Cyber Threat Information Sharing: Perceived Benefits and Barriers

Adam Zibak and Andrew Simpson
Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford OX1 3QD, UK
firstname.lastname@cs.ox.ac.uk

ABSTRACT

The literature on cyber security information sharing enumerates an extensive list of potential benefits for organisations in both the public and private sectors. However, despite the potential benefits, successful cyber security information sharing has been difficult to achieve. We report upon a study that sought to measure the extent to which the benefits and barriers suggested by the cyber security information sharing literature are reflected in the attitudes of practising security managers and analysts.

A self-administered online survey was used. The survey consisted of: several questions about the participants' experience with cyber security information sharing; and two sets of Likert-type scale items to measure the respondents' attitudes regarding the benefits and barriers identified in the literature.

Our findings aim to highlight the gap between the theory and practice of information sharing and provide input for future research into design principles for information sharing systems and ways to mitigate threat information sharing challenges.

KEYWORDS

cyber security information sharing; threat intelligence sharing; threat intelligence management platforms

ACM Reference Format:
Adam Zibak and Andrew Simpson. 2019. Cyber Threat Information Sharing: Perceived Benefits and Barriers. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3339252.3340528

1 INTRODUCTION

A close look at the current cyber security threat landscape reveals increasing sophistication and speed of attacks, the professionalisation of threat actors, and diversification in targets [31, 34]. Disjoint efforts to understand the complex nature of threats and the tactics and techniques of threat actors behind them give rise to insufficient and fragmented analysis.

Information gleaned on incidents could provide valuable insights to multiple teams across an organisation, including incident responders and executive-level decision makers. It is also important for outside parties, including law enforcement, government, supply chain members and other organisations in the same sector [2].

Various stakeholders have begun to collaborate in a coordinated manner to address cyber security threats. Information sharing mechanisms often constitute the core of those collaborative efforts and a significant amount of the literature has examined the potential benefits of information sharing. Such benefits range from supporting incident response to cost savings and deterrence.

Nevertheless, despite the numerous benefits, sharing is difficult to initiate or sustain. Discussions of cyber security information sharing almost always highlight "standardisation", "competition" and "trust" as reasons why organisations struggle to share information pertinent to security incidents and threats [7, 20, 32]. These concepts are so pervasive and abstract that they present significant obstacles. These challenges, as the authors of [30] explain, are rooted in the fact that cyber security information sharing entails a great deal of multi-disciplinary research.

Although the establishment of such efforts is, in many cases, reduced to an exclusive focus on technical aspects, it is an equally significant challenge for policy makers, standardisation groups, and social, economic and legal experts. This has resulted in the proliferation of what is widely known as threat intelligence management solutions as a key component of information sharing efforts [28].

A *Threat Intelligence Management Platform* (TIMP) aims to manage cyber threat data garnered from various sources and transform this data into actionable information that can be fed into different tools and disseminated to stakeholders [2]. This concept was introduced in [4], in which the authors defined the high-level requirements of a TIMP as: 1) facilitating information sharing; 2) enabling automation; and 3) facilitating the generation, refinement and analysis of data through burden-sharing collaboration or outsourcing. Information pertinent to cyber threats can be obtained from a variety of sources, including sharing communities and partnerships, as well as open-source and commercial feeds providing information spanning different levels and timescales. However, immediately actionable information tend to be low-level observed artefacts, known as indicators of compromise (IoCs), such as virus signatures, malware hash values or IP addresses of botnet command and control servers, where a system can respond automatically.

The extent to which TIMPs enable effective threat intelligence sharing remains unclear since very limited empirical analysis of the state-of-the-art of those sharing platforms exists [25]. Therefore, in this paper, we attempt to fill this gap by measuring the extent to which the benefits and risks suggested by the information sharing

ARES '19, August 26–29, 2019, Canterbury, United Kingdom
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-7164-3/19/08...$15.00
https://doi.org/10.1145/3339252.3340528

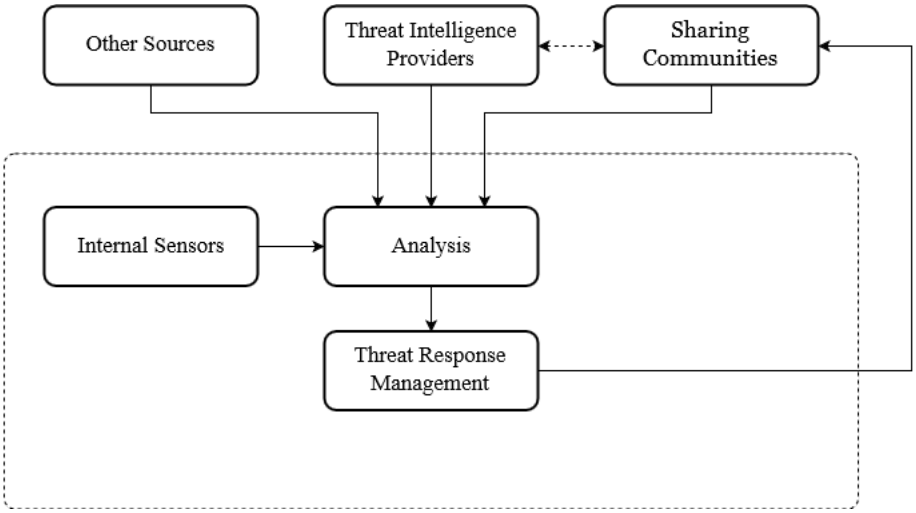

Figure 1: Threat Intelligence Management System Model (adapted from [1])

literature are reflected in the attitudes of practising cyber security professionals. Based on our findings, we highlight the gap between theory and real-world application, and discuss the implications for research in this area. To achieve our goal, we: 1) reviewed grey and academic literature pertaining to the theoretical benefits and barriers to cyber threat information sharing; 2) categorised our findings into four levels; 3) designed a survey based on those categories; and 4) surveyed 67 practitioners who are involved in cyber threat intelligence sharing efforts. Based on the survey results, our research has concluded that longstanding issues such as establishing trust among participants and free riding are no longer the primary concerns for organisations involved in threat intelligence sharing. It also showed that standardisation and automation efforts have had a positive real-world impact.

