# A Success Model for Cyber Threat Intelligence Platforms




Adam Zibak

Keble College

University of Oxford

A dissertation submitted for the degree of

*Doctor of Philosophy*

Michaelmas Term 2020

# Acknowledgements

First and foremost I am extremely grateful to my supervisor Andrew Simpson for his support, patience and genuine care during my DPhil journey. His constant reminder that there is more to life than a PhD kept me grounded and ensured I enjoyed my time in Oxford to the fullest.

I would also like to thank Clemens Sauerwein for his insightful comments, contribution and belief in my work. My appreciation also goes to everyone involved in the CDT, in particular David and Maureen, and to Keble college for giving me a home away from home.

My friends, Andy, Ben, Chris, Daniel, Francesco, Ian, Jackie, Jan, Javi, Klaudia, Olmo, Rashmi, Rivers, Tess and Zack — thank you for making my Oxford years the best time of my life.

I would also like to express my gratitude to my family who, despite the thousands of miles and countless barriers that separated us, were there to encourage and support me all through this journey. Finally, I could not have got through the last year of this DPhil without the tremendous support and understanding of David - thank you for all you have done.

# Abstract

Cyber security information sharing is increasingly playing an important role in improving the organisational and national overall security posture. Efforts in the public and private sectors to foster information sharing initiatives have intensified in recent years resulting in the current complex constellation of sharing organisations, forums, platforms and tools, including threat intelligence management solutions. However, despite the growing interest, a number of questions pertaining to the nature of cyber security information sharing and its success remain unanswered.

This dissertation uses mixed methods to consider *How can cyber security information sharing be made more successful?* In answering this question we draw on practitioners' experiences and collect empirical data to ensure that our conclusions can contribute to practice and theory. As with all evaluation efforts, this dissertation relies on the well-established premise that the success of a process cannot be reasonably assessed without a coherent understanding of the goals it is designed to attain.

Our first contribution therefore provides a nuanced conceptualisation of cyber security information sharing. This includes surveying practitioners for their understandings and attitudes towards different aspects of the process and what it is trying to achieve. It also addresses the disparity among them when it comes to distinguishing between the different forms information sharing can take by proposing a high-level classification of these forms and their objectives.

Our second contribution examines the extent to which the benefits and barriers to successful cyber security information sharing mentioned in the literature are reflected in the attitudes of cyber security professionals. A categorisation of the benefits and barriers is introduced followed by a self-administered survey of practitioners. The results show a degree of inconsistency between theory and practice. It also highlights quality issues as a primary concern for practitioners and a hindrance impacting the success of these efforts.

Our third and main contribution is two-fold. First, we investigate the quality problem further in the context of threat intelligence platforms. Through a systematic review of the literature and a modified Delphi study we identify a set of quality dimensions practitioners employ in determining the quality of the platform's content. Second, we draw together the previous findings, as well as the theories and practices of information systems literature to develop and test a holistic success model — a framework for understanding and measuring the key success factors and their interrelationships — for threat intelligence management platforms.

# Contents

**List of Figures** **xi**

**List of Tables** **xiii**

**List of Abbreviations** **xv**

**1 Introduction** **1**
1.1 Overview . . . 1
1.2 Contributions . . . 4
1.3 Structure . . . 5
1.4 Publications . . . 6

**2 Background and Motivation** **9**
2.1 Cyber security information sharing . . . 10
2.1.1 Overview . . . 10
2.1.2 A brief history . . . 11
2.1.3 Definition and classification . . . 12
2.2 Threat-centric information sharing . . . 14
2.2.1 From information sharing to threat management . . . 15
2.2.2 Threat intelligence sharing ecosystem . . . 16
2.2.3 Threat intelligence management platforms . . . 17
2.3 Information systems success . . . 20
2.4 Data and information quality . . . 22
2.4.1 Quality in traditional intelligence . . . 23
2.4.2 Quality in cyber threat intelligence . . . 28
2.5 Summary . . . 30

**3 Methodology** **33**
3.1 Phase 1: Conceptualisation . . . 35
3.1.1 First survey . . . 35
3.1.2 Second survey . . . 36
3.2 Phase 2: Model development and validation . . . 37
3.2.1 Part 1: Systematic literature review . . . 37

3.2.2 Part 2: Modified Delphi study . . . 40
3.2.3 Part 3: Hypotheses formulation and testing . . . 43
3.3 Summary . . . 44

**4 Conceptualising Cyber Security Information Sharing 45**
4.1 Survey data . . . 46
4.2 Addressing conceptual ambiguity . . . 49
4.2.1 The sharing content . . . 49
4.2.2 The sharing process . . . 51
4.3 Untangling information sharing activities . . . 52
4.3.1 Threat-centric data sharing . . . 53
4.3.2 Triggers for action . . . 54
4.3.3 Knowledge sharing . . . 55
4.3.4 Expertise sharing . . . 55
4.3.5 Discussion . . . 56
4.4 Determining quality and effectiveness . . . 59
4.5 Summary . . . 61

**5 Cyber Threat Intelligence Sharing: Perceived Benefits & Barriers 63**
5.1 Benefits and barriers . . . 64
5.1.1 Benefits . . . 67
5.1.2 Barriers . . . 70
5.1.3 Summary . . . 75
5.2 Questionnaire development . . . 75
5.3 Results . . . 76
5.4 Discussion . . . 81
5.4.1 Operational level . . . 82
5.4.2 Organisational level . . . 83
5.4.3 Economic level . . . 84
5.4.4 Policy level . . . 86
5.5 Summary . . . 87

**6 Threat Intelligence Quality Dimensions 89**
6.1 Threat data, information and intelligence . . . 90
6.1.1 Cyber threat data . . . 92
6.1.2 Cyber threat information . . . 93
6.1.3 Cyber threat intelligence . . . 93
6.2 Identifying threat intelligence quality dimensions . . . 94
6.2.1 Results of the systematic literature review . . . 94
6.2.2 Results of Delphi round 1 . . . 96

6.2.3 Results of Delphi round 2 . . . 99
6.3 Threat intelligence quality dimensions . . . 99
6.3.1 Accuracy . . . 100
6.3.2 Actionability . . . 101
6.3.3 Interoperability . . . 101
6.3.4 Provenance . . . 102
6.3.5 Relevance . . . 103
6.3.6 Reliability . . . 103
6.3.7 Timeliness . . . 104
6.4 Discussion . . . 105
6.5 Summary . . . 108

**7 A Model for Measuring Threat Intelligence Success 111**
7.1 D&M information systems success model . . . 112
7.2 TIMP characterisation . . . 114
7.3 Theoretical model and hypotheses . . . 115
7.3.1 Constructs . . . 116
7.3.2 Hypotheses . . . 123
7.4 Data collection . . . 123
7.5 Analysis and results . . . 124
7.5.1 Demographics and descriptive statistics . . . 125
7.5.2 Measurement model evaluation . . . 126
7.5.3 Structural model evaluation . . . 131
7.6 Discussion . . . 138
7.7 Summary . . . 140

**8 Conclusions 143**
8.1 Benefits and impact . . . 145
8.2 Future work . . . 146
8.3 Conclusion . . . 147

**References 149**

**Appendices**

**A Questionnaire 1 169**

**B Questionnaire 2 171**

**C Questionnaire 3 173**

**D Questionnaire 4 175**

# List of Figures


1.1 The dissertation's chapters mapped to publications & contributions. 4

2.1 A high level conceptualisation of a TIMP . . . . . 17
2.2 DeLone and McLean's updated information systems success model . 21
2.3 Data quality dimensions proposed by Wang and Strong [71]. . . . . 24

3.1 Overview of the research methodology. . . . . 34

4.1 Different information sharing models according to survey responses. 52
4.2 Survey responses by frequency of participation in each category. . . 57
4.3 Survey responses by the usefulness to participate in each category. . 57
4.4 Survey responses by the willingness to participate in each category . 58
4.5 Survey responses by the difficulty to determine the content quality . 59
4.6 Survey responses by the difficulty to determine the effectiveness . . 60

5.1 Box plot of responses to the survey statements . . . . . 78
5.2 Spearman's rank correlation matrix of questionnaire statements . . 80
5.3 Attitudes towards the operational benefits and barriers . . . . . 81
5.4 Attitudes towards the organisational benefits and barriers . . . . . 84
5.5 Attitudes towards the economic benefits and barriers . . . . . 85
5.6 Attitudes towards the policy benefits and barriers . . . . . 87

6.1 Literature-based quality dimensions grouped by scope. . . . . 96
6.2 Experts' ranking of dimensions in order of importance from high to low. . . . . 105

7.1 DeLone and McLean's updated information systems success model . 113
7.2 Our proposed research model. . . . . 116
7.3 Path coefficients of Partial Least Square (PLS) analysis. . . . . 132

# List of Tables


2.1 Examples of threat intelligence management platforms [47, 49]. . . . 19
2.2 Commonly used threat intelligence standards and protocols [23, 47]. 20
2.3 NATO scale for source and information evaluation [75]. . . . . 26
2.4 Brei's quality dimensions for intelligence products [87]. . . . . 27
2.5 Evaluation matrix for intelligence products based on [82] . . . . . 28

3.1 Studies identified through the SLR grouped by year of publication. 39

4.1 Description of the survey respondents. . . . . 48
4.2 Survey responses presented as median with interquartile range (IQR). 56
4.3 Survey responses presented as median with interquartile range (IQR). 61

5.1 Summary of the benefits and barriers associated with threat intelligence sharing as reported in the literature. . . . . 66
5.2 Description of the survey respondents and their organisations. . . . 77
5.3 Survey responses presented as median with interquartile range (IQR). 78
5.4 Survey responses presented as median with interquartile range (IQR). 79

6.1 Overview of the Delphi panel experts and their organisations. . . . 91
6.2 Experts' agreement with each of the literature-derived definitions. . 92
6.3 Quality dimensions extracted from the literature. . . . . 97
6.4 Experts' agreement with the dimensions in Delphi round 2. . . . . 99
6.5 Final set of quality dimensions for threat data and intelligence. . . . 100

7.1 The model's constructs and operationalisation . . . . . 117
7.2 Research hypotheses. . . . . 124
7.3 Description of the survey respondents and their organisations. . . . 125
7.4 Descriptive statistics of the survey items. . . . . 127
7.5 Assessment of unidimensionality of measured constructs using EFA. 128
7.6 Multicollinearity test using VIF. . . . . 129
7.7 Internal consistency and convergent validity. . . . . 130
7.8 Outer and cross-loadings of each indicator in the model. . . . . 133
7.9 Inter-construct correlations. . . . . 134
7.10 Hypothesis testing results. . . . . 135

# List of Abbreviations

**APT** . . . . . Advanced Persistent Threat

**AVE** . . . . . Average Variance Extracted

**CDXI** . . . . . Cyber Security Data Exchange and Collaboration Infrastructure

**C&C** . . . . . Command and Control

**CERT** . . . . . Computer Emergency Response Team

**CFA** . . . . . Confirmatory Factor Analysis

**CiSP** . . . . . Cyber Security Information Sharing Partnership

**EFA** . . . . . Exploratory Factor Analysis

**ENISA** . . . . . European Network and Information Security Agency

**FCC** . . . . . Federal Communications Commission

**GBDe** . . . . . Global Business Dialogue on Electronic Commerce

**GDPR** . . . . . General Data Protection Regulation

**ICC** . . . . . The International Chamber of Commerce

**IoC** . . . . . Indicator of Compromise

**ISAC** . . . . . Information Sharing and Analysis Centre

**MISP** . . . . . Malware Information Sharing Platform

**NCSC** . . . . . National Cyber Security Centre

**PLS** . . . . . Partial Least Square

**SEM** . . . . . Structural Equation Modelling

**SLR** . . . . . Systematic Literature Review

**STIX** . . . . . Structured Threat Information eXpression

**TAXII** . . . . . Trusted Automated eXchange of Intelligence Information

**TIMP** . . . . . Threat Intelligence Management Platform

**VIF** . . . . . Variance Inflation Factor

# 1 Introduction

## 1.1 Overview

Information systems are facing an increasingly complex cyber threat ecosystem. The unprecedented scale and sophistication of the threats have made it difficult for a single defender to provide around-the-clock protection against all cyber attacks [1]. Consequently, information sharing has emerged as a paradigm where organisations, in addition to collecting data internally, exchange information between themselves in order to leverage collective knowledge and establish a more holistic understanding of the threat landscape [2]. After all, in the absence of information sharing, threat actors can exploit the same vulnerability in multiple targets while each defender is required to individually detect and remedy all attacks.

Information sharing as a form of cooperation has been present in various contexts since long before the advent of the Internet age [3]. However, early efforts at security-focused information sharing can be traced back to the late 1990s when the US Government took the lead in promoting public-private information sharing schemes including the establishment of sectoral Information Sharing and Analysis Centres (ISACs). The initiative was born out of the conviction that higher levels of cooperation and information sharing would significantly contribute to the defence of national critical infrastructure [4, 5].

