)L + z^*\left(\bar{p}+\delta\right)\right].$$

Hence,

$$\frac{dG}{d\delta} = \frac{d\left[(\bar{p}+\delta)\cdot s\left(\tilde{z}\left(\bar{p}\right), v\right)L + \tilde{z}\left(\bar{p}\right)\right]}{d\delta} - \frac{d\left[(\bar{p}+\delta)\cdot s\left(z^*\left(\bar{p}+\delta\right), v\right)L + z^*\left(\bar{p}+\delta\right)\right]}{d\delta}. \tag{C1}$$

Based on the Envelope Theorem,

$$\frac{d\left[(\bar{p}+\delta)\cdot s\left(z^*\left(\bar{p}+\delta\right), v\right)L + z^*\left(\bar{p}+\delta\right)\right]}{d\delta} = s\left(z^*, v\right)L. \tag{C2}$$

It follows that

$$\frac{dG}{d\delta} = s\left(\tilde{z}\left(\bar{p}\right), v\right)L - s\left(z^*\left(\bar{p}+\delta\right), v\right)L. \tag{C3}$$

Given $s_z < 0$ and $z_p^* > 0$, Equation (C3) is consistent with Proposition 2 that $\frac{dG}{d\delta} > 0$ if $p - \bar{p} > 0$ and $\frac{dG}{d\delta} < 0$ if $p - \bar{p} < 0$.

From Equation (C3), we have

$$\frac{d^2G}{d\delta^2} = -s_z\left(z^*\left(\bar{p}+\delta\right), v\right)L \cdot z_p^*\left(\bar{p}+\delta\right) > 0.$$

Therefore, G is convex in $p - \bar{p}$. ■