The remainder of this paper is structured as follows. Section 2 provides a theoretical background including a summary of the benefits and barriers of information sharing as suggested by the literature categorised in four different levels. Section 3 describes the methodology and research instrument employed. Section 4 presents the findings of the research. Section 5 discusses these findings in relation to the four categories. The final section summarises the contribution of the paper.

2 BACKGROUND

As highlighted in Section 1, Cyber Security Information Sharing (CSIS) efforts have in recent years focused primarily on threat-based information sharing, which is often carried out through threat intelligence management solutions [18]. In cyber security practice (and research), threat intelligence is a young field and, as the authors of [25] observe, both academic and commercial interest in this topic is increasing. As a consequence, a wide range of products and activities are often combined together under the banner of "threat intelligence" [3, 25]. Therefore, in this section we aim to contextualise the research described in this paper by providing brief background information on key concepts and components of the threat intelligence ecosystem. We also provide a summary of related work.

2.1 Conceptual framing

In cyber security theory, *threat intelligence* is often referred to as the task of collecting evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, pertaining to an existing or emerging menace or hazard to an organisation's asset in order to inform its response decisions [20]. In other words, threat intelligence is the analysis of threat actors, including their capabilities and motivation and how they use the cyber domain to achieve their aims [23].

As with traditional intelligence, cyber threat intelligence is, above all, about reducing uncertainty. In practice, its goal is to determine facts and subsequently to derive reliable conclusions and predictions that can assist decision making and facilitate operational processes such as detection, prevention and response [2].

A notable example of cyber threat intelligence at work is the identification of a threat actor known as the Axiom Group who had targeted and infiltrated companies and individuals for over six years. In 2014, upon the detection of malware used by the group, a number of victim organisations and industry partners joined efforts and exchanged information, which led to the identification of patterns including the behaviour of the group as well as the regions and sectors targeted. The conclusions they published helped incident response teams in many other organisation detect and respond to this threat [23].

However, the extent to which the information being shared through threat intelligence solutions meets the traditional definition of intelligence is a contested issue. The majority of platforms examined by the authors in [25] serve as data aggregators with limited analytical features. A similar observation is made in [3], where the authors argue that the services and products marketed as threat intelligence solutions differ in their content, scope, usability and design goals between, on the one hand, high-level written or oral briefs that offer updates on a particular threat or geographic

Category	Benefits	Barriers
Operational	• Reduces duplicate information handling [32] • Supports breach detection [38] • Reduces damage caused by breaches [38] • Supports incident response [16] • Supports deterrence efforts [26]	• Lack of standardisation [20, 32] • Vaguely defined terminology [20, 38] • Capacity limits [32] • Determining accuracy [32] • Validating quality [28, 35] • Ensuring timeliness [32] • Achieving interoperability and automation [13] • Safeguarding sensitive information [13, 22] • Handling unused or irrelevant data [13, 38]
Organisational	• Expands professional networks [32] • Supports greater defensive agility and resilience [19] • Validates intelligence derived from other sources [13] • Improves overall security posture [13, 20] • Improves situational awareness [13] • Combats skills gap [21]	• Proliferation of redundant efforts [32] • Competition [32] • The risk of reputation damage [10, 36] • Establishing trust among participants [7] • Lack of trained staff [27, 32]
Economic	• Cost savings [7, 11] • Allows subsidies provision by governments [7, 26] • Lowers cyber insurance premiums [7] • Reduces uncertainty associated with cyber security investment decisions [12]	• Free riding [10, 21] • Resource draining [19] • Loss of clients confidence and satisfaction [8, 17]
Policy	• Reinforces relationship with government agencies [6] • Offers liability protection [38]	• The risk of violating privacy or antitrust laws [36] • Government over-classification [37] • Upholding public values [6] • Different legal frameworks across jurisdictions [32]

Table 1: Benefits and barriers associated with cyber security information sharing as reported in the literature

region, and lower-level stream of indicators of compromise, such as IP addresses or binary hashes.

2.2 Cyber threat intelligence ecosystem

A general workflow for a Threat Intelligence Management System (TIMS) can receive and process threat information from different sources in order to develop a better understanding of the threat and recommend an appropriate set of actions [1]. These sources include, but are not limited to, commercial threat intelligence providers, information sharing communities, such as CiSP[1], and internal sources.

A simplified conceptual model of a TIMS (based on that of [1]) is shown in Figure 1. Here, Threat Intelligence (TI) producers disseminate threat intelligence that can be consumed by a Threat Response Management (TRM) ecosystem that determines appropriate defensive actions. This ecosystem takes action by deploying one or more Threat Response Systems including network or endpoint controllers, security elements or data centre controllers [1].

2.3 Related work

Despite the increased interest in CSIS, there is a notable paucity of empirical research relating to the value and impact of threat intelligence management platforms [28].

Most of what is written in this area is theoretical. Although useful for establishing hypotheses, such contributions do not provide solid grounds for either policy making or business decisions. A search of the literature reveals few studies that have attempted to support the theoretical assumptions surrounding CSIS issues with some empirical evidence. Some of the most notable examples are the studies conducted by researchers based at the University of Innsbruck who utilised a combination of focus groups and exploratory surveys to examine cyber threat sharing in practice [24, 25, 28, 29].

Arguments in favour of cyber security information sharing, in both the grey literature and the academic literature, present an extensive list of reasons as to why information sharing could be beneficial to the public and private sectors. However, we cannot appreciate those incentives without examining the corresponding barriers as successful implementations of CSIS efforts have faced various challenges. We summarise these benefits and barriers with respect to four categories in Table 1.