Throughout the following two decades, recognition of the importance of information sharing continued to grow as increasing volumes of data were being generated and collected. Nevertheless, driven by the perception that sharing initiatives were not advancing fast enough, governments attempted to facilitate the sharing process in various ways, including legislation — as is the case with the Cybersecurity Information Sharing Act (CISA) in the US or through fostering sharing communities such as the UK Government's Cyber Security Information Sharing Partnership (CiSP) programme [6, 7]. The emergence of information sharing as a plausible solution to addressing cyber threats is clearly attested in President Obama's statement that the only way to defend against cyber threats is "through government and industry working together, sharing appropriate information as true partners" [8].

Today, information sharing has been embraced by various communities resulting in the current complex constellation of information sharing organisations on national and regional levels. Aside from government and industry sharing collectives, enterprise organisations have also established homegrown information sharing capabilities, or what has become commonly known as *cyber threat intelligence*, as a response to the increasingly evolved threat landscape. These capabilities are often designed to collect, process and analyse internal as well as external threat information [9]. This trend has created an opportunity and an expanding market[1] for software vendors who have begun to offer organisations various forms of information sharing services often promoted under the umbrella term *Threat Intelligence Management Platform (TIMP)* [3, 10].

Nevertheless, despite the widespread recognition of its potential, a number of issues pertinent to the nature of cyber security information sharing and its success remain unexplored. When it comes to thoroughly distinguishing between the various forms of information sharing and what they are designed to achieve, there is evidence of a degree of inconsistency among different stakeholders. Moreover, there remains a paucity of evidence on the impact and effectiveness of these activities, as well as the ability to measure their value; further, empirical data examining

[1] Global Threat Intelligence Market Size to exceed $13bn by 2025: https://www.gminsights.com/pressrelease/threat-intelligence-market

the success of threat intelligence management platforms is lacking [10–12]. To the best of our knowledge, there have been no attempts to understand or model the various factors that make these platforms successful following their initial adoption. The challenge in addressing these issues stems from the fact that cyber security information sharing requires a great deal of multidisciplinary research. Although the establishment of such efforts is, in most cases, reduced to an exclusive focus on technical aspects, it is an equally significant challenge for policy makers and standardisation groups, as well as social, economic and legal experts [13].

Although measuring traditional information system success has been discussed at length in the literature, there have been no attempts to model the success of a TIMP as a form of an information system. In this dissertation we develop and validate a comprehensive multi-dimensional model for determining the success of a TIMP. To this end, we draw inspiration from DeLone and McLean (D&M) whose interdependent and multi-construct view of information systems success is widely accepted and has been applied to a variety of contexts including information security practices [14–16].

In the light of the above, the overarching question that drives the research discussed in this dissertation is:

*How can cyber security information sharing be made more successful?*

A comprehensive answer at this stage is beyond our scope and arguably unattainable in the foreseeable future given the multidimensional nature of the problem, so we instead consider specific decisions in isolation. Thus, this dissertation reports upon a study that seeks to answer the following questions:

RQ1: *What is the practitioners' understanding of cyber security information sharing and how do they distinguish between its different activities?*

RQ2: *What are the benefits of and barriers to successful implementation of threat intelligence sharing?*

RQ3: *Is it possible to develop a success model for threat intelligence management platforms?*

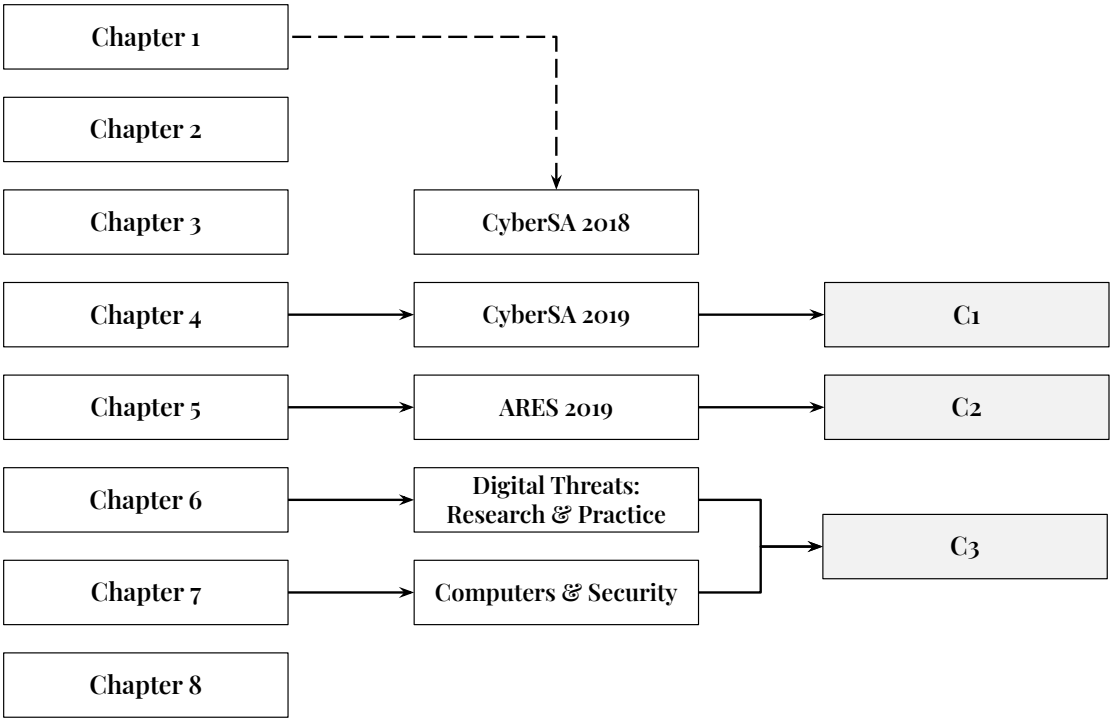



**Figure 1.1:** The dissertation's chapters mapped to publications and contributions.

## 1.2 Contributions

This section identifies which parts of the DPhil dissertation represent novel contributions. Figure 1.1 describes how they map to the chapters and to publications. We summarise each of the contributions in the following.

C1: This contribution captures the practitioners' understanding of cyber security information sharing and what it is designed to achieve. In this study, we review the different definitions of information sharing in the cyber security literature to untangle the different types of activities that appear under the term. It also probes the perceived usefulness and willingness to participate in each of these activities.

C2: This study examines the extent to which the benefits of and barriers to successful threat intelligence sharing suggested by the literature are reflected in real-world practices. In order to do so, we conducted a literature review followed by a survey of cyber security professionals.

C3: Our contribution in this study is two-fold. First, we investigate the quality problem further in the context of threat intelligence platforms. Through a systematic review of the literature and a modified Delphi study, we identify a set of quality dimensions practitioners' employ in determining the quality of the platform's content. Thirty experts from seven European countries participated in the Delphi panel. Second, we draw together the previous findings, as well as the theories and practices of information systems literature to develop and validate a success model for threat intelligence management platforms. A success model is a framework that attempts to describe the causal interrelationships between a diverse set of factors that make a system successful.

## 1.3 Structure

We present a high-level view of how chapters relate to the contributions described in the previous subsection in Figure 1.1. This section outlines the structure of the dissertation and provides an overview of the content of each chapter.

While this first chapter introduces our research questions along with a brief background, the remainder of the study is organised to correspond to our research contributions.

Chapter 2 begins by laying out the theoretical dimensions of the research reflecting the cross-disciplinary nature of our study, and gives a brief overview of the recent history of cyber security information sharing. Its main purpose is to explore the key factors in the evolution of information sharing ideas into commercial threat intelligence platforms. It also includes an analytical review and synthesis of the current literature on data and information quality theories and their application in the traditional intelligence field.

Chapter 3 is concerned with the methodology employed in this study. It discusses the rationale behind the use of a mixed methods research design. It also specifies the data sources, as well as the data collection instruments and procedures for our empirical work. It presents the sequence that links our empirically collected

data to the research's main questions and the results and conclusions discussed in Chapters 4–7.

Chapter 4 provides a conceptualisation of cyber security information sharing by exploring the practitioners' understanding of the term. Based on a literature review and a survey of experts we attempt to untangle the different activities that appear under the term by presenting a categorisation of sharing efforts in the cyber security domain. The study goes on to assess which of those categories stakeholders perceive as more useful and are more willing to participate in.

Chapter 5 explores the extent to which the benefits of and barriers to successful implementation of threat intelligence sharing suggested by the literature are reflected in the attitudes of cyber security professionals. In order to do so, a literature review and a survey of practitioners were conducted. The findings aim to highlight the gap between theory and practice and provide guidance for future research into the challenges to successful threat intelligence sharing.

Chapter 6 introduces a set of data quality dimensions practitioners use in determining the content quality of threat intelligence management platforms. This is the result of a systematic literature review followed by a two-round modified Delphi study. The dimensions identified in this chapter contribute to the development of the model in the following chapter.

Chapter 7 builds on the findings of previous chapters to develop and validate a success model for threat intelligence management platforms. The final model consists of seven constructs and a set of associated hypotheses.

Chapter 8 concludes the dissertation by placing the findings of the study into context. We link our contributions back to our overarching research objectives and discuss their implications for theory and practice before concluding with recommendations for future research.

## 1.4 Publications

I am an author on the following publications:

1. A. Zibak and A. Simpson. Can We Evaluate the Effectiveness of Cyber Security Information Sharing Efforts? In: Proceedings of the 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment. CyberSA 2018. Glasgow, UK: IEEE, 2018.

2. A. Zibak and A. Simpson. Towards Better Understanding of Cyber Security Information Sharing. In: Proceedings of the 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment. CyberSA 2019. Oxford, UK: IEEE, 2019.

3. A. Zibak and A. Simpson. Cyber Threat Information Sharing: Perceived Benefits and Barriers. In: Proceedings of the 14th International Conference on Availability, Reliability and Security. ARES '19. Canterbury, UK:ACM, 2019, 85:1–85:9.

4. (Submitted) A. Zibak, C. Sauerwein and A. Simpson. Towards a Cyber Threat Intelligence Quality Model for Research and Practice. *Digital Threats: Research and Practice*.

5. (Submitted) A. Zibak, C. Sauerwein and A. Simpson. A Success Model for Threat Intelligence Platforms. *Computers & Security*.

Chapter 2 includes text imported from the related work section of paper 1 to paper 5. Chapter 3 contains text from the methodology section of paper 2 to paper 5. Chapter 4, Chapter 5, Chapter 6 and Chapter 7 are derived from paper 2, paper 3, paper 4 and paper 5 respectively.

# 2

# Background and Motivation

This chapter reviews academic and grey literature pertinent to our research questions and lays out the motivation for this study. It also attempts to contextualise the research by providing background information on key concepts and developments in the field.

The first section of this chapter provides necessary background information and a historic overview of cyber security information sharing. It highlights the lack of a thorough understanding of what information sharing is trying to achieve and points to the paucity of empirical research in this area. Section 2.2 explores the evolution of threat-centric information sharing and the emergence of threat intelligence concepts and technologies. Section 2.3 highlights attempts in the literature to model the success of an information system based on several quality constructs and how it can be applied to threat intelligence platforms. Section 2.4 discusses key theoretical concepts in data and information quality followed by a summary of quality evaluation practices in traditional intelligence. The section then examines how these concepts relate to the current attempts to evaluate quality in cyber threat intelligence. The final section ties together these areas and links related work to the content of subsequent chapters.

## 2.1 Cyber security information sharing

### 2.1.1 Overview

Information sharing activities have been gaining momentum and attracting new participants as recognition of their crucial role in improving cyber security and protecting information systems continue to grow [13, 17]. The evolving threat landscape as well as the increasing frequency and sophistication of cyber attacks make it difficult for an organisation to defend itself on its own. Collaboration based on information exchanges is therefore seen as an opportunity to leverage collective knowledge and capabilities across a broad community to protect against a multitude of cyber threats [17, 18].

The growing recognition of the importance of information sharing over the past two decades has manifested in four main developments [19]:

1. The creation of legal and regulatory frameworks to provide a legal basis and to encourage the adoption of cyber security information sharing activities. These regulatory efforts take various forms, ranging from traditional regulation [20], to alternative forms such as self- and co-regulation [21]. Information sharing has also been highlighted as a crucial element in a number of national cyber security strategies [21].

2. The creation of standards and specifications by standardisation bodies to comply with the frameworks mentioned above and to enable efficient information sharing, such as those in [18] and [22].

