Towards Better Understanding of Cyber Security Information Sharing

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

***Abstract*—There is an increased recognition of the importance of information sharing within cyber security. Nevertheless, and despite the widespread use of the term "information sharing", it is difficult to associate a precise meaning with it — not least because it is used to describe a range of different activities that are driven by a variety of goals. Furthermore, when it comes to distinguishing between the various forms of information-sharing efforts, there is evidence of a degree of inconsistency between stakeholders. In this paper we seek to understand the various definitions of cyber security information sharing; we also seek to develop a better categorisation of its different forms. In addition, we try to assess the extent to which practitioners are willing to engage in each of the derived categories. A literature review, combined with an online survey, were used to capture stakeholders' perspectives. We analyse the data with a view to establishing a more nuanced conceptualisation of information sharing. The hope is that our findings will have the potential to serve as a basis for future studies.**

I. Introduction

Intensified initiatives calling for cyber security information sharing in both the public and private sectors have yielded the current complex nexus of information sharing efforts and the widespread use of cyber threat intelligence sharing technologies [1]. Nevertheless, despite the omnipresent recognition of its role, a number of issues pertinent to the nature of cyber security information sharing and its impact remain unexplored. When it comes to thoroughly distinguishing between the various forms of information sharing efforts within the cyber security domain, there is evidence of a degree of inconsistency among different stakeholders. Moreover, literature on the impact and effectiveness of these efforts, as well as the ability to measure their value, remains scarce; further, empirical data examining the links between information sharing efforts and performance is lacking [1]–[5].

The challenges, as characterised in [6], stem from the fact that cyber security information sharing demands a significant deal of multidisciplinary research that recognises not just the technical aspects but also the legal, social and economic challenges. As such, the study described in this paper set out to explore stakeholders' understanding and attitudes towards several aspects of information sharing, as well as its role within cyber security enterprise practices. We build on this empirical study to explore a comprehensive definition of cyber security information sharing and to untangle the different forms of sharing that are currently placed under one general term.

Due to the small sample size, the generalisability of these results should be interpreted with caution. While a larger sample size could have allowed for the implementation of deeper statistical analysis, we opted for a smaller sample size to generate some 'quick wins' with a view to establishing the foundations for a long-term research agenda.

II. Background and motivation

Despite the recent resurgence of information sharing as a priority in the cyber security domain, early efforts focusing on security-related information sharing go back at least to the late 1990s [7], [8]. Over the past two decades, interest in cyber security information sharing has increased significantly. The growing recognition of the importance of information sharing is manifested in four main developments [9]:

1) *The creation of legal and regulatory frameworks to encourage the adoption of cyber security information sharing strategies.* Those efforts take various forms, ranging from traditional regulation [10], to alternative forms such as self- and co-regulation [11]. Information sharing has also been highlighted as a crucial element in a number of national cyber security strategies [11].
2) *The establishment of standards compliant with these frameworks to enable efficient information sharing, such as [12].*
3) *The emergence of national centrally coordinated sharing communities, such as the UK Cybersecurity Information Sharing Partnership (CiSP).*
4) *The proliferation of sharing technologies, including threat intelligence platforms and protocols that facilitate the sharing and management processes and help integrate information sharing into organisational cyber security processes [6], [13].*

In common with most processes, cyber security information sharing efforts require human and financial resources to ensure proper implementation. Importantly, they require a well-defined understanding of what the process is designed to achieve and what the intended outcomes are [14].

Identifying what such efforts are meant to achieve seems (in theory, at least) a straightforward task. Clearly, within the scope of cyber security practices, those efforts are designed to share information in order to produce better cyber security posture. However, examining the current practice and the details of existing cyber security information sharing efforts

TABLE I
SURVEY RESPONSES BY SECTOR AND NUMBER OF EMPLOYEES

Sector	Number of employees			
	1-49	50-249	250-999	>1,000
Manufacturing/utilities	0	1	2	6
Retail/wholesale	0	1	0	1
Information/communication	2	4	3	5
Finance/insurance	0	1	3	6
Public Sector/defence	1	0	1	1
Health/social care	0	1	1	1

TABLE II
SURVEY RESPONSES BY MATURITY LEVEL AND PROGRAMME LENGTH

Programme length	Maturity level		
	Immature	Maturing	Mature
Less than 1 year	6	1	0
Between 1 and 2 years	6	7	1
Between 2 and 5 years	7	5	2
More than 5 years	2	2	2

reveals a more complex reality. From platforms that offer real-time threat sharing and systems that link organisations, to cyber exercises and fusion centres that bring together experts from different organisations to collectively tackle challenges, the term cyber security information sharing is used as an umbrella term describing very different systems and efforts that are in many cases seeking to achieve different goals.