While a number of studies have recognised some of the overall opportunities and challenges facing CSIS efforts in general, research

[1] https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

Statement	Category	Dimension	Median (IQR)
(st1) Threat actors are deterred by intelligence sharing among organisations	Operational	Benefit	3 (2.5)
(st2) Threat intelligence sharing supports incident response efforts	Operational	Benefit	4 (2.5)
(st3) Threat intelligence sharing contributes to breach detection and recovery	Operational	Benefit	5 (2)
(st4) Sharing of threat intelligence reduces duplicate information handling	Operational	Benefit	3 (3)
(st5) Threat intelligence sharing strengthens and expands professional networks	Organisational	Benefit	5 (2)
(st6) Threat intelligence sharing validates and complements other sources of intelligence	Organisational	Benefit	5 (3)
(st7) Threat intelligence sharing improves overall security posture and situational awareness	Organisational	Benefit	5 (3)
(st8) Threat intelligence sharing enhances defensive agility and resilience	Organisational	Benefit	5 (2)
(st9) Threat intelligence sharing helps in combating cyber security skills shortage	Organisational	Benefit	4 (4)
(st10) Threat intelligence sharing reduces overall cyber security costs	Economic	Benefit	3 (4)
(st11) Threat intelligence sharing lowers cyber insurance premiums	Economic	Benefit	2 (1.5)
(st12) Threat intelligence sharing reduces uncertainty surrounding security investment decisions	Economic	Benefit	4 (3)
(st13) Threat intelligence sharing strengthens relationship with government agencies	Policy	Benefit	5 (2)
(st14) Threat intelligence sharing offers organisations liability protection	Policy	Benefit	3 (3)
(st15) Standardisation issues continue to hinder threat intelligence sharing	Operational	Barrier	4 (4)
(st16) Inconsistent definitions and terminology undermine efficient threat intelligence sharing	Operational	Barrier	5 (2)
(st17) It is difficult to determine the accuracy and quality of shared threat intelligence	Operational	Barrier	5 (2)
(st18) It is difficult to ensure the timeliness of shared threat intelligence	Operational	Barrier	5 (2)
(st19) The interoperability and automation of threat intelligence sharing are difficult to achieve	Operational	Barrier	4 (4)
(st20) Threat intelligence sharing results in redundant and irrelevant data	Operational	Barrier	5 (1)
(st21) There is a shortage of analysts with the skills required to handle shared threat intelligence	Organisational	Barrier	5 (2)
(st22) It is difficult to trust the other participants in threat intelligence sharing efforts	Organisational	Barrier	3 (3)
(st23) Free riding will impede threat intelligence sharing efforts	Organisational	Barrier	3 (3)
(st24) Setting up the threat intelligence sharing infrastructure is expensive and drains resources	Economic	Barrier	5 (2)
(st25) Threat intelligence sharing erodes clients' confidence	Economic	Barrier	5 (3)
(st26) Government over-classification undermine effective threat intelligence sharing	Policy	Barrier	4 (2.5)
(st27) Privacy and antitrust legal concerns impede threat intelligence sharing	Policy	Barrier	5 (3)
(st28) Inconsistent legal frameworks undermines cross-border threat intelligence sharing	Policy	Barrier	5 (3.5)

Table 2: Survey items, along with their median and Inter-Quartile Range (IQR) scores, 7 = strongly agree; 1 = strongly disagree

has yet to systematically investigate stakeholders' attitudes and perspectives. One of the early attempts was [7], in which the European Union Agency for Network and Information Security (ENISA) interviewed nine experts from six EU countries to identify CSIS barriers and incentives that are most relevant in daily practice, with a view to address efforts to address critical infrastructure protection.

More recently, in 2016, an advisory committee within the US Federal Communications Commission (FCC), was tasked with reviewing the state of CSIS within the communications industry [32]. A working group formed of representatives of the communications industry in the US explored the challenges preventing companies in the sector from effectively sharing cyber threat information pertinent to communications' critical infrastructure within the private sector. Unfortunately, the limited scope of the study, as well as the unclear methodology, makes it difficult for their findings to be generalised. A similarly limited study (in terms of scope and sample size) is described in [15], where the authors surveyed 25 practitioners to test a number of hypotheses. The aim was to understand what incentives and barriers determine a firm's decision to share or not share information with CSIS organisations in general. However, of the 25 respondents, only 9 firms were members of at least one CSIS organisation. Nevertheless, despite their different research scopes, both [32] and [15] provide useful frameworks for categorising the incentives and barriers for CSIS — from which we derived the categories adopted in this study.

2.4 Summary

The paucity of empirical support for cyber security information sharing highlights two important issues. First, private sector organisations are sometimes cautious or unwilling to join information sharing efforts. This is due to a number of reasons, including competition, liability and perceived return on investment. Without empirical evidence of the value of cyber security information sharing, it is difficult to incentivise participation. Second, the absence of evaluation methods for cyber security information sharing efforts and technology hinders identifying and remedying their shortfalls.

3 METHODOLOGY

The research described in this paper was conducted between January and April 2019. We started with a systematic analysis of grey and academic literature on the benefits and challenges of information sharing in cyber security. We categorised the extracted information into four levels: operational, organisational, economic and policy. The resulting compilation of benefits and challenges served as the basis of our subsequent online survey.