3. The emergence of national and regional centrally coordinated sharing communities. Examples of recent efforts include, but are not limited to, the UK Cyber-security Information Sharing Partnership (CiSP) in 2013,[1] the Canadian Cyber Threat Exchange (CCTX) in 2016,[2] and the Australian Joint Cyber Security Centre in 2017.[3]

[1] https://www.ncsc.gov.uk/cisp
[2] https://cctx.ca/aboutcctx/
[3] https://www.jcsc.gov.au

4. The development and widespread adoption of sharing solutions to underpin the sharing processes, including threat intelligence platforms and protocols that facilitate the sharing and management of information and help integrate information sharing into organisational cyber security processes [13, 23].

### 2.1.2 A brief history

Early calls for cyber security focused information sharing can be traced back to the late 1990s when the President's Commission on Critical Infrastructure Protection was tasked with preparing a comprehensive study on the security of all infrastructure systems in the US [4]. In its final report, the commission highlighted information sharing between all critical infrastructure stakeholders as "the most immediate need" for the protection of those systems [4].

In line with the commission's recommendations, the US Government urged individual sectors to embrace public-private partnerships and to establish Information Sharing and Analysis Centres (ISACs) designed to exchange information on security incidents and disruptions, as well as best practices among organisations in the same industry. The US financial service companies were the earliest adopters of this scheme in 1999, followed by other sectors shortly after [24].

Following the US's lead, many other governments followed suit and encouraged similar programmes in which information sharing between critical infrastructure stakeholders was facilitated. In 2007, the European Council invited member states to exchange information between relevant government agencies and organisations on a national level and urged network operators and service providers as well as the private sector to "share and implement good security practices" [25].

While governments viewed cyber security as a public good, private sector organisations considered it as a means to maximise profit [26]. Therefore, early debates surrounding cyber security information sharing often focused on the economic incentive. When deciding on whether to share cyber security information or not, firms prioritised their private welfare and in particular their financial interests [27].

According to [28], the voluntary participation in ISACs offered no incentives to encourage full reporting and minimise free-riding, which may have led to organisations under-investing in the development of information security measures hoping to obtain them for free from other ISAC participants. This gap prompted researchers to study the various aspects of information sharing economics [28–30].

Those efforts continued to grow around the world to encompass different organisations that shared geographic region, political boundaries, business interest or threat space [18] resulting in the current complex information sharing landscape.

### 2.1.3 Definition and classification

Asking what cyber security information sharing activities are or what they are supposed to accomplish might seem a simple question with a straightforward answer. In theory, at least, they are designed to share information, and they are meant to do so in order to improve security.

Much like physical attacks, most data breaches and other cyber incidents are seen as security or intelligence failures. A common explanation is that individual pieces of information pertinent to a vulnerability or threat actor were not available to the defender either because they were never collected or because the defending organisations lacked the capacity to act upon the received information. Even if relevant information were known, they were known by different people, organisations or government agencies, and as a result the full picture remained fragmented since the pieces were not available to be analysed together [31]. Although such an explanation ignores the role of hindsight in identifying which of the numerous pieces of information are most relevant, information sharing is often considered as the solution to this problem [31, 32]. Proponents of information sharing argue that by bringing data from various sources together in one place, security teams with the required skills are more likely to spot signs of a compromise or discover vulnerabilities and, by extension, they are less likely to miss signals of imminent threats or system breaches [33].

However, examination of academic and grey literature pertaining to cyber security information sharing, as well as the details of a number of existing sharing activities, reveals a more complicated 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 *information sharing* is used as an umbrella term describing very different systems and efforts that are in many cases seeking to achieve somewhat different goals.

While some acknowledge the confusion surrounding the term and the different meanings it holds [34], others discuss the concept in its broadest form. For example, in [35] information sharing is defined as "the voluntary act of making information possessed by one entity available to another entity." The US Department of Defense in its Information Sharing Strategy elaborates on this definition in saying that it is "making information available to participants (people, processes, or systems)" and that information sharing includes "the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant" [36]. Similarly, in [37], Fleming et al. 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." Such a broad definition is a recurrent theme in the policy literature and debate surrounding this topic. National strategies and policy documents draw the boundaries of information sharing broadly in order to include activities beyond the intuitive concept of "collecting all the dots" in one place so they can be scrutinised [31]. The European Union Agency for Cybersecurity (ENISA) for example refers to cyber security information sharing as "network security information exchanges" that constitute "a form of strategic partnership among key public and private stakeholders" [38]. In another document, ENISA adopts a more technical definition of information sharing as "the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice" [25].

Although there has been an uptake in the number of studies focusing on this area, little academic research has attempted to define cyber security information sharing and almost no study offers a clear and comprehensive definition of the term, reflecting an implicit assumption that the term is self-explanatory. The focus is placed instead on the types of information being shared. For example, the researchers in [39] define information sharing as an activity through which security-relevant information is shared between stakeholders. This information includes "vulnerabilities, phishing, malware, and data breaches, as well as threat intelligence, best practices, early warnings, and expert advice and insight" [39].

## 2.2 Threat-centric information sharing

The cyber threat landscape continues to evolve as more organised and highly sophisticated threat actors have emerged targeting individual end users, businesses and government agencies. Motivated by a range of factors from financial gain to ideological espionage, dynamic, stealthy and persistent attacks gave rise to terms like spear phishing and Advanced Persistent Threats (APTs) [40].

Traditional signature- or list-based defence methods, including firewalls, intrusion prevention systems and anti-virus software, have become increasingly insufficient in the face of the new generation of cyber attacks that aim to bypass known signatures and exploit several unknown and zero-day vulnerabilities on different systems simultaneously [2, 13, 40]. To defend their organisations' systems, security teams and decision-makers require a more comprehensive awareness and understanding of the continuously evolving threats. The flow of cyber threat information is therefore of critical importance in order for them to swiftly adapt their systems to new threats and minimise human delay in information sharing [13]. Information pertinent to cyber threats can be obtained from a variety of sources, including sharing communities, open-source and commercial feeds as well as the organisation's internal networks, and can range from low-level Indicators of Compromise (IoCs) such as known malware hashes and command-and-control (C&C) server IP addresses to

higher-level threat information including threat campaigns and attackers' behaviour and methods [2].

Libicki in [6] notes that threat-centric information sharing has in recent years become the most prevalent form of sharing and has, in many cases, overshadowed other types of equally if not more useful information like best practices and vulnerability disclosures. This observation is supported by industry standards in which threat-based data is the main focus [18, 41]. Threat data is commonly defined as any data related to a threat that might help organisations protect themselves against a threat or detect the activities of an adversary [18].

This type of information exchange has become known as *cyber threat intelligence sharing* (or simply *threat intelligence sharing*). The accuracy of this widely used term is still contested. As [10] points out, the "Intelligence" being shared through the majority of sharing communities does not constitute intelligence in its strictest definition. This is mainly because the production process does not follow the traditional intelligence cycle, which includes planning, data collection, analysis and dissemination [42]. Most of those platforms are merely data warehouses with limited analysis and visualisation capabilities [10].

### 2.2.1 From information sharing to threat management

Information sharing including threat intelligence programmes has become a major trend as organisations continuously wonder what they are overlooking and continue to collect more data [2]. However, organisations have traditionally approached information sharing using ad-hoc solutions and mechanisms ranging from informal conduits such as a phone calls, emails, distribution lists and web-based collaboration tools such as portals and wikis, to more formal arrangements such as working groups, professional conferences and tabletop exercises [43, 44].

With an increasing amount of data being collected, the need for automating and standardising the collection, analysis and sharing processes has become imperative to cope with the sheer speed of cyber threats [44–46]. Manual information handling is seen as labour-intensive, inefficient and time-consuming, which renders information

rapidly irrelevant [47]. According to a Ponemon Institute survey conducted in 2017, 44% of participants stated that slow and manual sharing processes hinder full participation in information sharing, while 37% answered that slow and manual sharing processes stops them from sharing at all [48]. The automation and standardisation of information sharing practices provides an effective pathway for information to be exchanged between multiple parties by simplifying or speeding up the sharing, documentation, assessment, or remediation of security information [23]. The automation of information sharing is also seen as an opportunity for smaller organisations to benefit from mature organisations' experience, as many of them do not have the resources to develop an independent cyber security programme [10, 45]. This has resulted in the proliferation of various information sharing ontologies and threat intelligence management tool-sets such as those discussed in [13]. It has also encouraged organisations to set up or expand their threat intelligence capabilities and practices that enable them to collect, analyse and disseminate internal as well as external intelligence [49].

### 2.2.2 Threat intelligence sharing ecosystem

Threat intelligence sharing programmes are comprised of processes, technology and participants [49]. Participants in this context are not limited to individuals but can range between a non-affiliated individual on one end to companies and government entities on the other end [45]. Participants' interaction may be formal or informal and result in the exchange of various types of cyber threat-centric information in order to help other participants recognise, understand, process and respond to threats [50].

A successful threat intelligence sharing programme allows participants to come together with minimal friction. Although participants can act in different roles within this system, according to [45], each participant in a single transaction must have a well-defined role in order for the system to succeed. The authors of [45] distinguish between the following roles within the threat intelligence sharing ecosystem:

- Information producer: the entity that composes a piece of information for dissemination.

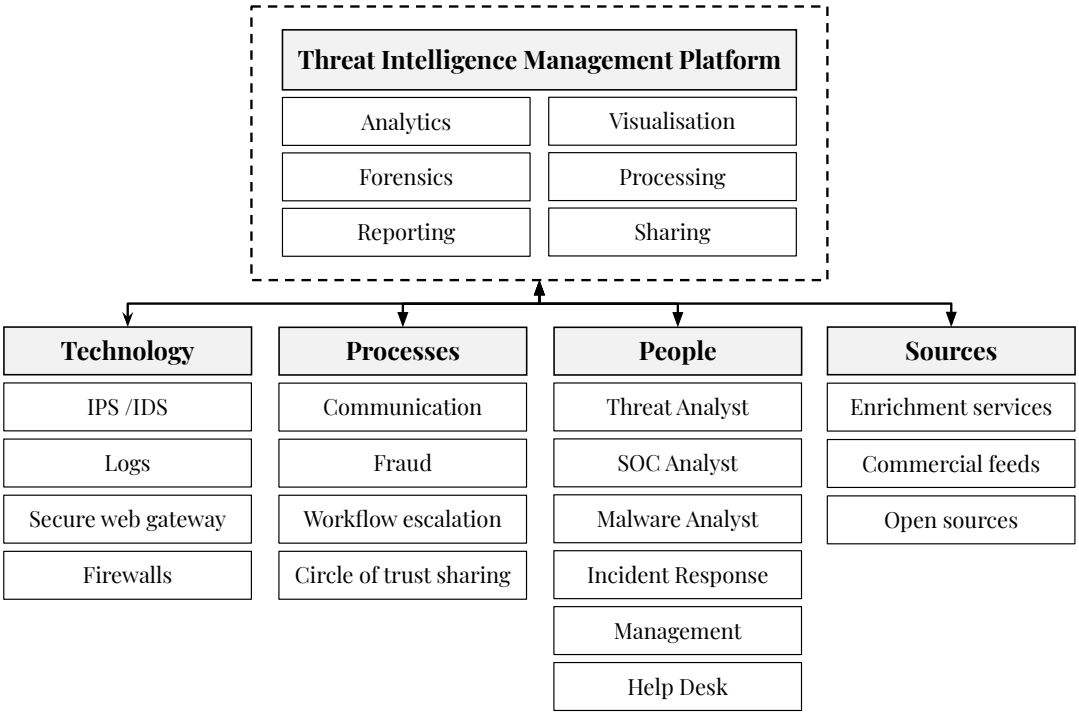



**Figure 2.1:** A high level conceptualisation of a TIMP, adapted from [49].

- Information provider: the entity that disseminates the information to the repository. This may not always be the same as the information producer.
- Information consumer: the entities that consume a piece of information.
- Information broker: the entity that arranges or facilities the production and consumption of information between two or more participants.

### 2.2.3 Threat intelligence management platforms

The growing interest in gathering and sharing threat data, as well as the increasing diversity of open and commercial data sources, has resulted in information overload and created a need for effective search and discovery tools [2]. Furthermore, considering the speed at which cyber attacks unfold, timely decision-making has become essential [51]. These two requirements created a need for greater automation of some of the processes, as discussed earlier [47, 52].

An early conceptualisation of a system designed to collect, analyse, and share cyber threat data was introduced in a US patent in 2000 [53]. In addition to collecting and storing data from multiple sources, the system can also filter, tag,

classify and eliminate redundant data before sharing them with various stakeholders. The authors of [51], however, were the first to specify high-level requirements for a knowledge management infrastructure specifically designed for cyber security threat intelligence called *Cyber Security Data Exchange and Collaboration Infrastructure (CDXI)*. Similar systems later became known as *Threat Intelligence Management Platforms (TIMPs)* or *Threat Intelligence Sharing Platforms (TISPs)* [2, 44].