We draw upon the existing definitions as well as stakeholders' input to develop a more nuanced understanding of the term. This also builds on the information sharing classification framework proposed in [15] to derive a useful categorisation of cyber security information sharing efforts. As noted in [16], data pertaining to cyber threats is the most prevalent type of information sharing and has, in many cases, overshadowed other types of useful information sharing, such as best practices and vulnerability disclosures. This observation is mirrored in the academic literature [17], [18] and in industry standards, where threat-based data is the main focus [12], [19].

Untangling the different types of information sharing is also crucial if we are to determine the value of such efforts. The foundation of any evaluation effort is based on the premise that the value of programmes cannot be reasonably and fairly assessed without a clear understanding of the goals that they are designed to achieve [14].

Across a variety of sectors, more resources are being allocated for the production and sharing of cyber security information, as well as the creation of systems to automate this sharing: around three-quarters of the 304 enterprise organisations surveyed in [20] said that they would be increasing spending on cyber security threat intelligence programmes in the subsequent two years. Implicit in the rationale for developing those programmes is the assumption that automated cyber security information sharing is of value to security analysts and that access to shared cyber threat information via those systems can help analysts do their jobs more efficiently. This assumption lies at the heart of our research.

Similarly, because of the ways in which such different efforts function and the different goals they are trying to achieve, the assumption that more sharing is the solution to perceived cyber security challenges does not hold up to examination [15]. Therefore, in order to determine whether the benefits of cyber security information sharing efforts outweigh their costs, it is essential to evaluate their effectiveness. Furthermore, it is an important step towards exploring the broader issue of how cyber security information sharing efforts and technologies can be compared with other approaches to tackle security challenges [15]. In order to obtain the highest levels of security at the least cost, at a time when resources are limited, stakeholders require a broader and holistic understanding to evaluate the value of investment in these efforts. Focus is shifting therefore from establishing interoperable sharing tools to operationalising and generating value from those exchanges [21]. However, empirical research that supports the claims of the positive impact of cyber information sharing is limited. Beyond broad and anecdotal evidence lie the entire realm of cyber security information sharing initiatives and technology, as well as the question of their role in improving organisational cyber security posture.

III. METHOD

An anonymous, web-based survey was developed to examine stakeholder understanding and attitudes towards cyber security information sharing. In addition to general information about the participants and their organisation (such as the size and sector), the questionnaire covered four thematic areas:

(a) the participant's definition of the term cyber security information sharing;
(b) the participant's attitudes towards the different forms of information sharing;
(c) the maturity levels of information sharing efforts in the participant's organisation; and
(d) attempts to evaluate the efficacy of information sharing efforts within the the participant's organisation.

Emergent concepts from both grey and academic literature, as well as previous research, were used to generate the questionnaire items. The full questionnaire consisted of 17 questions. Questions were worded carefully and clearly with a view to avoiding leading or biased statements. The following question types were used: five-level Likert items; multiple choice requiring respondents to choose one response from a list of alternatives; check lists in which respondents selected the items that apply; and open questions that allowed respondents to formulate their own statements.

The questionnaire was sent out via email to 63 cyber security professionals with at least one year of working experience belonging to a wide range of industries in the UK, including financial services, manufacturing, and information and communication. Data collection took place during January–March 2018. The primary distribution method was a form of snowball or referral sampling in which participants were

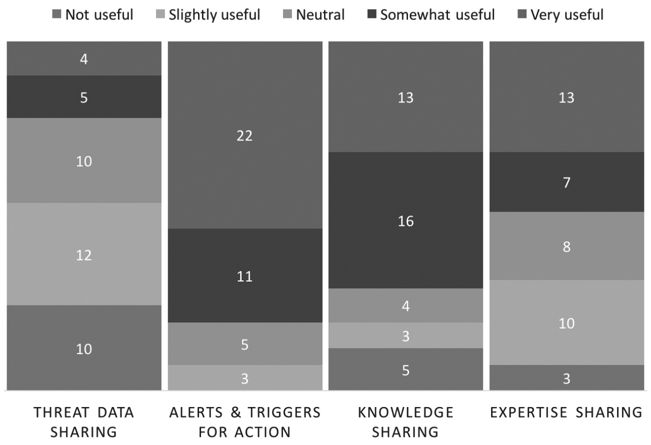

Fig. 1. Survey responses by the usefulness to engage in each category

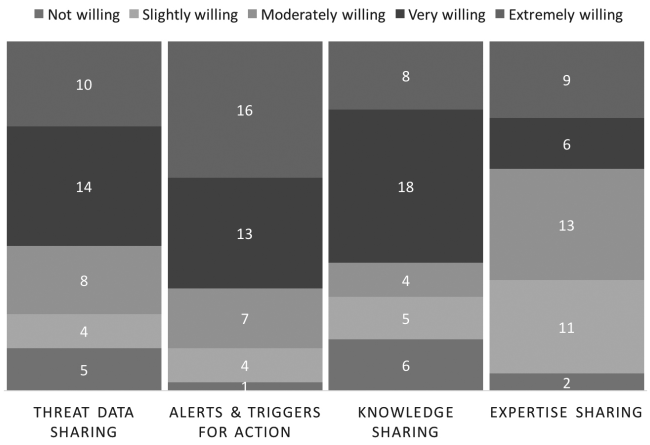

Fig. 2. Survey responses by the willingness to engage in each category

asked to distribute the survey among acquaintances working in similar positions in different organisations. This ensured access to groups beyond our immediate circle and made it possible to collect data across various industries. A total of 46 completed questionnaires were collected.