3.1 Multivocal Literature Review

Given the practical and novel nature of the field of interest, it is important to examine the state of the practice as well as the relevant academic literature. As such, we employed a Multivocal Literature Review (MLR), which is a form of a systematic literature review

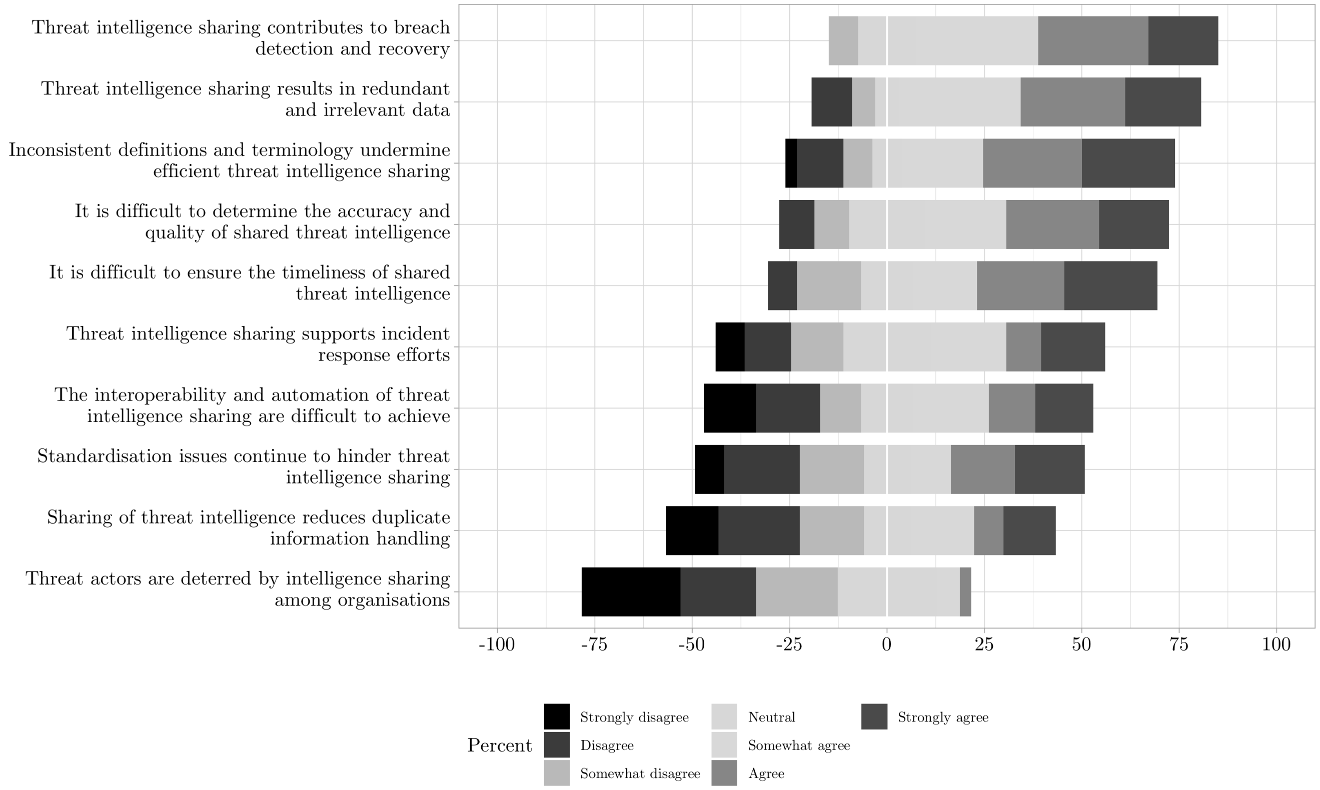

Figure 2: Respondents' attitudes towards cyber threat information sharing benefit and barriers - Operational level

that examines grey literature in addition to the formal literature [9]. The MLR was conducted to extract the benefits and challenges mentioned in research and practice through a systematic analysis of academic literature and grey literature including white papers and think-tank reports.

Given the lack of systematic guidelines for conducting such a review in Computer Science, we followed the steps specified in [25], the authors of which utilised a MLR to compile a list of threat intelligence management platforms used in research and practice. Those steps are: identifying data sources and search strategy; identifying inclusion and exclusion criteria; and assessing the quality of the results in terms of the position of the source, clarity, detail, consistency and alignment with our study's focus [33].

Our starting point for the review was the information sharing literature familiar to us from previous research ([39, 40]). This was expanded by following up the citations in the initial set of sources. We also identified literature using academic search engines, namely ACM Digital Library, ScienceDirect, Google Scholar and IEEE Digital Library as well as Google. The keywords we used are based on those derived in [25]: *(cyber Security OR threat) AND (intelligence OR information OR data) AND (sharing OR exchange).*

Examining the identified documents, we excluded literature that did not address peer-to-peer information sharing such as literature on breach notification, CERTS, software vulnerabilities disclosure and so on. In total, we gave consideration to around 60 articles, from which we compiled a list of information sharing benefits and challenges before categorising them into four levels: operational, organisational, economic and policy. This categorisation aims to reflect the multidisciplinary and multi-stakeholder nature of the topic as well as the complexity of public-private partnerships. It was largely based on earlier classification attempts such as those in [7, 32].

3.2 Survey

The applied search strategy and selection criteria described in the previous subsection identified around 38 items, as shown in Table 1. We used those items to derive our survey questions.

From March to April 2019, we sought to measure the extent to which the benefits and barriers of cyber security information sharing suggested by the literature are reflected in the attitudes of practising cyber security professionals in the UK.

In total, 41 organisations were included in the study. The survey population consisted of 67 cyber security professionals.

Among the 5 professional job types, response rates were: 56.7% from security analysts; 14.9% from security administrators; and 13.4% from Chief Information Security Officers (CISOs).