A TIMP aims to manage threat data and transform it into actionable information that can be fed into different tools and disseminated to relevant stakeholders [2]. Dandurand and Serrano outlined three main objectives for a Threat Intelligence Management Platform [51]:

1. It facilitates information sharing.
2. It enables automation.
3. It facilitates the generation, refinement and vetting of data through burden-sharing collaboration or outsourcing.

Despite still being an emerging technology, TIMPs have become the centre of organisations' threat intelligence and incident response programmes. Proponents of those platforms argue that they help improve organisations' overall cyber security posture by enabling security teams to streamline the core processes of collecting, classifying, enriching, correlating, analysing and sharing threat information [49]. A TIMP's role in threat management operations is illustrated in Figure 2.1. The platform can receive, process, analyse, visualise and share threat data from one or more sources including commercial and open-source feeds. People with different roles within the organisation can use the platform in order to produce a comprehensive report and formulate recommendations for a set of measures to be taken. Actions can be taken by utilising a number of integrated processes and technologies (Figure 2.1).

The growing interest in TIMPs is fostering the growth of the global threat intelligence market, which is expected to surpass $13 billion by 2025.[4] Many

[4]Market Watch. "Threat intelligence market Size Analysis by Key players Trends, Growth Till 2025." marketwatch.com. `https://on.mktw.net/38bBGCP` (accessed January 16, 2020)

| Name | Year | Type | Provider |
|---|---|---|---|
| Malware Information Sharing Platform (MISP) | 2012 | Open Source | CIRCL |
| Collective Intelligence Framework | 2012 | Open Source | CSIRT Gadgets |
| Collaborative Research Into Threats | 2014 | Open Source | MITRE |
| MineMeld | 2016 | Open Source | Palo Alto |
| Yeti | 2017 | Open Source | Yeti |
| ThreatStream | 2013 | Commercial | Anomali |
| EclecticIQ Platform | 2014 | Commercial | EclecticIQ |
| scoutTHREAT | 2015 | Commercial | LookingGlass |
| ThreatQ Platform | 2015 | Commercial | ThreatQuotient |
| Fusion | 2018 | Commercial | Recorded Future |
| Open Threat Exchange | 2012 | Community | AT&T Cybersecurity |
| ThreatExchange | 2015 | Community | Facebook |
| X-Force Exchange | 2015 | Community | IBM |

**Table 2.1:** Examples of threat intelligence management platforms [47, 49].

companies are currently offering a plethora of solutions in this area, with different levels of ambition. Those include traditional endpoint security vendors, security service providers, and a new category of specialist threat intelligence vendors. While some solutions serve mainly as data aggregators, others focus on providing a holistic threat management service [2, 10]. Table 2.1 shows examples of both commercial and open source threat intelligence solutions. The primary focus of solutions like ThreatExchange and X-Force Exchange is content aggregation, whereas other solutions like ThreatStream and Fusion offer other management capabilities [2]. However, this gap as noted in [2] is narrowing as content aggregation solutions increasingly seek to offer advanced threat intelligence management features.

Adopting standardised data formats and transport protocols (such as those shown in Table 2.2) in sharing threat data facilitates the automation of threat intelligence collection and analysis. Automation, in turn, enables the rapid sharing, transformation, enrichment and analysis of threat data and allows speedy decision making with less need for manual intervention [18].

A systematic review of 22 TIMPs was conducted by Sauerwein et al. in 2017 [10]. Looking at use cases, intelligence sharing functionalities and collaboration capabilities, they conclude that the Structured Threat Information eXpression (STIX) has become the de facto standard taxonomy for describing threat intelligence. STIX is a formal XML-based language designed to represent a wide variety of cyber

| Name | | Adoption |
|---|---|---|
| STIX | Structured Threat Information eXpression | Extensive |
| TAXII | Trusted Automated eXchange of Indicator Information | Extensive |
| IODEF | Incident Object Description Exchange Format | Extensive |
| CybOX | Cyber Observable Expression | Moderate |
| MAEC | Malware Attribution Enumeration and Characterisation | Moderate |
| VERIS | Vocabulary for Event Recoding and Incident Sharing | Limited |
| OpenTPX | Open Threat Partner Exchange | Limited |

**Table 2.2:** Commonly used threat intelligence standards and protocols [23, 47].

threat information along with actionable details in structured formats that can help with incident response activities across a wide range of use cases [54, 55].

## 2.3 Information systems success

Early attempts to define what makes some information systems successful failed to capture the complex, interdependent and multi-dimensional nature of IS success [56]. With this in mind, DeLone and McLean built upon a comprehensive review of relevant literature to propose a model for IS success that consisted of six interrelated constructs: *system quality*, *information quality*, *use*, *user satisfaction*, *individual impact* and *organisational impact* [14]. The model suggested that the quality of the system and information influence use and user satisfaction. It also suggested that use and user satisfaction influence each other and the individual impacts of the use of the system. Individual impacts, in turn, were proposed to influence organisational impacts of the information system.

The model was subsequently subjected to close scrutiny including a number of modifications [57, 58]. In their follow-up work, DeLone and McLean examined these suggestions and revised their original model accordingly [15]. The updated version, as shown in Figure 2.2, extended the concept of quality to include *service quality* in addition to information and system quality as antecedents of use and user satisfaction. The use construct was also further clarified in the new model by adding the *intention to use* construct to measure the user's attitude. A third and final refinement to the model stemmed from the argument that the impact of an information system can stretch beyond the individual and organisational levels [59].

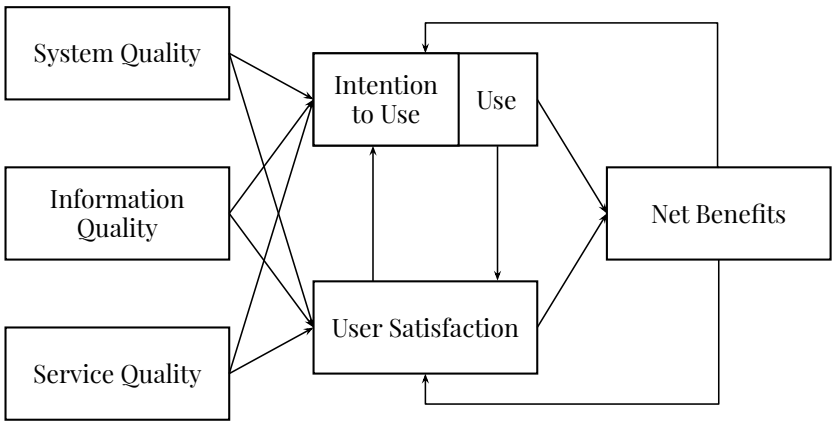



**Figure 2.2:** DeLone and McLean's updated information systems success model [15].

The revised model therefore substituted individual impact and organisational impact with *net benefits* to account for benefits occurring on multiple levels of analysis [56].

The revised model has since been utilised as a framework to guide and organise measuring success factors in information systems [56]. In various applications of the model, researchers derive variables that describe the success of the system in accordance with the six main success constructs of the updated model, which include [15]: *information quality*, *system quality*, *service quality*, *use*, *user satisfaction* and *net benefits*, which refers to the degree to which the system is contributing to the overall success of its users, departments, organisations, industries or societies depending on the context and level of analysis.

Practical application of the success model requires an understanding of the information system and its organisational context. This allows for the selection of appropriate dimensions that are used to measure each of the success constructs [56]. Determining success constructs and the associated metrics depend on the specific nature and objectives of the system being assessed [60].

The DeLone and McLean model has been applied to a variety of contexts. In [16], Montesdioca and Maçada built on the DeLone and McLean model in measuring users' satisfaction with information security practices. A survey of system users followed and structural equations modelling were used to develop a model and test its relationships. Their study was the first to apply the DeLone and McLean model in the context of information security. Other applications of the model include

knowledge management systems [61, 62], e-commerce systems [63], e-government systems [64], and employee portals [65].

## 2.4 Data and information quality

In its basic form, quality is often defined as "fitness for use" [66]. It has also been referred to as "conformance to requirements" [67] and "user satisfaction" [68]. These definitions imply that the concept of quality is not absolute and cannot be determined independently of the consumers [69, 70]. In accordance with quality literature, *data quality* is defined as "data that are fit for use by data consumers" [70, 71].

Data and information quality literature have highlighted the complex and multi-disciplinary process for achieving the desired level of quality due to the variety of information types and information systems [68]. Research in this area has been characterised by the diversity of methodologies, topics and applications, which stems from the cross-disciplinary nature of quality problems as well as the emphasis on the fitness for use definition [72]. Researchers in statistics, management and computer science have investigated various data and information quality issues, further diversifying the related body of knowledge.

However, defining dimensions or attributes to describe or analyse the level of data and information quality has long been considered a cornerstone for most quality-related activities [68, 69]. According to [71], the literature explores three distinct approaches for deriving comprehensive sets of dimension definitions: an intuitive approach, a theoretical approach and an empirical approach. The majority of studies fall under the intuitive approach in which researchers define dimensions based on common sense or their practical experience [73]. The theoretical approach utilises formal models and focuses on the inconsistencies observed with the real world in order to define or justify the dimensions [74]. The drawback of both of these approaches is that they focus on the development features instead of the use features of the product and thus fail to accurately represent the consumer's voice [71]. The empirical approach therefore aims to mitigate this by determining the set of dimensions using experiments, interviews and surveys in order to capture

the attributes that are important to data consumers [68, 71]. A widely cited example of the empirical approach is the hierarchical framework for classifying data quality dimensions proposed in [71] and shown in Figure 2.3. The framework classifies data quality dimensions into four distinct categories: *intrinsic*, *contextual*, *representational* and *accessibility*. Intrinsic dimensions imply that data has quality in its own right, whereas contextual dimensions are those measured within the context or purpose of the data. Both the representational and accessibility categories include quality dimensions influenced by the system [71].

Examining the extensive literature on quality dimensions reveals that there is no general consensus on which set of dimensions defines data or information quality, nor on the precise meaning of each dimension [68]. Regardless of the approach used, the derived dimensions are defined by descriptive sentences with various degrees of specificity [68]. Nevertheless, these dimensions serve as a reference framework allowing organisations to describe and, in some cases, assess the quality of datasets. Furthermore, determining and measuring quality dimensions facilitate comparison with certain benchmark or target values in order to achieve a certain level of quality in the organisation [68]. Therefore, quality dimensions are core elements of any effort to measure or improve data and information quality in an organisation [68]. While the literature on intelligence quality goes back decades, investigating quality issues in cyber threat intelligence in the literature is a more recent and fragmented area of study. Therefore, in the next section we examine efforts to determine the quality of traditional intelligence products and processes. In doing so, we draw on the existing literature and practices to discuss the strength and weaknesses of a number of evaluation concepts and methods. Afterwards, we examine how these concepts relate to the current attempts to evaluate quality in cyber threat intelligence.

### 2.4.1 Quality in traditional intelligence

Evaluation of information quality has been regarded as a core element of the intelligence production process [75]. Poor evaluation of data and information quality has been directly linked to strategic and operational intelligence failures [76].

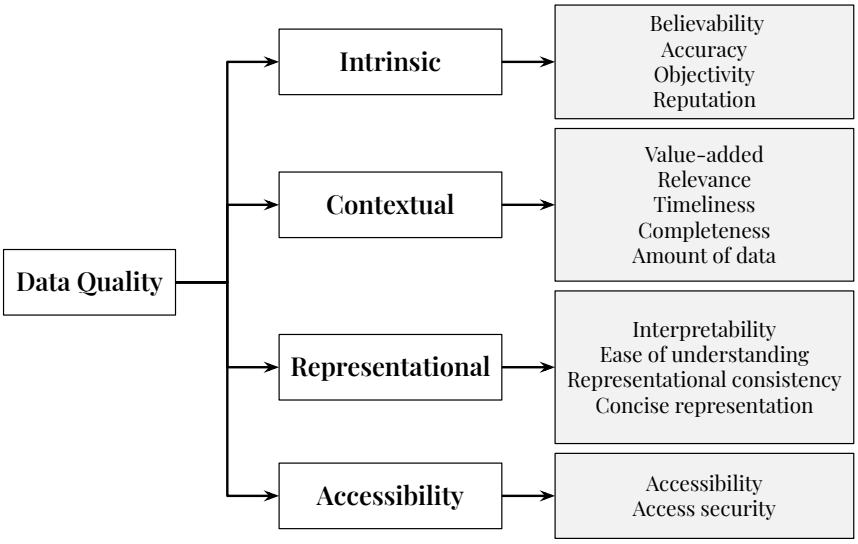



**Figure 2.3:** Data quality dimensions proposed by Wang and Strong [71].

Despite the widespread recognition of its importance, a number of researchers have raised concerns about the current state of quality evaluation in the intelligence community describing it as involving insufficient intellectual rigour and susceptible to being disregarded or trivialised [77]. Quality of intelligence products have largely been assessed using quantitative methods — volumes of processed data, number of reports issued, etc. — or in some cases qualitative measures that rely on consumers' feedback and level of satisfaction [78]. Critics of these approaches argue that counting the number of reports or other intelligence products does not address the questions surrounding the quality of these products and that consumers' feedback suffers from systematic biases [79].