IV. Data

To get a sense for how aware respondents were of cyber security information sharing efforts and their potential impact, we asked professionals whether their teams produced, consumed and/or used information sharing as part of their cyber security practices. Of the 46 responses, only two stated that their organisations do not share information pertinent to cyber security with other organisations; two noted that they plan to do so in the next 12–24 months; and one expressed interest in engaging in some sort of cyber security information sharing effort sometime in the future. Those five responses were excluded from our analysis.

The top three industries represented were: information and communication (34.1%); finance and insurance (24.3%); and manufacturing and utilities (22%). The remaining sectors (19.5%) are shown in Table I. The classification was based on the UK's Standard Industrial Classification of Economic Activities (UK SIC 2007) [22].

Respondents' organisations ranged in size from small, with fewer than 50 employees, to large, with more than 250 employees. Roughly three-quarters of the respondents represented large organisations (73.1%), followed by medium- and small-sized organisations (19.5%) and (7.3%) respectively.

The sample frame for this study was cyber security practitioners including managers and analysts with at least one year of working experience. Roughly half of those surveyed (48.8%) reported having 5 or more years of work experience. Just over a third had 2–5 years of experience (34.1%); the remaining 17% had 1–2 years of practice.

To get a sense of the participants' attitudes towards each category of cyber security information sharing (which will be discussed in detail in Section V-B), the survey employed a 5-point Likert scale. For each category, the survey focused on three variables: the usefulness for the participant's organisation to engage in this category of information sharing efforts; the organisation's willingness to engage in the category; and the frequency of the organisation's participation in this category of efforts. The results are shown in Figures 1–3. To understand the participants' perception of the difficulty of assessing the quality and effectiveness of information sharing efforts, a 5-point Likert scale, where a reply of 1 indicated extremely difficult and a reply of 5 indicated extremely easy, was used (as shown in Figures 4 and 5).

The survey also sought to explore maturity levels of cyber security information sharing efforts among the respondents' organisations as can be seen in Table II. To this end, we adopted the maturity model of [20].

V. Findings and discussion

The section is structured in accordance with the four areas explored in the questionnaire. We start, in Section V-A, by discussing the participants' understanding of the term cyber security information sharing and how we can draw on this understanding to clarify some of the ambiguity surrounding the use of the term. In Section V-B we present our categorisation of information sharing efforts and the participants' engagement with each of them. Building on those categories, we then examine the participants' attitudes towards the usefulness and willingness to participate in each of the categories. Finally, in Section V-D, we touch on the respondents' thoughts on evaluating the effectiveness of those efforts.

A. *Definitional ambiguity*

Despite the seemingly straightforward concept, examination of the debates surrounding cyber security information sharing among practitioners and policy makers, as well as details of existing information sharing efforts, reveals a more complicated picture. In cyber security discussions, the term information sharing is often used to describe various systems and activities that are practically seeking to accomplish different objectives.

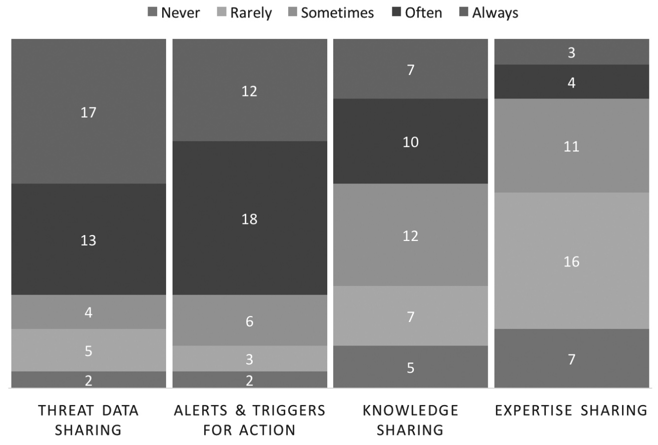

Fig. 3. Survey responses by participation in each category

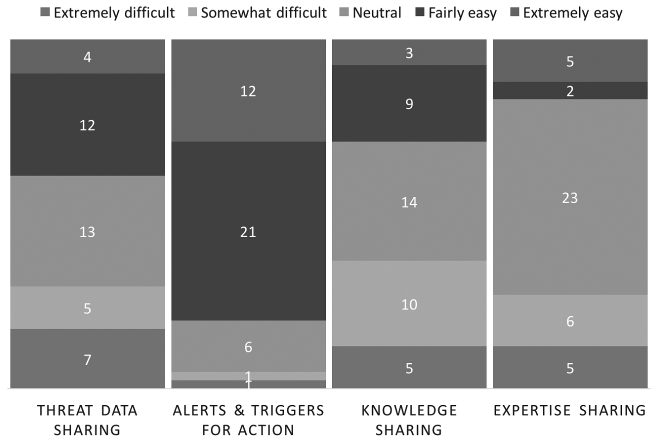

Fig. 4. Survey responses by the difficulty to evaluate the quality of each category