Respondents were experienced professionals, averaging 3.8 years of working experience, representing organisations from 7 different sectors: finance or insurance, information or communication, public sector or defence, utilities, health or social care, retail or wholesale, and education. Over 88% of the respondents had some direct experience in inter-organisational cyber security information

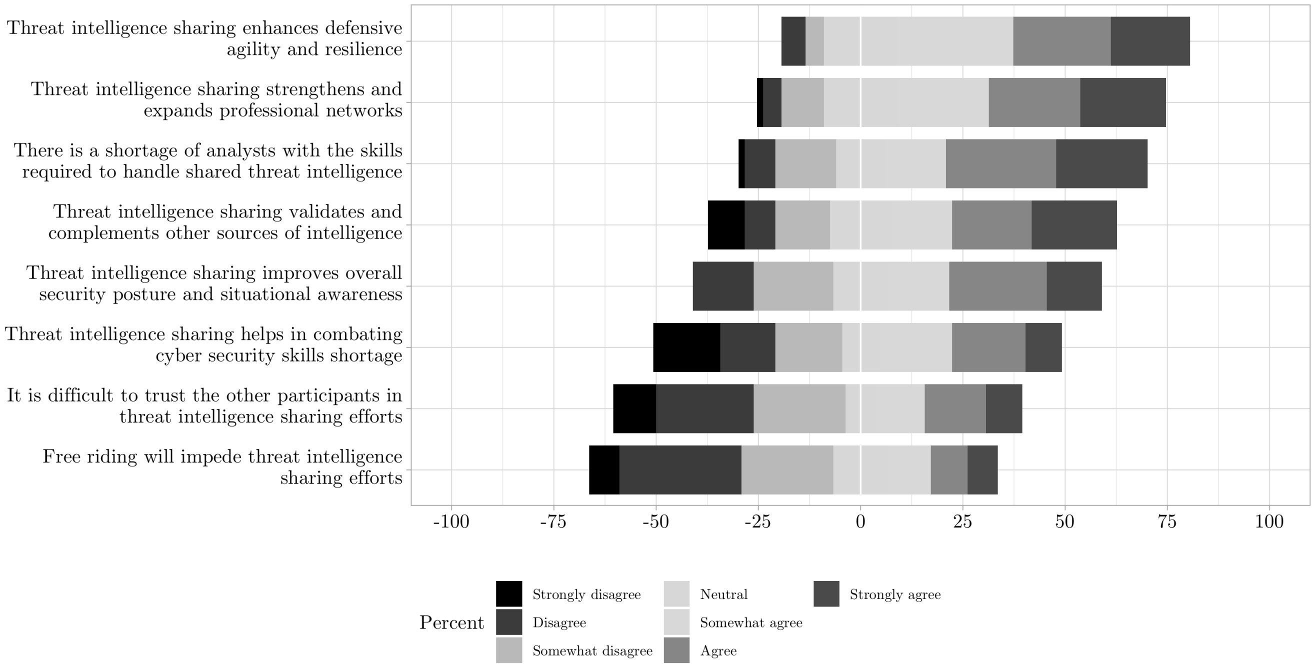

Figure 3: Respondents' attitudes towards cyber threat information sharing benefit and barriers - Organisational level

sharing, with 67% involved in a sharing effort at the time of the survey.

The survey consisted of several questions about the respondents' experience with threat intelligence sharing; and two sets of Likert-type scale items that measured attitudes toward the benefits and barriers identified in the literature. Each survey item was accompanied by a brief explanation to allow the participants to better understand the statement.

4 RESEARCH FINDINGS

Attitudes towards cyber security information sharing were measured by asking respondents to agree or disagree with 28 statements about the role of threat intelligence sharing platforms in issues such as incident response and breach detection, and about the barriers preventing their organisations from effective utilisation of cyber threat intelligence sharing. The full set of items along with the median and Inter-Quartile Range (IQR) of each item are listed in Table 2.

Overall, respondents tended to agree that threat intelligence sharing has a positive effect on their organisations' security posture as noted in the literature. However, they also highlighted several barriers that can significantly undermine the effectiveness of sharing efforts.

Neither job position nor organisation's sector accounted for any statistically significant differences in regards to the attitudes towards the benefits and barriers of cyber threat intelligence sharing.

Looking at Table 2, we can see that the participants expressed strongest agreement with the ideas that threat intelligence sharing supports breach detection and recovery efforts, develops and maintains strong professional relationships, and improves the organisation's resilience. Weaker agreement was expressed about the ability of threat intelligence sharing to reduce overall cyber security costs and to deter threat actors. Respondents did not agree that sharing would help lower cyber insurance premiums or that it would offer their organisations protection from liability.

On the negative side, respondents agreed that threat intelligence sharing incurs expensive infrastructure costs that may divert resources from other activities. They strongly agreed that determining the quality and accuracy of the shared data is difficult and that vaguely defined terminology still undermines sharing efforts. Their responses affirmed that government over-classification as well as the risk of violating privacy or antitrust laws can undermine the effective sharing of threat intelligence. There was also some agreement that the information being shared is often redundant or irrelevant. Respondents did not agree, however, that it is hard to trust the other participants or that standardisation is still a major issue hindering threat intelligence sharing.

5 DISCUSSION

We now relate our results (Table 2) to the categories first introduced in Section 2.

5.1 Operational level

The results of threat intelligence sharing efforts depend to a great extent on the effectiveness of implementation from an operational viewpoint [32]. Threat intelligence sharing efforts are still facing significant technical and operational challenges (Figure 2). Over 58% of survey respondents strongly agreed that inconsistent definitions and terminology are undermining efficient threat intelligence