The researchers in [78] argue in favour of an alternative holistic approach to quality evaluation that depicts it as a continuum between two main factors: the intelligence process and intelligence product. In other words, they suggest an evaluation model that factors in the results as well as the means by which the analyst reached those results [80].

### Quality of intelligence process

The literature on evaluating the intelligence process is limited and often relies on studies concerning measuring the quality of decision making in other fields [81].

In [78], a successful intelligence process rests on two main conditions: efficient management including customer and community relations, and rigorous analysis. Traditionally, the intelligence community has relied on a set of quality assurance propositions for intelligence analysis known as the Kent doctrine [82]. These propositions as enumerated in [83] are: 1) focus on policymaker concerns; 2) avoidance of a personal policy agenda; 3) intellectual rigour; 4) conscious efforts to avoid analytic biases; 5) willingness to consider other judgements; 6) systematic use of outside experts; 7) collective responsibility for judgement; 8) effective communication of policy-support information and judgements; and 9) candid admission of mistakes. Elements of high-quality intelligence analytic process are further investigated in [81] in which Peterson presents six main factors that contribute to the analytic confidence: 1) use of structured analytical methods; 2) source reliability; 3) subject matter expertise; 4) amount of collaboration among analysts; 5) complexity of the task; and 6) time pressure.

**Quality of intelligence products**

The literature on evaluating intelligence products quality points to a number of evaluation frameworks that have been adopted by intelligence analysts worldwide. Among those systems is the widely-used Admiralty System, also known as the NATO System, through which a particular piece of information is evaluated along two dimensions: source reliability and information credibility [84]. Information is independently graded on two distinct scales as shown in Table 2.3, resulting in a rating expressed through the corresponding alphanumeric values.

A more detailed version of the Admiralty System, known as STANAG 2511, provides a qualitative explanation for each of the values on the reliability and credibility scales [85]. Source reliability is mapped to the *confidence* in that source determined upon past performance, while information credibility indicates the degree to which this particular piece of information conforms to previous accounts [85]. Organisations around the world have adapted this model to meet their needs. For example, the police service in the UK uses a variant of the Admiralty Scale

| Source reliability | Information credibility |
|---|---|
| A - Completely reliable | 1 - Confirmed by other sources |
| B - Usually reliable | 2 - Probably true |
| C - Fairly reliable | 3 - Possible true |
| D - Not usually reliable | 4 - Doubtful |
| E - Unreliable | 5 - Improbable |
| F - Reliability cannot be judged | 6 - Truth cannot be judged |

**Table 2.3:** NATO scale for source and information evaluation [75].

commonly known as the $5 \times 5 \times 5$ system. In addition to source reliability and information credibility, the $5 \times 5 \times 5$ model rates the handling sensitivity of the information against a third dimension [86].

Critics of the Admiralty System and its variations argue that the scale does not itself evaluate information but, rather, it collates already evaluated information [75]. They point out various limitations of the model pertaining to the subjective interpretations of the boundaries between the scale's scores, as well as the implicit treatment of the source reliability as a constant regardless of the context and the nature of the information reported [85].

The reliance of intelligence analysts and their managers on subjective and often intuitive evaluation methods stems from the lack of explicit consumer feedback regarding the quality of the intelligence. Without constructive feedback from the consumer, analysts are unsure whether the intelligence they provide is fit for purpose [78].

Brei's evaluation framework [87] is often mentioned as a more effective method of quality evaluation as it is built around the consumer's needs and therefore ensures that the intelligence product is aligned with its purpose [78]. The framework is built on six core values that, according to Brei, provide specific qualitative objectives and standards against which intelligence products can be evaluated. Despite being consumer-oriented, the framework could still be utilised for self-evaluation in the case where consumer feedback is not available. It is important to note that those dimensions can overlap, reinforce or interfere with each other — unverified intelligence can diminish the accuracy of the product as well as its relevance to the

| Dimension | Definition |
|---|---|
| **Readiness** | Intelligence systems must be responsive to existing intelligence requirements of consumers at all levels. |
| **Timeliness** | Intelligence must be delivered while the content is still actionable under the consumer's circumstances. |
| **Accuracy** | All sources and data must be evaluated for the possibility of technical error, misperception, and hostile efforts to mislead. |
| **Objectivity** | All judgements must be evaluated for the possibility of deliberate distortions and manipulations due to self-interest. |
| **Usability** | All intelligence communications must be in a form that facilitates ready comprehension and immediate application. Intelligence products must be compatible with the consumer's capabilities for receiving, manipulating, protecting, and storing the product. |
| **Relevance** | Information must be selected and organised for its applicability to a consumer's requirements, with potential consequences and significance of the information made explicit to the consumer's circumstances. |

**Table 2.4:** Brei's quality dimensions for intelligence products [87].

consumer [78]. The criteria are used to evaluate the products of the sub-processes of the intelligence cycle as shown in Table 2.5 [82].

In addition to assessing the quality of intelligence process and products, a growing body of literature explores an analyst-centric approach to evaluation. Proponents of this approach argue that the analyst is a core element of intelligence production [78] and that analysts not only contribute significantly to decision-making processes but they themselves are decision makers continuously forming opinions based on available information [88]. The increasing focus on the analyst's role is demonstrated in two strands of research: defining the attributes of a successful analyst including the related set of skills and knowledge [78, 88, 89], and understanding the analyst's thinking and reasoning processes [75, 90, 91].

Each of the approaches explored above has its own strengths and limitations prompting studies such as [78] to suggest that a comprehensive evaluation system can only be achieved by considering all three strands together, that is, the evaluation of the products, process and personnel. However, although intelligence analysis has been a function of governments and businesses worldwide for decades, when

| | Definition | Collection | Processing | Analysis | Production |
|---|---|---|---|---|---|
| Readiness | | | | | |
| Timeliness | | | | | |
| Accuracy | | | | | |
| Objectivity | | | | | |
| Usability | | | | | |
| Relevance | | | | | |

**Table 2.5:** Evaluation matrix for intelligence products based on Brei's principles [82].

it comes to evaluating the quality of intelligence, different people use different metrics or standards. While studies like that of [75] have attributed this to the limited and superficial nature of the existing evaluation literature, others like that of [92] have argued that the reason behind the lack of a unified evaluation standard stems from the fact that neither practitioners nor scholars have reached a consensus on what intelligence analysis is supposed to do. Evaluating and improving the quality of intelligence analysis according to Marrin, the author of [92], cannot be carried out successfully without determining what the goal of intelligence is and how to best achieve it [92].

### 2.4.2 Quality in cyber threat intelligence

A number of recent surveys have observed an increase in spending on threat intelligence solutions including the adoption of various TIMPs among businesses and governments [93, 94]. With this trend only expected to grow [10], organisations are increasingly seeking evidence for the effectiveness of their investment in threat intelligence solutions prompting increased research into the quality and impact of those platforms. In this section we review attempts by scholars and practitioners to develop threat intelligence quality models.

In addition to the examination of data quality issues in the context of information systems and big data [95–97], useful discussions of data quality models can be found in various aspects of the information security literature including access control policies [98, 99], encryption [100] and incident response [101], as well as risk and compliance management [102, 103].

The authors of [104] were the first to shed light on data quality issues in the context of threat intelligence management platforms. A series of focus group discussions highlighted a number of quality challenges facing intelligence practitioners and end users of TIMPs. The study concluded by pointing out the need for more empirical research in order to gain insights into the true value those platforms provide. This study was followed by a number of attempts to investigate various data and information quality aspects of threat intelligence.

As discussed in Section 2.4, defining quality attributes or dimensions is widely considered as the starting point for any data quality research. Research pertinent to quality in threat intelligence has to a large extent followed this notion. However, the examination of these attempts highlights the absence of an agreement on which data quality dimensions matter the most. This is partly due to the different understandings of what constitutes threat intelligence and varying motivations for each of those studies.

In [105] and [106], the researchers claim that measuring the quality of threat indicators, primarily malware features exchanged in a sharing community, could provide a useful way of assessing individual contributions of members in that community, which in turn could help identify free-riders. They do so by calculating a quality measure for each indicator that is the average of the weighted sum of four components: correctness, relevance, utility and uniqueness. The model proposed in [107] builds on the aforementioned quality measure in order to assign a quality score to the sharing community itself. This score factors in not only the indicators' quality but also the size of the community. Instead of evaluating the quality of an individual indicator or sharing community, the researchers in [108] focus on ranking collections of indicators known as threat intelligence feeds, particularly those that list IP addresses associated with malicious activities. This approach is based on modelling correlations between feeds as a graph on which a ranking algorithm is applied in order to quantify the relative quality of each feed relative to the whole set without a ground truth. Threat intelligence feeds are also the subject of the study presented in [109]. This study identifies and formally defines a set of quality

dimensions in order to assess and compare 47 data feeds providing IP addresses and malware hashes. Formal definitions for an alternative set of dimensions are specified by Schaberreiter et al. in [110], who use it in evaluating trust in a particular source.

Both [111] and [112] enumerate a number of information quality dimensions as part of larger evaluation framework. In [111] the proposed evaluation architecture focuses on creating a quantitative index system that is based on the end user's feedback, whereas the value creation model designed in [112] identifies information quality as one of six value parameters impacting the values of stakeholders in a cyber security information sharing ecosystem. The results in both studies demonstrate the important role of information quality in increasing the value of intelligence sharing for consumers.

Despite some attempts to validate the models presented in the literature, most of them remain largely elementary and cover a limited period of time. Furthermore, all the studies reviewed so far suffer from the fact that stakeholders were typically not involved in determining and defining data quality dimensions. Researchers have adopted an intuitive approach in deriving those dimensions based on their experience, previous studies or what they deemed to be common sense. However, as discussed in Section 2.4, the empirical and semantic validity of the intuitive approach are debatable. Due to their exploratory nature, the models developed using this approach tend to lack a conceptual base and theoretical justification [113].

## 2.5 Summary

The structure of this chapter reflects the cross-disciplinary nature of our research. Section 2.1 covered several aspects of cyber security information sharing that will inform our discussion in later chapters. In Section 2.1.3 we looked at the understanding of the concept in the literature. We found that the majority of relevant studies were limited in scope and there has been limited empirical study of practitioners' attitudes.

This dissertation will focus on how practitioners understand and conceptualise cyber security information sharing, and untangle the different forms it takes

(Chapter 4). This is born out of the belief that assessing the quality of sharing activities can not be carried out rigorously without understanding what those activities are trying to achieve. Section 2.2 examined the evolution of vulnerability information sharing into a threat-centric approach and the consequent emergence of the threat intelligence model. Chapter 5 measures to what extent practitioners' assessment of the risks and benefits of those models align with the assumptions that dominate in cyber security information sharing literature. We discuss our observations in four thematic categories: operational, organisational, economic and policy. The results highlight the severity of poor data quality in current practice and how it has become a primary concern for practitioners and a key factor impacting the effectiveness of information sharing activities.

In Section 2.2.2 we explored the threat intelligence model in more detail including threat intelligence management platforms and the relevant standards and protocols. In Section 2.3 we focused on widely accepted approaches to modelling the success of information systems in the literature. These practices, along with data and information quality theories discussed in Section 2.4, provide important context for understanding how practitioners approach quality issues in threat intelligence. Sections 2.4.1 and 2.4.2 reviewed the state-of-the-art in evaluating the quality of traditional intelligence and of cyber threat intelligence respectively in an attempt to derive useful lessons that feed into the design and analysis of this dissertation's success model in Chapters 6 and 7.

The next chapter discusses the methods used for data collection and analysis.

# 3 Methodology

The research described in this dissertation employed a mix of quantitative and qualitative methods including surveys and semi-structured interviews. To answer the research questions discussed in Chapter 1, we collected and analysed both quantitative and qualitative data in two phases. In the first phase, we used two surveys to conceptualise cyber security information sharing including its definitions, types, benefits and barriers. In phase two, we developed and validated a success model for threat intelligence management platforms.

Mixed methods research can help enhance and enrich the understanding of the phenomenon of interest that cannot be thoroughly understood by a single method [114]. This approach was chosen because it has the potential to answer a wide and more comprehensive set of research questions and can deliver deep insights for theory and practice [115]. Figure 3.1 provides an overview of the research methods and phases. The sequential nature of the design refers to the implementation of the different strands of the research in distinct consecutive phases, with the second phase arising from the first. The research questions addressed as well as the procedures used in one phase depend on the previous phase [116].