Although many efforts can be placed under the overarching rubric of information sharing, this ambiguity appears to be one driver of the often unfocused policy debate. But, while the intrinsic importance of information sharing has been widely recognised, few sources define information sharing as a concept with any specificity. In [23], the authors argue that information sharing broadly is:

> *"the process through which information is provided by one entity to one or more other entities to facilitate decision making under conditions of uncertainty."*

This observation was supported by our survey results. In response to the question *"What is your understanding of the term Cyber Security Information Sharing?"*, a range of perspectives was elicited. While the majority of participants provided a high level understanding of the term, a small number offered a more detailed interpretation. For example, one participant defined the term as:

> *"the sharing of information which could be useful in identifying or mitigating cyber attacks."*

This understanding was echoed by another participant who stated that it is the:

> *"process for sharing information about current / emerging threats, to help organisations improve their ability to defend against such threats."*

Answering the same question, another participant wrote:

> *"Cyber Security information sharing includes the discussion of tools and vendors, network architecture, and threat intelligence."*

A significant number of participants referred to the exchange of threat-related data as the main purpose of cyber security information sharing; others placed greater emphasis on the exchange of best practices and lessons learnt. A common view amongst the responses was that cyber security information sharing is the processes through which information is shared between organisations in the same sector or industry. However, a few responses expanded on that, saying that information could be shared *"internally"*, *"with relevant government agencies"*, or *"disclosed to the public."*

These statements, along with the limited attempts to define cyber security information sharing in the literature, point to two areas of ambiguity in the discourse: the nature of cyber security *information* and the process through which the *sharing* is done. Thus, it may be argued that the lack of clarity in the discussion surrounding cyber security information sharing stems from unclear agreement on the content of the exchange, as well as the process of the exchange itself.

***Cyber security information**:* Prior to examining the process of cyber security information sharing, we sought to explore what information in the context of cyber security is. The academic literature distinguishes between *data*, *information* and *knowledge*. However, both academic and grey literature support diversified meanings for each concept and a general consensus with regards to the definition and the boundaries of these concepts is lacking [24], [25]. Generally, unprocessed descriptions of objects of interest are regarded as data. Processed data on the other hand can be considered information or knowledge. To distinguish between the two concepts, information is seen as patterns imbued in data, and knowledge is viewed as contextualised information: knowledge is often considered as richer and more nuanced than information. What differentiates the two is how much processing or reflection they are subjected to [26].

Almost all the participants used the above terms interchangeably. Only one respondent drew a distinction between data and information.

***Sharing**:* The examination of the survey responses also revealed that the process of sharing cyber security information can take several forms:

1) a reciprocal exchange of information between two or more organisations;
2) one or more organisations providing information to a third party or parties;

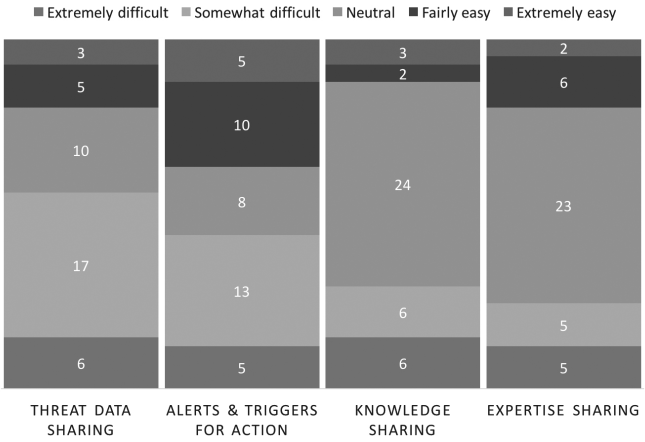

Fig. 5. Survey responses by the difficulty to evaluate the effectiveness of each category

3) several organisations pooling information and making it available to each other;
4) several organisations pooling information and making it available to a third party or parties;
5) exceptional, one-off disclosures of information in time-sensitive or emergency situations; or
6) different parts of the same organisation making information available to each other.

B. Different categories of information sharing

Before considering the effectiveness and value of cyber security information sharing efforts, we sought to adopt a more nuanced and sufficiently inclusive classification of those efforts and what they are designed to achieve.

Current attempts to categorise shared cyber security information (such as those proposed in [12] and [27]) are limited to threat-centred data (i.e. indicators of compromise, vulnerabilities, threat actors, etc.). We seek to adopt a higher level classification framework that offers a constructive way to discuss information sharing efforts and their objectives, and to explore adequate evaluation methods.