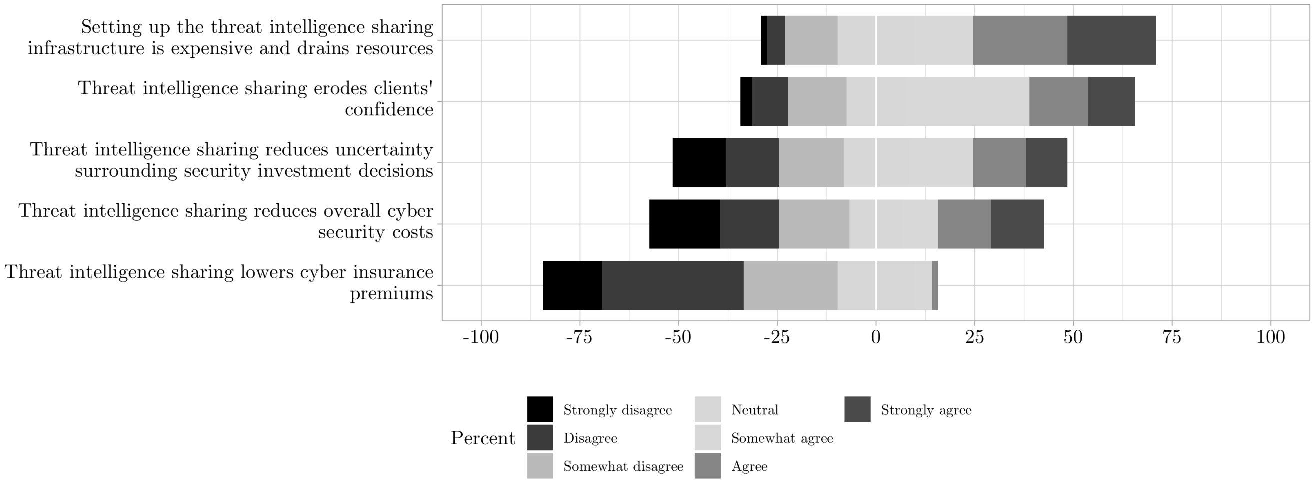

Figure 4: Respondents' attitudes towards cyber threat information sharing benefit and barriers - Economic level

sharing. This could be linked to further technical barriers such as determining the quality and accuracy of the shared data as well as ensuring the timely dissemination of information. This sentiment was confirmed by our survey respondents, 43% of whom either agreed or strongly agreed that determining the quality and accuracy is problematic. Similarly, over 61% agreed that sharing efforts often result in redundant or irrelevant data.

On a positive note, standardisation efforts appear to be yielding some practical results. Despite being repeatedly cited as an impediment to effective sharing in the literature, only 40% of respondents agreed that lack of standardisation continues to hinder sharing efforts, and only 38% considered the interoperability and automation of threat intelligence sharing difficult to achieve. This could be partially due to the emergence of several standards and ontologies such as SCAP, OpenIOC, VERIS, CYBEX, CybOX, STIX, and TAXII [14]. As a result, organisations have begun to adopt some of those specifications into their solutions, which helped address the interoperability and automation challenges. These results seem to confirm the argument presented in [2] that the challenge in threat information sharing is currently shifting from how to develop interoperable systems for data sharing to how to operationalise and generate value from the information received.

5.2 Organisational level

Overall, respondents acknowledged the positive role of threat intelligence sharing in improving the the organisation's security posture, situational awareness and resilience (Figure 3). This sentiment seems to be built upon the constructive role of intelligence sharing on the operational level as expressed by the respondents earlier.

Surprisingly, respondents did not seem concerned about traditional information sharing challenges such as establishing trust and free riding. Around 56% did not agree that establishing trust among participants in intelligence sharing efforts is difficult to achieve, while 60% did not consider free riding a significant impediment.

However, skills shortage of cyber security professionals with the required skills to handle threat intelligence sharing was among the most agreed on statements with over 64% of the respondents. The author of [27] mentions some of those skills including awareness of attack patterns and knowledge of indicators of compromise as well as intelligence analysis and incident response. Our finding therefore serves as further evidence of the wider cyber security skills shortage or mismatch as highlighted in [5], and calls for further research into the nature of the required soft and technical skills for processing threat intelligence.

5.3 Economic level

Financial incentives to information sharing have long been the focus of extensive research in various contexts [11]. After all, organisations are less likely to participate in information sharing efforts if their associated costs outweigh the benefits they produce. While the majority of respondents agreed that establishing threat intelligence sharing infrastructure is expensive and could drain resources, 72% supported the idea that, in the long run, intelligence sharing could help bring down the overall security cost (Figure 4). This may stem from faster response to threats, vulnerabilities and incidents, or from anticipating network failures [7]. The associated expenses, as explained in [32], are most acute for small and mid-sized organisations with limited financial and human resources.

Some studies have suggested that sharing threat intelligence could lower the organisation's cyber insurance premiums which in turn could further incentivise the participation in sharing efforts. However, over 74% of our respondents did not agree with this notion. This finding is consistent with that of [7] which claims that, in practice, merely sharing cyber threat information is not sufficient to convince insurance companies to lower premiums.

5.4 Policy level

Cooperation with the government continue to enjoy considerable support among the survey respondents with 65% of them agreeing that threat intelligence sharing helps build and strengthens relationships with government agencies (Figure 5). However, 45% seem to support the idea that government over-classification of data

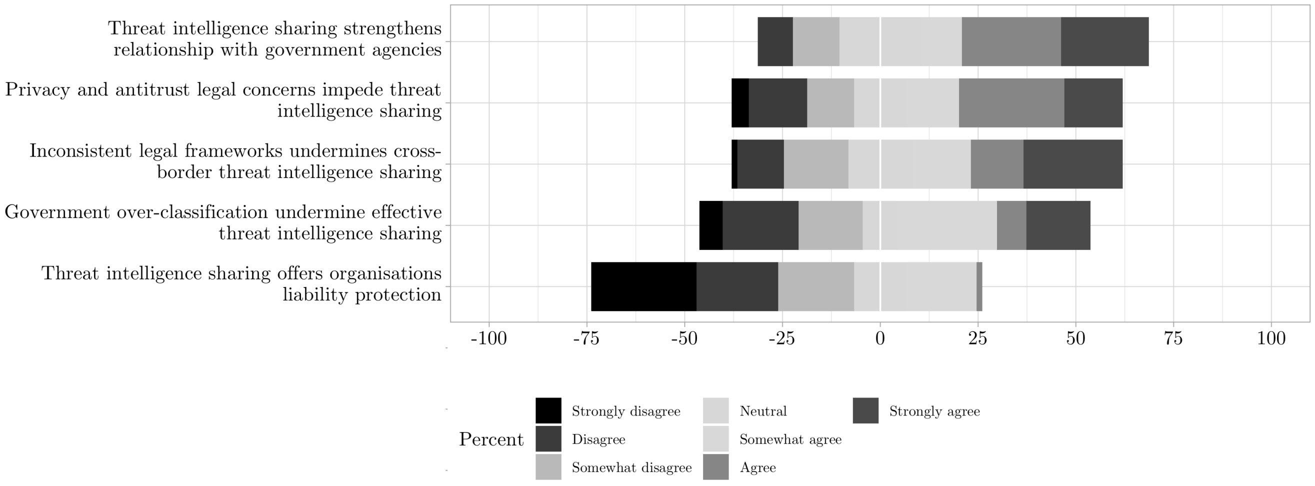

Figure 5: Respondents' attitudes towards cyber threat information sharing benefit and barriers - Policy level