In the first phase, we used two consecutive surveys to conceptualise cyber security information sharing and to capture practitioners' attitudes and understandings of its objectives, types, benefits and barriers. The collection and analysis of quantitative

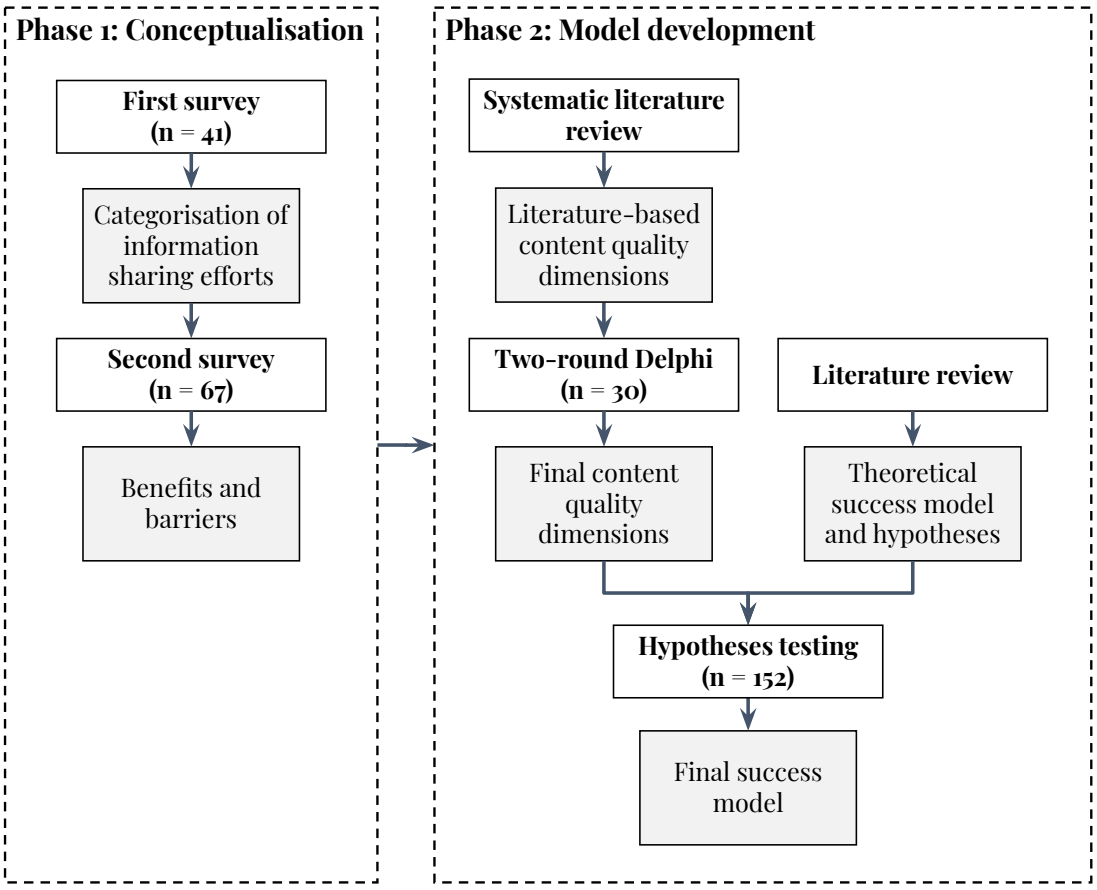



**Figure 3.1:** Overview of the research methodology.

data captures information on various aspects from a wide population and provides results that can be used in identifying trends and patterns [117]. The findings of this phase refined and directed the focus and procedures of the subsequent phase [116].

The second phase was dedicated to the development and validation of a success model for threat intelligence platforms. In this phase, we employed a systematic literature review followed by a two-round Delphi study to identify and define a set of content quality dimensions. These dimensions, along with observations from the literature, were later used to develop and test the hypotheses and success model. The use of qualitative methods in this phase provided an opportunity to expand and explore the data from the previous phase in more depth with fewer participants [117].

Given the limited empirical research in this area, the approach outlined above was deemed appropriate as it allowed for initial information to be collected through two separate surveys and then explored in more depth in a second phase.

The rest of this chapter is structured in accordance with the research phases. Section 3.1 describes the conceptualisation phase. Section 3.2 provides a detailed account of the model development and testing process. Section 3.3 offers a summary of this chapter.

## 3.1 Phase 1: Conceptualisation

### 3.1.1 First survey

The purpose of the first survey was to explore the conceptual ambiguity surrounding the use of the term *cyber security information sharing* by examining the stakeholders' understanding of the term and the different types of sharing.

#### Subjects

Since our main focus was the experiences and attitudes of practitioners towards cyber security information sharing, we targeted UK-based cyber security professionals with at least one year of working experience and direct involvement in cyber security information sharing efforts. These efforts can range from a simple project where one organisation gives information pertinent to specific security incident to another, to a complex multiparty effort to create a common information resource that they all use.

#### Survey instrument

We developed an anonymous, web-based questionnaire to capture the participants' views. In addition to background information about the participants and their organisations (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 types 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 participant's organisation. The questionnaire is presented in Appendix A.

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-point Likert-type scale; 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-ended questions that allowed respondents to expand on their responses.

### 3.1.2 Second survey

The results of the first survey highlighted the practitioners' concerns regarding the usefulness and level of participation in some types of information sharing efforts. In particular, threat-centric data sharing was the most popular category of sharing among the participants despite being perceived as the least useful. The second survey, therefore, aimed to investigate the reasons behind such inconsistency by examining the extent to which the benefits and barriers suggested in the literature are reflected in practice. We started by analysing relevant grey and academic literature on the benefits and challenges of information sharing in cyber security. Given the practical and novel nature of the field of interest, it was important to examine the state of the practice as well as the relevant academic literature. As such, we examined grey literature including white papers and think-tank reports in addition to academic literature [118]. A similar approach was adopted in [10] in order to compile a list of threat intelligence management platforms used in research and practice.

We grouped the findings into four categories: operational, organisational, economic and policy. The resulting compilation of benefits and challenges served as the basis of our subsequent online questionnaire. This categorisation aims to reflect the complex and multidisciplinary nature of the topic. It was largely based on earlier classification attempts such as those in [25] and [119].

#### Subjects

Similar to the criteria in the first survey (Section 3.1.1), the participants were UK-based cyber security professionals with, this time, a minimum of two years

experience in information sharing.

**Survey instrument**

The applied search and selection strategy identified around 38 items that were used in deriving the questionnaire's statements.

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. The questionnaire is presented in Appendix B.

## 3.2 Phase 2: Model development and validation

The second phase of the research consisted of three parts. First, we conducted a systematic literature review to identify preliminary definitions of the terms *threat data*, *information* and *intelligence*, as well as to extract a set of literature-based content quality dimensions for TIMPs. Secondly, we used a modified two-round Delphi study with a panel of 30 experts to revise and validate the final set of content quality dimensions. In the third part, we built on the findings of the research thus far to develop and validate a success model for TIMPs. Data collection in this phase was completed in collaboration with Clemens Sauerwein at the University of Innsbruck.

### 3.2.1 Part 1: Systematic literature review

A systematic literature review (SLR) is an explicit and reproducible research method that is typically used to systematically identify, evaluate and interpret the existing body of research pertinent to a study's area of interest [120]. We performed an SLR to extract quality dimensions mentioned in the literature with a view to developing a data quality model. We designed and conducted the review in accordance with the guidelines proposed by Kitchenham and Charters [121] which included the following steps: creating search and selection strategy; conducting the search, selecting the papers and extracting the relevant data; and reporting the results.

**Search and selection strategy**

A systematic search of the literature was carried out between August and September 2019 in order to identify the review's primary sources.

The following search string was derived from our research objectives and previous work, and was adapted to comply with each engine's settings: *(security) AND ((“information quality”) OR (“data quality”) OR (“intelligence quality”))*. It was applied to the title, abstract and keywords of the articles included in eight repositories: IEEE Xplore, ScienceDirect, Wiley, ACM Digital Library, AISEL, Taylor & Francis, MISQ and Springer. The search was limited to studies published between 2014 (the year the term *threat intelligence management platform* was coined by Dandurand and Serrano [51]) and 2019 (the year that the review took place). This yielded a total of 523 papers.

After discarding duplicates, the full list of papers identified by the searches was evaluated against our initial exclusion criteria. They were as follows:

- Papers that are written in languages other than English.
- Papers that are not available in full-text.
- Papers that are not relevant to cyber or information security.
- Papers that are not published in a peer-reviewed proceeding or journal.
- Papers that do not focus on quality dimensions, characteristics, attributes, models, metrics or assessment methods for data, information or intelligence.

As a result, a total of 24 papers were selected. A preliminary review of the papers' titles followed by a complete or partial reading of the articles that had not been excluded in the previous phase, led to the identification of 11 irrelevant articles. Using the remaining 13 studies as a foundation, a snowballing search [122] was conducted. The reference list of each of the 13 articles, as well as their citations, were reviewed for additional potentially relevant articles. A further nine relevant articles were added to our sources list.

| Year | Study | |
|---|---|---|
| **2014** | Mu et al. [123] | |
| **2015** | Montesdioca and Maçada [16] | Sillaber and Breu [102] |
| **2016** | Sillaber et al. [104] | Sicari et al. [124] |
| **2017** | Mohaisen et al. [105]<br>Wagner et al. [125] | Li et al. [109]<br>Shamala et al. [126] |
| **2018** | Meier et al. [108]<br>Qiang et al. [111]<br>Phua and Ko [96] | Park et al. [106]<br>Bertino et al. [99] |
| **2019** | Rashid et al. [112]<br>Li et al. [127]<br>Schaberreiter et al. [110]<br>Sillaber et al. [103] | Chandel et al. [107]<br>Wagner et al. [128]<br>Talha et al. [95]<br>Grispos et al. [101] |

**Table 3.1:** Studies identified through the SLR grouped by year of publication.

Finally, 22 papers were selected to the next phase of data extraction (Table 3.1). Of these studies, 12 focused mainly on threat intelligence while the rest focused on quality dimensions in other aspects of information security but were considered useful to the development of our model. The full results are discussed in Chapter 6.

### Data extraction

Each of the 22 selected papers was read thoroughly to extract relevant quality dimensions or models. Where available, we also recorded the corresponding definition or context for each of the dimensions as stated in the studies to better understand what they meant. This allowed us to merge some dimensions with identical or similar meanings in order to simplify the resulting model. For example the *Volume* dimension in [127] was merged with *Amount of data* dimension mentioned in [126] into a single dimension.

According to each paper's stated focus, we categorised the identified dimensions into three groups: data quality dimensions, information quality dimensions and intelligence quality dimensions.

### 3.2.2 Part 2: Modified Delphi study

We chose the Delphi method [129] to systematically capture expert opinions with the aim to refine and validate our literature-based quality model. The Delphi method is an iterative process through which a group of subject experts is consulted anonymously over several rounds [129]. In each round, they receive feedback and have the opportunity to revise their assessments. The process usually concludes when a defined consensus is reached [130]. In this study, we defined consensus as agreement between the experts on including a quality dimension. We set 66.7% as a minimum level of agreement on any particular dimension in order for it to be included [131]. Although the number of rounds varies depending on the purpose of research, two or three iterations are usually sufficient [132]. Our study is a modified two-round Delphi study since the first round is structured around the results of the literature review [133].

The Delphi method is a well suited tool for building a consensus with respect to a complex issue [134]. It has been used in various fields to develop a complete range of alternatives, explore or capture underlying assumptions, and correlate opinions on an issue spanning a range of disciplines [135]. The Delphi method does not require proximity or a face-to-face meeting, which allows communication among panellists regardless of geographical constraints [136]. This allows for experts' independent thought as there is less opportunity for one view to dominate over the rest of the group [137]. The technique also provides anonymity for participants, which encourages creativity and honesty, and reduces the negative influence of group dynamics on the outcomes [136].

Potential expert panel participants were selected from the Open Web Application Security Project (OWASP) and several European security interest groups, as well as through LinkedIn and personal contacts. Participant selection was based on the following criteria: hands-on experience in threat intelligence; availability and willingness to participate; and working for an organisation that operated globally. In total, 30 experts agreed to participate.

At the time of the study, most of the participants were employed at multinational companies operating in the information, communication, financial or insurance sectors. Over half of the experts (53.3%) were located in the UK, with the rest spread across six other European countries. The Delphi study was conducted in collaboration with Clemens Sauerwein at the University of Innsbruck, who helped in conducting and transcribing 11 of the 30 interviews.

**Round 1**

The first round took place between October 2019 and March 2020, during which we interviewed each expert individually. A detailed protocol was developed to guide the interviewer and to guarantee the reproducibility, objectivity and comparability of the interviews. In addition to background questions related to the participants and their organisations, each interview was split into two main parts.

The first part focused on the expert's understanding of the terms *threat data*, *information* and *intelligence*. We asked the expert to indicate the extent to which they agreed with each of the literature-derived definitions using a five-point Likert-type scale. This was followed by an open-ended discussion on how to improve these definitions along with practical examples.