Using a small number of categories to simplify subsequent discussion, the authors of [15] propose a classification framework for traditional intelligence sharing efforts with a view to capturing most of the intended goals and outcomes of those efforts. Accordingly, we adopt the framework of [15] and adapt it to meet the requirements of the cyber security sharing landscape. Four categories of cyber security information sharing efforts are therefore identified. In the following, supported by examples, we highlight how these categories differ in terms of what is being shared and why.

1) Threat data sharing: Threat-centred data sharing efforts are designed to transmit specific security data to enable the recipient to have a more complete picture of the nature of the threat, security incident or system vulnerability. The main aim of those efforts is to inform a decision or assessment or to increase the chance of a successful detection of, triage of, and response to, cyber threats. Consider, for example, a situation in which an organisation discovers that they are a victim of a data breach where the attackers have transferred confidential information to an external server. In order to help other organisations in detecting a similar threat, the victim organisation shares the known properties of the attack, such as the IP address and domain name of the external server. Based on the available shared information, other organisations can investigate if there are similar malicious attempts to exploit their own networks. If they successfully detect suspicious activity, it might be an indication that these other organisations are being targeted with the same attack. Threat data sharing efforts often take the form of clearinghouses or data feeds.[1]

2) Triggers for action: Instead of disseminating individual data on suspicious IP addresses, malware signatures or phishing emails, some cyber security information sharing efforts are designed to communicate alerts and notifications: from one organisation that holds a particular piece of information to other organisations that are in a position to act upon it. Such efforts often seek to direct the attention of the receiving organisation to an unknown threat or vulnerability. Such notifications and alerts bring to attention the need for decisions the organisation did not know were required before receiving the warning. Triggers for action often take the form of sharing finished intelligence products and warnings from intelligence agencies. For example, in the wake of the Sony Pictures Entertainment data breach, the FBI sent a five-page memo to information security personnel at some US organisations warning them of destructive malware targeting US businesses.[2] In addition to some technical details about the malware, the confidential flash report provided guidance for how to recognise and respond to the malware and a summary of what was known about the group behind the threat. The alert also urged businesses to contact the FBI if they identified similar malware. Similar examples of triggers for actions are demonstrated by the UK's National Cyber Security Centre (NCSC) various services, such as its alerts and advisories.[3]

3) Knowledge sharing: A variety of information sharing efforts are designed not only to share immediate threat-specific or time-sensitive information, but to also build a common pool of knowledge, advisories and lessons learnt among an array of organisations. These efforts focus on the exchange of information that is often captured in documents, briefs, and other explicit knowledge. In addition to examples, such as post-breach reports and case studies, some analysis produced by security vendors, such as intelligence bulletins issued periodically, are intended to share information with organisations on an unclassified basis. These briefs are not alerts that give specific instructions to organisations on blocking a specific threat or patching a vulnerability; rather, they are an effort to educate and raise general awareness about cyber security

[1] e.g. https://www.phishtank.com and https://cymon.io.

[2] https://uk.reuters.com/article/uk-sony-cybersecurity-malware/exclusive-fbi-warns-of-destructive-malware-in-wake-of-sony-attack-idUKKCN0JF3FM20141202

[3] https://www.ncsc.gov.uk/index/alerts-and-advisories

issues. Those efforts can vary in formality and structure. Examples include industry-based inter-organisational social media systems designed to catalyse direct person-to-person information sharing and human-mediated sharing for educational knowledge sharing among different organisations through mechanisms such as joint training activities including cyber exercises and war games.

4) Expertise sharing: Some information sharing efforts are designed to link and bring together experts from various organisations so their multidisciplinary expertise can be applied to tackle common security challenges. Sharing of expertise may be a necessity to take full advantage of shared information, since the knowledge and skills needed to understand and apply the information may not all be available in all receiving organisations. As a result, expertise sharing may be a path to gain access to the needed capabilities without requiring independent investments to build them in every organisation. A prime example of those efforts are Computer Emergency Response Teams (CERTs), where a diverse group of researchers, software engineers, security analysts and intelligence specialists from various sectors including government, industry and academia come together to study problems that have widespread cyber security implications and develop methods and tools to counter cyber threats. Another example is the NCSC's Industry 100 scheme where experts from the private sector are invited to fill a range of both technical and managerial positions at different levels of operation at the agency for a period of time with the aim of sharing expertise and building ties between industry and government. The experts can later return to the private sector and draw on their experience at the NCSC to drive change within industry. Other online collaborative environments act not only as nodes for knowledge sharing but also as a means to link the authors of that knowledge for sharing expertise.

These four categories capture the main differences between cyber security information sharing efforts and the main benefits for building bridges between different organisations or individuals working in different domains or industries. While some information sharing efforts focus on only one of these categories (e.g. data feeds and security portals designed for very specific sharing functions), others are designed to facilitate several simultaneously (e.g. CiSP, fusion centres, etc.). Neither the focus on a single category nor the pursuit of several categories of cyber security information sharing is necessarily more desirable; rather, the category an effort is facilitating should decide how its success is assessed.