could undermine the effectiveness of those efforts. This concern among others have led the UK's National Cyber Security Centre (NCSC) to implement various forms of public-private initiatives that promote closer collaboration and information sharing. Further research could assess the effectiveness of those different initiatives and determine the ideal method to mitigate the participants' concerns.

The risk of violating privacy and antitrust laws is a major concern for our respondents, with 41% of them agreeing or strongly agreeing that it could impede threat intelligence sharing. Further legal risks explored in [15] include the disclosure of trade secrets, liabilities and legal actions arising after the disclosure of cyber breach or attack details as well as the accompanying reputational damage.

About a quarter of our respondents strongly agreed that inconsistent legal frameworks present challenges to international threat intelligence sharing. This finding mirrors the claim of [32] that the complex and vague legal frameworks are thwarting real time sharing of cyber threat information internationally.

6 CONCLUSIONS

The available literature on cyber security information sharing is limited and consists largely of theoretical studies. In this paper, we have attempted to establish empirical insights to inform policy and practice in relation to threat information sharing.

We report upon a study that sought to measure the extent to which the benefits and barriers suggested by the cyber security information sharing literature are reflected in the attitudes of practising security professionals. We wished to get a deeper understanding of which benefits and barriers are influencing organisations' decision to share cyber threat information, and why. Empirical research such as this has the potential to: help determine why cyber security information sharing has posed a significant challenge for the public and private sectors; help guide future research to mitigate those challenges; and inform decision makers in private firms and security vendors about how to develop and maintain appropriate incentives for sharing.

We should acknowledge that we have surveyed only a limited number of experts from a handful of sectors in one country. The barriers to cyber threat information sharing might be very specific to country and industry and, therefore, the attitudes towards sharing arrangements might vary to some extent. However, the findings of this research are a first step to developing an evidence base in this field — and they are steps that we intend building on. For example, the study reported in this paper does not cover other aspects of information sharing such as the disclosure of security vulnerabilities or the notification of breaches of personal data — even though some of the theoretical or empirical evidence from these domains may have a bearing on the sharing of information for cyber threats. This is one of the issues that we intend addressing in future work.

Acknowledgements

The authors would like to thank the reviewers for their helpful and constructive comments. Adam Zibak's research is funded by EPSRC via the Centre for Doctoral Training in Cyber Security at the University of Oxford.

REFERENCES

[1] Syam Appala, Nancy Cam-Winget, David McGrew, and Jyoti Verma. 2015. An Actionable Threat Intelligence system using a Publish-Subscribe communications model. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security (WISCS '15)*. ACM, 61–70. https://doi.org/10.1145/2808128.2808131
[2] Sarah Brown, Joep Gommers, and Oscar Serrano. 2015. From Cyber Security Information Sharing to Threat Management. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security (WISCS '15)*. ACM, 43–49. https://doi.org/10.1145/2808128.2808133
[3] David Chismon and Martyn Ruks. 2015. Threat Intelligence: Collecting, Analysing, Evaluating. https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf.
[4] Luc Dandurand and Oscar Serrano. 2013. Towards improved cyber security information sharing . In *Proceedings of the 5th International Conference on Cyber Conflict (CyCon 2013)*. IEEE. https://doi.org/10.1109/HICSS.2014.252
[5] Tommaso De Zan. 2019. Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions. https://gcsec.org/mind-the-gap-the-cyber-security-skills-shortage-and-pubblic-policy-interventions-2/.
[6] Kristen E Eichensehr. 2017. Public-Private Cybersecurity. *Texas Law Review* 95, 3 (2017), 467–538.

[7] ENISA. 2010. Incentives and Challenges for Information Sharing in the Context of Network and Information Security. https://www.enisa.europa.eu/news/enisa-news/incentives-challenges-for-cyber-security-information-sharing-in-europe-identified.

[8] Esther Gal-Or and Anindya Ghose. 2005. The economic incentives for sharing security information. *Information Systems Research* 16, 2 (2005), 186–208. https://doi.org/10.1287/isre.1050.0053

[9] Vahid Garousi, Michael Felderer, and Mika V. Mäntylä. 2016. The Need for Multivocal Literature Reviews in Software Engineering: Complementing Systematic Literature Reviews with Grey Literature. In *Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering (EASE '16)*. ACM, Article 26, 26:1–26:6 pages. https://doi.org/10.1145/2915970.2916008

[10] Roberto Garrido-Pelaz, Lorena González-Manzano, and Sergio Pastrana. 2016. Shall We Collaborate? A Model to Analyse the Benefits of Information Sharing. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (WISCS '16)*. ACM, 15–24. https://doi.org/10.1145/2994539.2994543

[11] Lawrence A. Gordon, Martin P. Loeb, and William Lucyshyn. 2003. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* 22, 6 (2003), 461–485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

[12] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Lei Zhou. 2015. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy* 34, 5 (2015), 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

[13] Christopher S. Johnson, Mark Lee Badger, David A. Waltermire, Julie Snyder, and Clem Skorupka. 2016. *Guide to Cyber Threat Information Sharing*. Technical Report 800-150. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-150

[14] Panos Kampanakis. 2014. Security Automation and Threat Information-Sharing Options. *IEEE Security Privacy* 12, 5 (2014), 42–51. https://doi.org/10.1109/MSP.2014.99

[15] Priscilla Koepke. 2016. Cybersecurity Information Sharing Incentives and Barriers. http://web.mit.edu/smadnick/www/wp/2017-13.pdf.