The second part aimed to identify the quality dimensions used in practice and to get feedback on our literature-derived preliminary data quality model. Participants were asked about the quality dimensions they value the most and whether our model contains any irrelevant dimensions. We also discussed existing or potential concrete metrics that can be used to measure any of the identified quality dimensions.

On average, each interview lasted for approximately 30 minutes. We created a transcript document for each interview. Two interviews were conducted in German and their transcripts were translated into English by Clemens Sauerwein at the University of Innsbruck.

The transcripts were then analysed to produce qualitative summaries and extract information relevant to our research [138]. Participants' answers to each question were grouped together and coded. A thematic analysis of the grouped answers

resulted in an updated version of our definitions of cyber threat data, information and intelligence, and a revised quality model.

**Round 2**

The second round was designed to be more specific. All 30 experts were invited to participate in the second round. We presented the panelists with the revised quality model that resulted from the previous round. Using a questionnaire, we asked each of them to indicate the extent to which they agreed with each quality dimension in the revised model (Appendix C). They were also asked to rank these dimensions in order of importance. Their agreement was measured on a five-point Likert-type scale. The percentages of agreement and disagreement were calculated, as were the median and interquartile range of all ratings. As mentioned earlier in this section, consensus was defined a priori as agreement between the experts on rating each quality dimension within a specific round. We set 66.7% as a minimum level of agreement (LA), which meant that consensus was achieved when at least two-thirds of the experts agreed or strongly agreed to include the dimension ('4' or '5' on a five-point Likert-type scale). Experts reached agreement on the refined model in the second round with all dimensions achieving consensus and, consequently, it was not necessary to conduct a third round [131].

**Limitations**

The Delphi method is considered time-consuming and laborious for the researchers and participants, which makes it vulnerable to drop-outs and low response rates. If a certain number of the panellists withdraw their participation in any stage of the Delphi process, the quality of information obtained could be affected [135]. To minimise this risk, we informed the panellists of the process and expectations at the outset, and we maintained effective communication throughout the process by providing regular updates and timeline reminders [139].

The generalisability of the results to a wider population is limited by the inherent constraints of the Delphi method. By definition, the method relies on a limited non-representative sample of experts to examine complex, multi-disciplinary

problems [134]. We tried to minimise the impact by recruiting a large panel of 30 experts from around Europe representing a number of sectors. We also tried to overcome recruitment bias by using a form of snowball or referral sampling to ensure access to groups beyond our immediate circle.

### 3.2.3 Part 3: Hypotheses formulation and testing

In line with the established practices of information system success studies [65], we developed and employed a survey-based approach to collect the data required for the empirical assessment of our theoretical success model. Quantitative methods are generally preferred to qualitative research when it comes to hypotheses testing [140].

#### Survey instrument and pretest

Our primary measurement tool was a self-administered questionnaire based on previous empirical research. To ensure content validity we thoroughly examined relevant empirical and theoretical literature covering studies in both the information systems and threat intelligence fields. This was used in identifying the appropriate operational definitions and measures for each of the constructs. The questionnaire was then pretested for readability, clarity and ease of comprehension. We first discussed the draft within our research team and modified it accordingly. Next, 15 threat intelligence specialists were invited to examine and comment on the wording and layout of the questionnaire to ensure face validity. As a result, we finalised the questionnaires' presentation and instructions including the rewording of eight items and the removal of one. We discuss the constructs and their operationalisation in more detail in Chapter 7.

In addition to questions regarding the respondent's background, all seven constructs in our model were measured using a seven-point Likert-type scale with 1 = 'strongly disagree', 7 = 'strongly agree', and 4 = 'neither agree nor disagree' (Appendix D).

## 3.3 Summary

This chapter is concerned with the methodology employed in this dissertation. Data collection and analysis are conducted over two main phases. In the first phase we survey practitioners and analyse the literature to understand the different types of cyber security information sharing and the challenges they face with the aim to bridge the gap between theory and practice.

The empirical observations of the first phase inform our modelling decisions in the second phase, which builds on information system theory [14, 15] in developing and testing a success model for threat intelligence platforms.

# 4

# Conceptualising Cyber Security Information Sharing

A well-defined understanding of what cyber security information sharing activities are designed to achieve and what the intended outcomes are, is required to ensure successful implementation and evaluation of those efforts [141].

Identifying what such activities are meant to achieve seems (in theory, at least) a straightforward task. Clearly, within the scope of cyber security practices, they are designed to share information in order to improve cyber security. However, examining the current practice and the details of existing cyber security information sharing activities reveals a more complex reality. From platforms that offer real-time threat information sharing and systems that link one organisation with another, 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 different activities and systems that are in many cases seeking to achieve different goals.

Untangling the different types of information sharing is also crucial if we are to determine the success and effectiveness 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 [141].

In this chapter we discuss the findings of an exploratory survey we conducted with the aim of gaining insights into practitioners' understanding and attitudes towards several aspects of cyber security information sharing. We draw upon the existing definitions as well as respondents' input to develop a more nuanced understanding of the term. We also build on the categories of information sharing proposed in [31] to derive a useful classification of cyber security information sharing activities.

Following an overview of the respondents' profiles in Section 4.1, Section 4.2 presents results on how practitioners define cyber security information sharing activities. In Section 4.3 we propose a high-level classification of those activities. In Section 4.4 we briefly touch on the participants' attempts to evaluate information sharing activities in their organisations, a topic that we will cover in detail in later chapters. We offer conclusions and link the results to the forthcoming chapters in Section 4.5. The work described in this chapter was previously presented as [142].

## 4.1 Survey data

An anonymous, web-based survey was designed to capture practitioners' understanding and attitudes towards several aspects of cyber security information sharing. A detailed discussion of the questionnaire's design is provided in Chapter 3.

Data collection took place between January and March 2018. The primary distribution method was a form of snowball or referral sampling in which participants were asked to distribute the questionnaire 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.

The questionnaire was sent out via email to 63 cyber security professionals with at least one year of working experience from a wide range of industries in the UK, including financial services, manufacturing, and information and communication. A total of 46 completed questionnaires were collected.

To get a sense for how aware respondents were of cyber security information sharing activities 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 sometime in the future. Those five responses were excluded from our analysis.

The top three industries represented were: information or communication (34.1%); finance or insurance (24.3%); and manufacturing (22%). The remaining sectors (19.5%) are shown in Table 4.1. The classification was based on the UK's Standard Industrial Classification of Economic Activities (UK SIC 2007) [143].

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 professionals with at least one year of working experience. Roughly half of those surveyed (48.8%) reported having over five years of work experience. Just over a third (34.1%) had 3–5 years of experience; the rest (17.1%) had less than 2 years of practice. All those who responded had first-hand experience in at least one of their organisations' information sharing activities.

The survey sought to explore maturity levels of cyber security information sharing among the respondents' organisations as can be seen in Table 4.1. To this end, we adopted the maturity model of [9], which takes into account the allocation and training of staff as well as the formality of the collection and analysis processes. The majority of organisations (85.4%) have had a cyber security information sharing programme for less than five years. Only five organisations considered their information sharing activities mature, while half of the sample size regarded their programmes as immature.

| Variable | | Frequency (n=41) | Percentage |
|---|---|---|---|
| **Sector** | Information or communication | 14 | 34.1% |
| | Finance or insurance | 10 | 24.4% |
| | Manufacturing | 9 | 22.0% |
| | Health or social care | 3 | 7.3% |
| | Public Sector or defence | 3 | 7.3% |
| | Retail or wholesale | 2 | 4.9% |
| **Number of employees** | >1,000 | 20 | 48.8% |
| | 250–1000 | 10 | 24.4% |
| | 50–249 | 8 | 19.5% |
| | <50 | 3 | 7.3% |
| **Programme length** | <1 year | 7 | 17.1% |
| | 1–2 years | 14 | 34.1% |
| | 3–5 years | 14 | 34.1% |
| | >5 years | 6 | 14.6% |
| **Maturity level** | Immature | 21 | 51.2% |
| | Maturing | 15 | 36.6% |
| | Mature | 5 | 12.2% |
| **Experience in cyber security** | <2 years | 7 | 17.1% |
| | 2–5 years | 14 | 34.1% |
| | >5 years | 20 | 48.8% |

**Table 4.1:** Description of the survey respondents.

The survey also sought to capture the respondents' attitudes towards different category of cyber security information sharing activities using a five-point Likert-type scale. For each category, the survey tried to capture three variables: the usefulness of this category to the respondent's organisation; the organisation's willingness to participate in it; and the frequency at which the organisation participates in this category. A detailed discussion of these categories as well as the respondents' attitudes will be examined in Section 4.3.

Similarly, to understand the participants' perception of the difficulty of assessing the quality and effectiveness of information sharing activities, a five-point Likert-type scale, where a reply of 1 indicated extremely difficult and a reply of 5 indicated extremely easy, was used.

## 4.2 Addressing conceptual ambiguity

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

While the intrinsic importance of information sharing has been widely recognised, few sources define information sharing as a concept with any specificity as we discussed in Chapter 2. 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.

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* by which the exchange is conducted.

### 4.2.1 The sharing content

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 the terms *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 [144, 145].

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 embedded 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 [146]. It is arguable whether this established distinction between data, information and knowledge is applicable to cyber security information sharing. A detailed discussion of these terms and their use in the context of cyber threat intelligence is presented in Chapter 6.

In our survey responses, a considerable number of participants referred to the exchange of low-level threat-centric data in response to confirmed or potential threat activity as the main purpose of cyber security information sharing. For example, one participant [P13] defined the term as:

> *"For me it's all about receiving and sending indicators of compromise, so things like IP addresses, logs, malware signatures, essentially any data that can help my team detect and respond to threats in a timely manner."*

This understanding was echoed by another participant [P5] who referred to the activity as "collecting dots":

> *"I believe that cyber security information sharing is the exchange of pieces of information regarding specific or even general threats between a number of trusted partners to help [the organisation] collect and connect the dots in order to understand the bigger picture and act accordingly."*

Others however placed greater emphasis on the exchange of best practices and lessons learnt as part of general expertise sharing. For example, one participant stated [P3]:

> *"It's the process through which information security experts share their experiences and the lessons they learnt in the aftermath of a breach or other security incidents with their peers ... sometimes [the sharing] happens in open forums like conferences and workshops and sometimes in a closed or one-on-one setting."*

Similarly, another respondent commented [P22]:

> *"While some of my colleagues would tell you that information sharing is all about sharing threat intelligence and IOCs, I am of the opinion that the sharing of lessons learnt and best practices is far more effective."*

Answering the same question, a couple of participants [P2, P12] pointed to the sharing of time-sensitive alerts prompted by imminent threat or hostile activity that often requires immediate action by the recipient of this information:

> *"It is when we receive actionable information from a government agency like the NCSC or the FBI about a malware or malicious actors and how to defend [our organisation] from them ... those alerts could also come from private security companies with deeper knowledge of the threat."* [P12]

Almost all the participants used the terms *data*, *information* and *intelligence* interchangeably. While the traditional distinction between those terms as discussed earlier is important, it offers little help when trying to untangle the different information sharing activities. A detailed examination of the use of these terms in the context of cyber security information sharing is presented in Chapter 6. We discuss an alternative framework for classifying these activities in Section 4.3.

### 4.2.2 The sharing process

The respondents highlighted in their answers several aspects of the sharing process including with whom the information is shared and the model it follows.