Survey participants reported a varied level of engagement with each category. As shown in Figure 3, around three-quarters of the organisations reported participating in threat data sharing either always or often. The same percentage stated that they exchange triggers for action followed by knowledge sharing and expertise sharing.

These findings broadly support the claims made in [16], in which Libicki suggests that, when talking about cyber security information sharing efforts, threat-centred information sharing has overshadowed other equally important types of sharing.

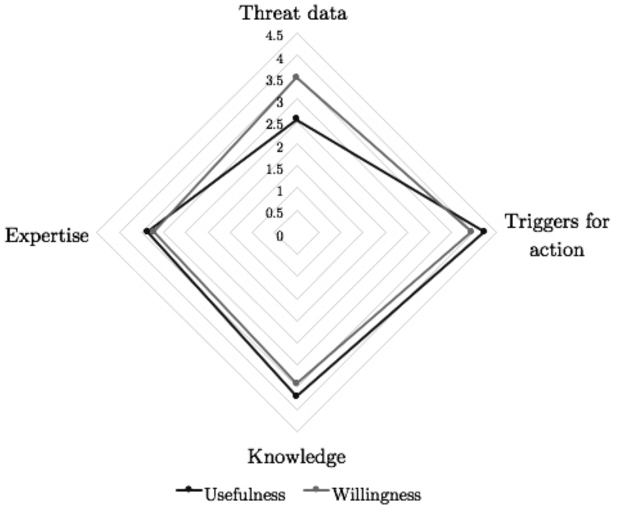

Fig. 6. Difference between mean metric scores for the Usefulness and Willingness variables

C. Usefulness, willingness and participation

One of the areas this study set out to explore was stakeholders' attitudes towards the usefulness of the different categories of cyber security information sharing laid out in Section V-B, as well as their willingness to join these efforts. Despite the proliferation of sharing efforts, empirical examination of their value to stakeholders is lacking. In [28], the authors surveyed 17 UK-based small and medium size enterprises to assess the consequences of sharing a particular set of cyber security metrics among the organisations' supply chains. Participants' attitudes towards the usefulness of implementing those metrics and their willingness to share them were captured. Despite the narrow scope and the small sample size, the study showed that the usefulness variable consistently scored higher than the sharing variable: in general, participants would prefer to implement the security metrics more than they would share them — especially metrics such as the financial losses of security incidents, number of known vulnerabilities and percentage of assets with anti-malware tools.

Participants' attitudes towards the different categories of cyber security information sharing proposed in Section V-B were recorded. As Figure 6 illustrates, when compared to other categories, *threat data sharing* was perceived as the least useful. The participants regarded *triggers for action* as the most useful form of sharing, followed by *knowledge and expertise sharing*. As for the willingness to engage in, *triggers for action* again scored the highest among participants, followed by *threat data* and *knowledge and expertise sharing*.

The usefulness of expertise, knowledge and triggers for action sharing consistently scored higher than the willingness to engage in those categories. One explanation could be the *free rider problem* discussed extensively in the economics literature [29].

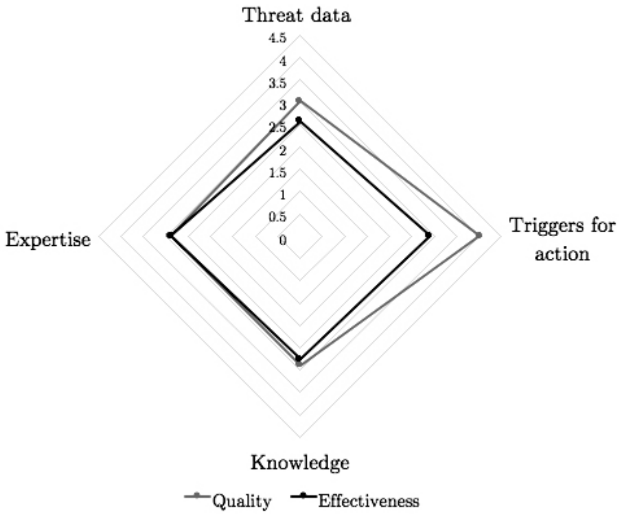

Fig. 7. Difference between mean metric scores for the Quality and Effectiveness variables

D. Maturity and evaluation

Despite high levels of participation in some forms of cyber security information sharing as shown in Figure 3, consensus as to the usefulness of those efforts, as can be seen in Figure 1, is lacking. This observation, coupled with the claim made in [21] that the focus in cyber security information sharing is shifting from creating interoperable sharing tools to operationalising and generating value from those exchanges, highlights several issues.

We asked the participants about the maturity of their organisations' information sharing efforts and how long they had been in place. To this end, we adapted the maturity model of [20]. Each level was defined according to the formality of the sharing processes, their integration into the organisation's other security practices and staff allocation and skills. The results are illustrated in Table II.

