

Can We Evaluate the Impact 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—Once concentrated on protecting critical infrastructure, cyber security information sharing efforts have evolved in recent years to now include many industries and have resulted in the current complex constellation of situational awareness sharing efforts on various levels. They have also yielded a plethora of cyber threat intelligence sharing technologies. Yet, despite the proliferation of these efforts and technologies, the literature measuring the value and the impact of cyber security information sharing remains limited. We aim to address the lack of empirical studies by using a triangulated mixed-methods research design to explore stakeholder attitudes towards cyber security information sharing benefits and risks, and to investigate the impact of this sharing on the productivity and performance of cyber security analysts.

Index Terms—cyber security; cyber situational awareness; information sharing; cyber threat intelligence

I. INTRODUCTION

Growing calls for cyber security information sharing have resulted in the current complex constellation of information sharing efforts and the proliferation of cyber threat intelligence sharing technologies [1]. However, despite this increased interest, a number of questions pertinent to the nature of cyber security information sharing and its impact remain unanswered. A certain degree of disparity remains among different stakeholders when it comes to distinguishing between different types of cyber security information sharing. Furthermore, the literature on the impact of these efforts and the ability to measure their value remains limited and empirical data establishing a link between cyber security information sharing and performance is lacking [1], [2]. Therefore, this study will look to answer the following questions using a triangulated mixed-methods research design consisting of a survey, semi-structured interviews and direct observation: *What are the different categories of cyber security information sharing from stakeholders' perspectives?*; *To what extent are the benefits and risks of cyber security information sharing suggested by the literature reflected in the attitudes of cyber security stakeholders?*; and *Does cyber security information sharing technology improve the effectiveness, productivity and overall performance of cyber security analysts?*

II. BACKGROUND AND MOTIVATION

Although early efforts at security-related information sharing can be traced to the late 1990s¹, there has been a significant growing interest in cyber security information sharing in recent years. This increased recognition manifests in four

main areas: the creation of legal and regulatory frameworks varying in forms and formality to encourage the adoption of cyber security information sharing strategies²; the establishment of standards compliant with these frameworks to enable efficient information sharing [3]; the emergence of national centrally coordinated sharing communities such as the UK Cybersecurity Information Sharing Partnership (CiSP); and the proliferation of sharing technologies including threat intelligence platforms and protocols that facilitate the sharing processes and help integrate information sharing into organisational cyber security processes [4].

Like all processes, cyber security information sharing needs human and financial resources to ensure proper implementation. Across 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 [5] said that they would be increasing spending on cyber security threat intelligence programmes in the following 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 will help analysts do their jobs more efficiently. This assumption lies at the heart of our research.

It is important to assess the effectiveness of those implemented efforts in order to determine whether the benefits they bring outweigh their costs. Furthermore, it is a necessary step towards answering the broader question of how information sharing efforts and technologies compare with other approaches to achieve the same cyber security ends. At a time when resources are limited, a broader holistic understanding is necessary to allow stakeholders to assess the investment in these efforts and compare it with other policies designed to achieve the same cyber security end result. Focus is shifting therefore from creating interoperable sharing tools to operationalising and generating value from those exchanges [6]. However, sparse and very limited empirical evidence exists to support the claims of the positive impact of cyber information sharing. Beyond general information sharing benefits and anecdotal evidence lie the entire realm of cyber information sharing efforts and technology, as well as the question of their role in improving organisational cyber

¹<https://fas.org/irp/offdocs/pdd/pdd-63.htm>

²e.g. www.dhs.gov/publication/executive-order-13691-promoting-private-sector-cybersecurity-information-sharing and www.enisa.europa.eu/publications/cybersecurity-information-sharing.

security posture.

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 because of a variety of reasons including competition, liability and 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.

III. METHOD

This study will employ a triangulated research design to help mitigate inherent weaknesses in single-method designs and to give us access to rich empirical data on an under-researched area. A non-experimental, survey design will be used as the primary data collection method.