[16] Tero Kokkonen, Jari Hautamaki, Jarmo Siltanen, and Timo Hamalainen. 2016. Model for sharing the information of cyber security situation awareness between organizations. In *Proceedings of 23rd International Conference on Telecommunications (ICT)*. IEEE, 1–5. https://doi.org/10.1109/ICT.2016.7500406

[17] MinJae Lee and JinKyu Lee. 2012. The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. *Information Systems Frontiers* 14, 2 (2012), 375–393. https://doi.org/10.1007/s10796-010-9253-1

[18] Martin C Libicki. 2015. Sharing information about threats is not a cybersecurity panacea. http://www.rand.org/pubs/testimonies/CT425.html. https://doi.org/10.1227/01.NEU.0000028830.90768.B8

[19] Eric Luiijf and Allard Kernkamp. 2015. Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach. http://resolver.tudelft.nl/uuid:1eeb81c7-4328-459f-944d-f55c52e31fb1.

[20] Vasileios Mavroeidis and Siri Bromander. 2017. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC 2017)*. IEEE, 91–98. https://doi.org/10.1109/EISIC.2017.20

[21] Aziz Mohaisen, Omar Al-Ibrahim, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. 2017. Rethinking Information Sharing for Threat Intelligence. In *Proceedings of the 5th ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb '17)*. ACM, 6:1–6:7. https://doi.org/10.1145/3132465.3132468

[22] Stuart Murdoch and Nick Leaver. 2015. Anonymity vs. Trust in Cyber-Security Collaboration. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security (WISCS '15)*. ACM, 27–29. https://doi.org/10.1145/2808128.2808134

[23] Scott J. Roberts and Rebekah Brown. 2017. *Intelligence-Driven Incident Response: Outwitting the Adversary*. O'Reilly Media. https://books.google.co.uk/books?id=t$_8$ejwEACAAJ

[24] Clemens Sauerwein, Christian Sillaber, and Ruth Breu. 2018. Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes. In *Proceedings of Multikonferenz Wirtschaftsinformatik 2018 (MKWI '18)*. 1333–1344.

[25] Clemens Sauerwein, Christian Sillaber, Andrea Mussmann, and Ruth Breu. 2017. Threat Intelligence Sharing Platforms : An Exploratory Study of Software Vendors and Research Perspectives. In *Proceedings of 13th International Conference on Wirtschaftsinformatik (WI 2017)*. 837–851. https://www.wi2017.ch/images/wi2017-0188.pdf

[26] Stuart E. Schechter and Michael D. Smith. 2003. How Much Security Is Enough to Stop a Thief?. In *Proceedings of the Financial Cryptography Conference*. Springer, 122–137. https://doi.org/10.1007/978-3-540-45126-6$_9$

[27] Dave Shackleford. 2017. Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/CRN360/20170314$_S$urvey$_C$TI-2017$_L$ookingGlass.pdf.

[28] Christian Sillaber, Clemens Sauerwein, Andrea Mussmann, and Ruth Breu. 2016. Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (WISCS '16)*. ACM, 65–70. https://doi.org/10.1145/2994539.2994546

[29] Christian Sillaber, Clemens Sauerwein, Andrea Mussmann, and Ruth Breu. 2018. Towards a Maturity Model for Inter-Organizational Cyber Threat Intelligence Sharing: A Case Study of Stakeholders' Expectations and Willingness to Share. In *Proceedings of Multikonferenz Wirtschaftsinformatik 2018 (MKWI '18)*. 1409–1420.

[30] Florian Skopik, Giuseppe Settanni, and Roman Fiedler. 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security* 60 (2016), 154–176. https://doi.org/10.1016/j.cose.2016.04.03

[31] Symantec. 2019. 2019 Internet Security Threat Report. https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

[32] Reliability The Communications Security and Interoperability Council. 2016. Cybersecurity Information Sharing Working Group Barriers Report. https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5$_I$nfo$_S$haring$_R$eport$_0$62016.pdf.

[33] Edith Tom, Aybüke Aurum, and Richard Vidgen. 2013. An exploration of technical debt. *Journal of Systems and Software* 86, 6 (2013), 1498–1516. https://doi.org/10.1016/j.jss.2012.12.052

[34] Wiem Tounsi and Helmi Rais. 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers and Security* 72 (2018), 212–233. https://doi.org/10.1016/j.cose.2017.09.001

[35] Cynthia Wagner, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. 2016. MISP - The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (WISCS '16)*. ACM, 49–56. https://doi.org/10.1145/2994539.2994542

[36] N. Eric Weiss. 2014. Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis. https://fas.org/sgp/crs/misc/R43821.pdf

[37] Kevin H. Wilson. 2017. Sharing Securely within Government: Best Practices for Facilitating Interagency Data Science. In *Proceedings of Data Science for Social Good (DSSG '17)*. https://dssg.uchicago.edu/wp-content/uploads/2017/09/kwilly.pdf

[38] Bronwyn Woods, Samuel J. Perl, and Brian Lindauer. 2015. Data Mining for Efficient Collaborative Information Discovery. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security (WISCS '15)*. ACM, 3–12. https://doi.org/10.1145/2808128.2808130

[39] Adam Zibak and Andrew Simpson. 2018. Can We Evaluate the Effectiveness of Cyber Security Information Sharing Efforts?. In *Proceedings of 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*. IEEE.

[40] Adam Zibak and Andrew Simpson. 2019. Towards Better Understanding of Cyber Security Information Sharing. In *Proceedings of 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*. IEEE.