Two observations stand out. First, the majority of organisations (85.4%) have had a cyber security information sharing programme for less than 5 years. Second, only five organisations considered their information sharing efforts mature, while half of the sample size regarded their programmes as immature. Understanding the reasons behind the identified maturity lag in information sharing efforts requires further research. In our exploratory study, we sought to capture the practitioners' perspectives on the difficulty of evaluating those efforts. This stems from the belief that cyber security information sharing is not an end in itself, but a means to an end: the set of goals it is designed to achieve [30]. Therefore, accurately evaluating the sharing effort and its performance is essential to identifying its shortcomings and the hindrances preventing it from achieving fully maturity.

We asked the survey participants several questions to gauge their attitudes towards the difficulty of evaluating both the quality of the information being shared in each category, as well as the effectiveness of those efforts. The results can be found in Figures 4 and 5.

Evaluating the quality was consistently perceived less difficult compared to assessing the effectiveness of cyber security information sharing efforts across the four categories as can be seen in Figure 7. In addition to the traditional challenges in evaluating the effectiveness and quality of a piece of information, the authors of [3] found that the cost and required effort of tracking and fixing data quality issues increases the difficulty of the evaluation process.

When asked whether their organisations had methods in place to assess the effectiveness of their cyber security information sharing efforts, 51.2% stated that they do not have methods in place, but they are interested in establishing them. A further third noted that they are either in the process of creating them or are planning to do so in the next 12 months. The remaining fifth of the surveyed organisations (21.9%) reported having established informal or formal methods.

VI. Conclusions and future work

The impulse to share information and intelligence to address collective threats has manifested in many areas over the years [31]. However, when it comes to cyber security information sharing, and despite the increased recognition of its importance, current research has been slow to address several aspects, with very limited work specifically focusing on the stakeholders' attitudes and understandings. By collecting and analysing the stakeholders' views, this study has been one of the first attempts to gain a better understanding of the current cyber security information sharing practices.

The study has contributed to conceptualising information sharing in cyber security by: (i) addressing the confusion that arises from the wide use of the term and drawing on stakeholders' input to clarify the ambiguity surrounding the use of the term; (ii) untangling the various types of information sharing by proposing a categorisation framework; (iii) capturing and analysing the stakeholders' views on the usefulness of the different kinds of information sharing and the participants' willingness to engage in each; and (iv) highlighting some of the issues that pertain to evaluating the quality and effectiveness of cyber security information sharing efforts.

The generalisability of these results is subject to several limitations. In addition to the difficulty of verifying self-reported data, our sample size was relatively small. A larger sample size could have generated more accurate results and allowed for the implementation of deeper statistical analysis and the uncovering of statistically significant relationships. Moreover, the sample was dominated by large organisations, which will have inevitably skewed the results. While certain industry sectors like information and communication were more represented than others, some sectors were out of the survey's reach and did not appear in the results.

Although the findings should be interpreted with caution, this study represents the start of a long-term research plan. Our research has thrown up many questions in need of further investigation. Our future research will seek to explore the challenges facing the achievement of effective cyber security information sharing, including exploring new methods to evaluate the effectiveness of the current models of cyber security information sharing efforts. This step is essential in order to determine whether the benefits information sharing brings outweigh its costs. It is also a step towards answering the broader question of how cyber security information sharing efforts and technologies compare with other approaches to achieve the same cyber security ends. At a time when resources are constrained, the broader understanding is necessary to make it possible to balance investment in these efforts with other policies designed to achieve the same cyber security end result.

Acknowledgments

The authors would like to thank the anonymous reviewers for their helpful 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] C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat Intelligence Sharing Platforms : An Exploratory Study of Software Vendors and Research Perspectives," in *Proceedings of the 13th International Conference on Wirtschaftsinformatik - WI 2017*, St. Gallen, Switzerland, 2017, pp. 837–851.

[2] K. Hausken, "Information sharing among firms and cyber attacks," *Journal of Accounting and Public Policy*, vol. 26, no. 6, pp. 639–688, 2007.

[3] C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, "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*. New York, New York, USA: ACM Press, 2016, pp. 65–70. [Online]. Available: http://doi.acm.org/10.1145/2994539.2994546http://dl.acm.org/citation.cfm?doid=2994539.2994546

[4] M. Davies and M. Patel, "Are we managing the risk of sharing cyber situational awareness? a UK public sector case study," in *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*. IEEE, 2016. [Online]. Available: https://doi.org/10.1109/cybersa.2016.7503292

[5] C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, "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 (MKWI)*, Lüneburg, Germany, 2018, pp. 1409–1420.

[6] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *Computers & Security*, vol. 60, pp. 154 – 176, 2016. [Online]. Available: //www.sciencedirect.com/science/article/pii/S0167404816300347

[7] United States. President's Commission on Critical Infrastructure Protection, "Critical foundations: Protecting America's infrastructure," https://www.hsdl.org/?view&did=986, 1997.