A. Survey

Part A is concerned with stakeholders' perspectives and understanding of the benefits and risks of cyber security information sharing. It will be presented to cyber security analysts and managers from a wide range of public and private organisations who are involved in cyber security information sharing efforts. Those efforts can range from a simple project where one organisation gives information pertinent to a specific cyber security incident to another, to a complex multiparty effort to create a common information resource that they all use, such as the aforementioned CiSP. The items of this survey will be generated from emergent concepts from both grey and academic literature.

Part B will focus on the impact of cyber security information sharing. This will be presented to two groups of cyber security analysts: a group that uses information sharing technology on a daily basis and a second group that does not. We will refer to them as the information sharing group and the comparison group. This study will use a control group to create a comparison baseline. The survey will examine the differences in perception of the value of information sharing between the two groups. It will seek to determine whether information sharing technology makes a difference in the analysts' assessment of the value of cyber security information sharing in the following areas: individual effectiveness, job performance, productivity, breach investigation and forensic support, and cyber security incidents and vulnerabilities. It will also examine the effects of potential intervening variables such as analysts skills and training.

B. Semi-structured interviews

The qualitative portion of our research methodology will involve interviewing cyber security analysts to gain insights into their use of cyber security information sharing technology and its impact on areas like their productivity and performance. The interview questions will be semi-structured and open-ended in order to elicit the participants' views, understandings and experiences on the topic, as well as other relevant aspects that are not predetermined by the original set of questions. The questions will be presented to the information sharing

group and the comparison group. Questions will include themes about the user's perception of the usefulness, comprehensiveness and quality of the information being shared, the technology's reliability and ease of use, and the user's performance measures.

C. Direct observation

Supplementing the interviews is the direct observation of a number of cyber security analysts from both study groups, during which the analysts' activities will be observed and documented while working a normal workday, noting the analysts' use of relevant technology and shared data.

D. Analysis

Data analysis will involve analysing the data from both the qualitative and quantitative approaches used in the study. Although in the study the quantitative and qualitative approaches will be given approximately equal weight, we will place a greater emphasis on the quantitative analysis phase, resulting in a sequential quantitative-dominant mixed analysis.

IV. CONCLUSIONS AND FUTURE WORK

In addition to exploring stakeholders' perspectives on the risks and benefits of cyber security information sharing, we believe that this study will provide important empirical evidence towards assessing the impact of cyber security information sharing and answering the question of whether sharing technology contribute to the overall performance and productivity of cyber security analysts. We expect the results of this study to have real-world implications and to provide the motivation and foundation for further empirical research in this area.

ACKNOWLEDGEMENT

Adam Zibak's research is funded by EPSRC via the Centre for Doctoral Training in Cyber Security at the University of Oxford.

REFERENCES

- [1] Clemens Sauerwein, Christian Sillaber, Andrea Mussmann, and Ruth Breu. Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. In *13th International Conference on Wirtschaftsinformatik (WI 2017)*, pages 837–851, 2017.
- [2] Christian Sillaber, Clemens Sauerwein, Andrea Mussmann, and Ruth 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 2016)*, pages 65–70, New York, New York, USA, 2016. ACM Press.
- [3] Christopher S. Johnson, Mark Lee Badger, David A. Waltermire, Julie Snyder, and Clem Skorupka. Guide to Cyber Threat Information Sharing. Technical Report 800-150, National Institute of Standards and Technology, October 2016.
- [4] Florian Skopik, Giuseppe Settanni, and Roman Fiedler. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, 60:154–176, 2016.
- [5] Jon Oltsik. Threat Intelligence and Its Role Within Enterprise Cybersecurity Practices. <https://research.esg-global.com/reportaction/threatintelligencecenterprisecybersecurity/Marketing>, 2015.
- [6] Sarah Brown, Joep Gommers, and Oscar Serrano. From Cyber Security Information Sharing to Threat Management. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security (WISCS 2015)*, pages 43–49, New York, New York, USA, 2015. ACM Press.