[8] A. K. Ghosh and M. J. Del Rosso, "The role of private industry and government in critical infrastructure assurance," http://gost.isi.edu/cctws/delroso-ghosh.pdf, 1998.

[9] A. Zibak and A. Simpson, "Can We Evaluate the Effectiveness of Cyber Security Information Sharing Efforts?" in *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*. IEEE, 2018.

[10] European Parliament, "Security of Network and Information Systems (the NIS Directive)," http://data.europa.eu/eli/dir/2016/1148/oj, 2009, eU Directive OJ L 194.

[11] D. Bedrijfsrevisoren, J. D. Muynck, and S. Portesi, "Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches," https://www.enisa.europa.eu/publications/cybersecurity-information-sharing, 2015.

[12] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, "Guide to Cyber Threat Information Sharing," National Institute of Standards and Technology, Tech. Rep. 800-150, 2016. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[13] P. Kampanakis, "Security Automation and Threat Information-Sharing Options," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 42–51, 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6924671/

[14] J. C. McDavid, I. Huse, and L. R. L. Hawthorn, *Program Evaluation and Performance Measurement*. SAGE Publications, 2012. [Online]. Available: https://books.google.co.uk/books?id=4785DQAAQBAJ

[15] B. A. Jackson, "How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts," http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR380/RAND_RR380.pdf, 2014.

[16] M. C. Libicki, "Sharing information about threats is not a cybersecurity panacea," RAND corporation, Tech. Rep. CT-425, March 2015. [Online]. Available: https://www.rand.org/pubs/testimonies/CT425.html

[17] O. Serrano, L. Dandurand, and S. Brown, "On the Design of a Cyber Security Data Sharing System," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security - WISCS'14*. New York, New York, USA: ACM Press, 2014, pp. 61–69. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2663876.2663882

[18] J. Steinberger, A. Sperotto, M. Golling, and H. Baier, "How to exchange security events? Overview and evaluation of formats and protocols," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2015, pp. 261–269. [Online]. Available: http://ieeexplore.ieee.org/document/7140300/

[19] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)," https://www.mitre.org/publications/technical-papers/standardizing-cyber-threat-intelligence-information-with-thee, 2014.

[20] J. Oltsik, "Threat Intelligence and Its Role Within Enterprise Cybersecurity Practices," https://research.esg-global.com/reportaction/threatintelligenceenterprisecybersecurity/Marketing, 2015.

[21] S. Brown, J. Gommers, and O. Serrano, "From Cyber Security Information Sharing to Threat Management," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security - WISCS'15*. New York, New York, USA: ACM Press, 2015, pp. 43–49.

[22] Office for National Statistics, "UK Standard Industrial Classification of Economic Activities 2007," https://www.ons.gov.uk/methodology/classificationsandstandards, 2007.

[23] M. Fleming, E. Goldstein, and J. K. Roman, "Evaluating the Impact of Cybersecurity Information Sharing on Cyber Incidents and Their Consequences," https://ssrn.com/abstract=2418357, 2014.

[24] C. Zins, "Conceptual approaches for defining data, information, and knowledge," *Journal of the American Society for Information Science and Technology*, vol. 58, no. 4, pp. 479–493, 2007. [Online]. Available: http://dx.doi.org/10.1002/asi.20508

[25] D. W. De Long and L. Fahey, "Diagnosing cultural barriers to knowledge management," *Academy of Management Perspectives*, vol. 14, no. 4, pp. 113–127, 2000. [Online]. Available: https://doi.org/10.5465/ame.2000.3979820

[26] L. Wortel, T. Grant, and J. Soeters, "C2 systems and information sharing in a cross cultural context: willing and able?" in *Proceedings of the 12th International Command and Control Research and Technology Symposium*, Breda, The Netherlands, 2007.

[27] ISAO Standards Organization, "Introduction to Information Sharing," Tech. Rep. ISAO 300-1, October 2016. [Online]. Available: https://www.isao.org/products/isao-300-1-introduction-to-information-sharing/

[28] R. Lewis, P. Louvieris, P. Abbott, N. Clewley, and K. Jones, "Cybersecurity information sharing: A framework for information security management in UK SME supply chains," in *Proceedings of the 22nd European Conference on Information Systems - ECIS 2014*, Tel Aviv, Israel, 2014.

[29] E. Gal-Or and A. Ghose, "The economic consequences of sharing security information," *Economics of Information Security*, vol. 16, no. 2, pp. 95–104, 2004.

[30] M. Fleming and E. Goldstein, "Metrics for Measuring the Efficacy of Critical-Infrastructure-Centric Cybersecurity Information Sharing Efforts," https://ssrn.com/abstract=2201033, 2012.

[31] C. Gilbert, "Scalable security: Cyber threat information sharing in the internet age," Master's thesis, Stanford University, 2014.