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 as stated in the answers of two participants [P6, P23]:

> *"[Information sharing is] receiving and sending threat data and intelligence with other companies in our industry who face similar challenges and threats."*

> *"we are regularly coordinating and exchanging data with most of our partners especially those operating in the same sector or geographic region."*

However, a few responses expanded on that, saying that information could also be shared *"internally"* [P31], *"with relevant government agencies"* [P9], or *"disclosed to the public"* [P29]. While most respondents discussed information sharing conducted on an organisational level, some answers pointed out that in some occasions information can be shared between *"individuals"* [P1, P17] or *"units"* [P9,

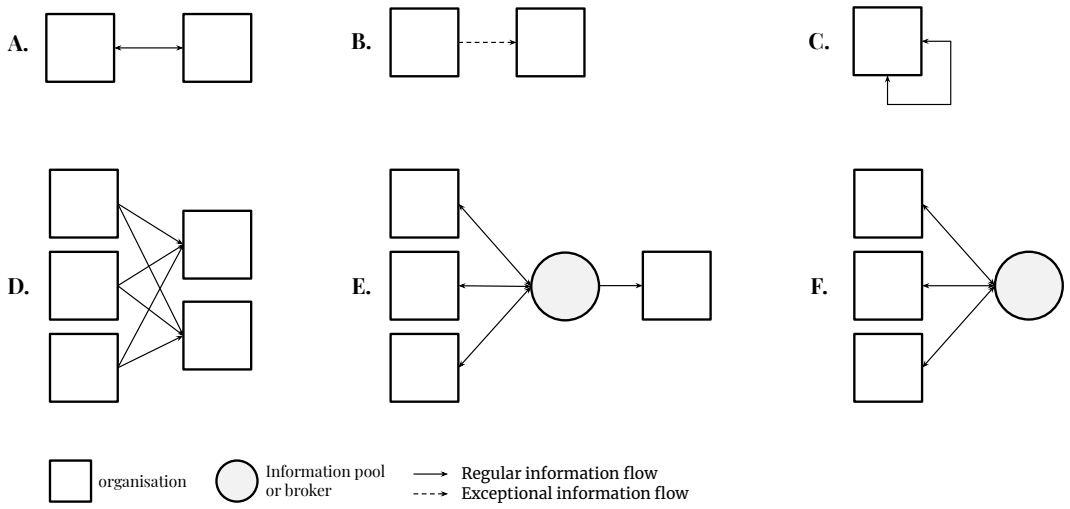



**Figure 4.1:** Different information sharing models according to survey responses.

P35]. Few answers mentioned that the sharing of cyber security information could also be carried out through less formal mechanisms such as *"phone calls"* [P1] and *"emails"* [P5]. The examination of the survey responses has revealed that the sharing process can follow one or several high-level models as illustrated in Figure 4.1:

A. A reciprocal exchange of information between two or more organisations.

B. One-off disclosures of information in time-sensitive or emergency situations.

C. Different parts of the organisation make information internally available.

D. One or more organisations provide information to third parties.

E. Several organisations pool information and make it available to third parties.

F. Several organisations pool information and make it available to each other.

## 4.3 Untangling information sharing activities

In light of the survey responses and the subsequent discussion in Sections 4.2.1 and 4.2.2, we sought to adopt a more nuanced and sufficiently inclusive classification of cyber security information sharing activities and the goals they are designed to achieve.

Current attempts to categorise shared cyber security information (such as those proposed in [18] and [41]) are limited to threat-centric data (i.e. indicators of compromise, vulnerabilities, threat actors, etc.). We seek to adopt a higher level classification that offers a constructive way to discuss information sharing activities and their objectives, and to explore adequate evaluation methods.

Using a small number of categories to simplify subsequent discussion, the authors of [31] propose a classification framework for traditional intelligence sharing activities with a view to capturing most of their intended goals and outcomes. Accordingly, we adopt the framework of [31] and adapt it to meet the requirements of the cyber security sharing landscape. Four types of cyber security information sharing activities are therefore identified. In the following, supported by examples, we highlight how these categories differ in terms of what is being shared and why.

### 4.3.1 Threat-centric data sharing

Threat-centric data sharing activities are designed to transmit specific cyber security data that enables the recipient to have a more complete picture of the nature of the threat, incident or vulnerability. Its main aim is to inform a decision or assessment, or to increase the chance of a successful detection of, triage of, and response to, cyber attack. Consider a situation in which an organisation discovers that it is a target of a data breach and that the attackers have transferred confidential information to an external server. In order to help other organisations in defending against 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 is likely an indication that they are also being targeted with the same attack.

Threat data sharing activities often take the form of clearinghouses or data feeds.[1] For example, IBM's X-Force Exchange, a cloud-based information sharing platform, provides organisations with a range of services including a crowd-sourced

[1] e.g. `https://www.phishtank.com`

list of IPs and URLs of known botnet command and control (C&C) servers. This list could help organisations detect malicious activities in their networks as connections to any of those addresses usually suggests a malware infection.[2]

### 4.3.2 Triggers for action

Instead of disseminating individual data on suspicious IP addresses, malware signatures or phishing emails, some cyber security information sharing activities 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 recipient to an unknown threat or vulnerability.

These notifications and alerts bring to the organisation's attention the need for actions that it 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 Federal Bureau of Investigation (FBI) in the US sent a five-page memo to information security personnel at some US organisations warning them of destructive malware targeting US businesses.[3] 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 reports and advisories feed.[4]

[2]IBM. "Botnet Command and Control Servers". Exchange.xforce.ibmcloud.com. `https://exchange.xforce.ibmcloud.com/collection` (accessed January 23, 2020).

[3]J. Finkle. "Exclusive - FBI warns of 'destructive' malware in wake of Sony attack." Reuters.com. `http://reut.rs/1rQjd31` (accessed January 16, 2020).

[4]National Cyber Security Centre. "Reports & advisories". NCSC.gov.uk. `https://www.ncsc.gov.uk/section/keep-up-to-date/reports-advisories` (accessed January 16, 2020).

### 4.3.3 Knowledge sharing

A variety of information sharing activities 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 a group of organisations. These activities focus on the exchange of information that is often captured in documents, briefs, and other explicit knowledge. In addition to post-breach reports and case studies, some analysis produced by security vendors, such as periodic intelligence bulletins, 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 issues. Those activities can vary in formality and structure. Examples include sector-specific inter-organisational social media systems designed to catalyse direct person-to-person information sharing and educational joint training activities. Systems that provide essential finished cyber intelligence products such as high-level analyses of threat vectors, campaigns or specific trending security topics designed to educate decision makers also fall in this category. For example, FireEye provides its clients with a regular regional or sector-specific intelligence bulletin covering the latest threat trends and predictions.[5]

### 4.3.4 Expertise sharing

Some information sharing activities 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

[5]FireEye. "Intelligence Briefings and Bulletins". Fireeye.com. `https://www.fireeye.com/current-threats.html` (accessed January 23, 2020).

| | **How often does your organisation participate in each of the following?[a] (n=41)** | **How useful does your organisation consider each of the following?[b] (n=41)** | **How willing is your organisation to participate in each of the following?[c] (n=41)** |
|---|---|---|---|
| Threat-centric data | 4 (3-5) | 2 (2-3) | 4 (3-4) |
| Triggers for action | 4 (3-5) | 5 (4-5) | 4 (3-5) |
| Knowledge | 3 (2-4) | 4 (3-5) | 4 (2-4) |
| Expertise | 2 (2-3) | 3 (2-5) | 3 (2-4) |

**Table 4.2:** Survey responses presented as median with interquartile range (IQR).
[a] measured on a five-point Likert-type scale: 1 (never) to 5 (always).
[b] measured on a five-point Likert-type scale: 1 (not useful) to 5 (very useful).
[c] measured on a five-point Likert-type scale: 1 (not willing) to 5 (very willing).

organisation. A prime example of those activities 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.[6] 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.

### 4.3.5 Discussion

When asked about this classification, survey participants expressed a wide range of views. Survey responses, presented as median and interquartile range (IQR) values, are summarised in Table 4.2.

[6]National Cyber Security Centre. "Industry 100". NCSC.gov.uk. `https://www.ncsc.gov.uk/information/industry-100` (accessed January 23, 2020).

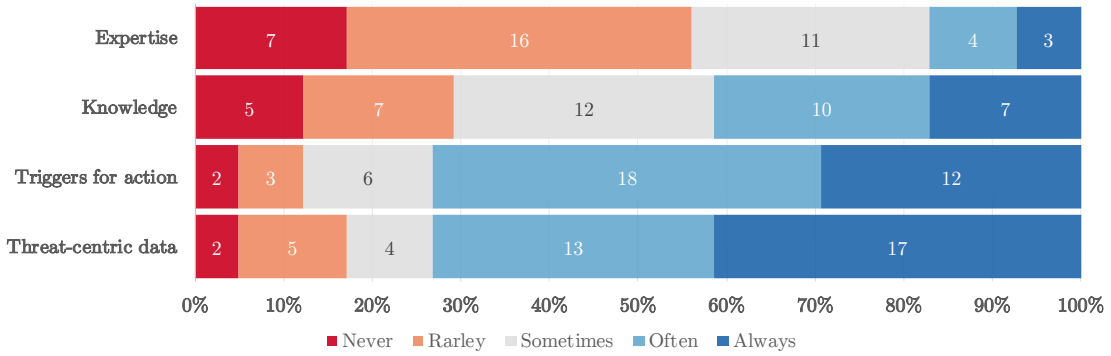



**Figure 4.2:** Survey responses by frequency of participation in each category.

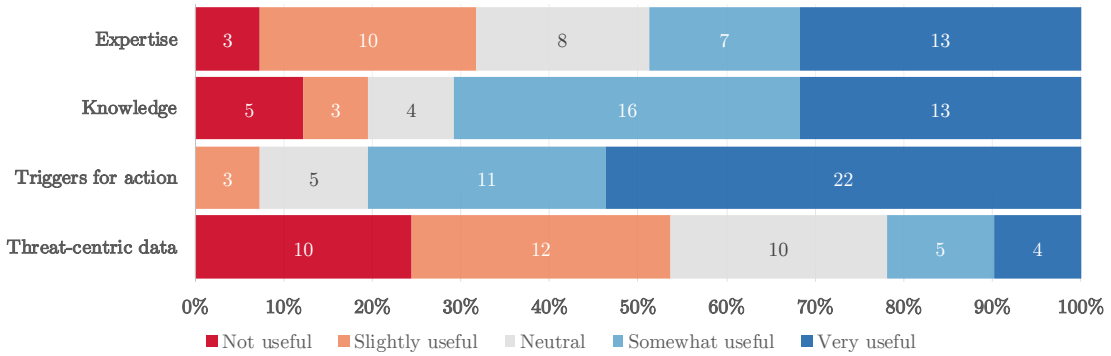



**Figure 4.3:** Survey responses by the usefulness to participate in each category.

Respondents reported varying frequency of engagement with each category. As shown in Figure 4.2, around three-quarters (73.2%) of the organisations reported participating in *threat-centric data sharing* either always or often. The same percentage of respondents (73.2%) stated that they send or receive *triggers for action* either always or often as well. When it came to *knowledge* and *expertise sharing*, participation rates dropped to 41.5% and 17.1% respectively.

These findings broadly support the claims made in [6] where Libicki suggests that, when talking about cyber security information sharing activities, threat-centric information sharing has overshadowed other equally important types of sharing.

The survey also explored stakeholders' thoughts on the usefulness of participating in each of these categories, as well as their willingness to do so. As Figure 4.3 illustrates, when compared to other categories, respondents perceived *threat-centric data sharing* activities as the least useful (median=2, IQR=1). Despite being the most common category, over half of responses (53.6%) said that this activity is

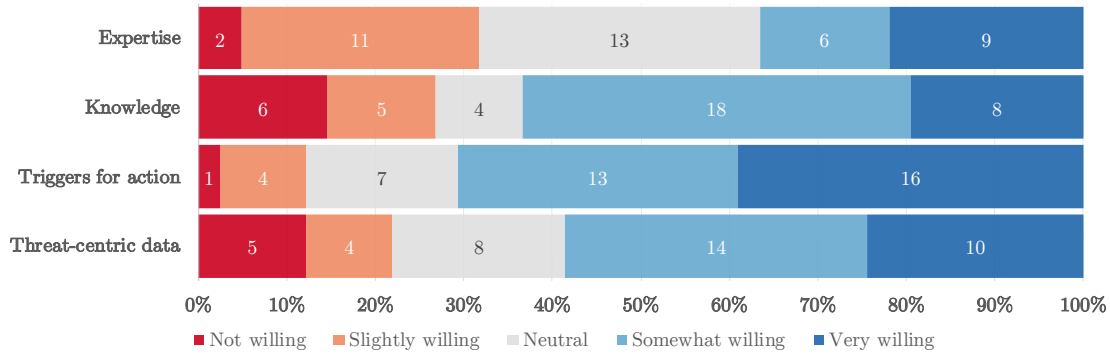



**Figure 4.4:** Survey responses by the willingness to participate in each category.

either slightly or not useful at all. Most participants (80.5%) regarded *triggers for action* as the most useful type of sharing (median=5, IQR=1), followed by *knowledge* and *expertise sharing*. As for the willingness to participate, *triggers for action* scored the highest among a large share of the participants (70.7%) who stated that they are willing to participate, followed by *knowledge sharing* (63.4%), *threat-centric data sharing* (58.5%), and *expertise sharing* (36.6%) (Figure 4.4).

Despite the reported usefulness of *expertise*, *knowledge* and *triggers for action sharing*, survey respondents were less enthusiastic about participating in these activities. One possible explanation could be the *free rider problem* discussed in Chapter 2.

A similar observation of inconsistency between perceived usefulness and willingness to share was made in [147], where 17 UK-based small and medium size enterprises were surveyed to assess the consequences of sharing a particular set of cyber security metrics among the organisations' supply chains. Despite the narrow scope and the small sample size, the study showed that the usefulness variable consistently scored higher than the sharing variable: participants 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.

The four categories presented in Section 4.3 capture the main differences between cyber security information sharing and the main benefits for establishing connections between different organisations. While some information sharing activities are designed to facilitate one of these categories (e.g. data feeds and security portals

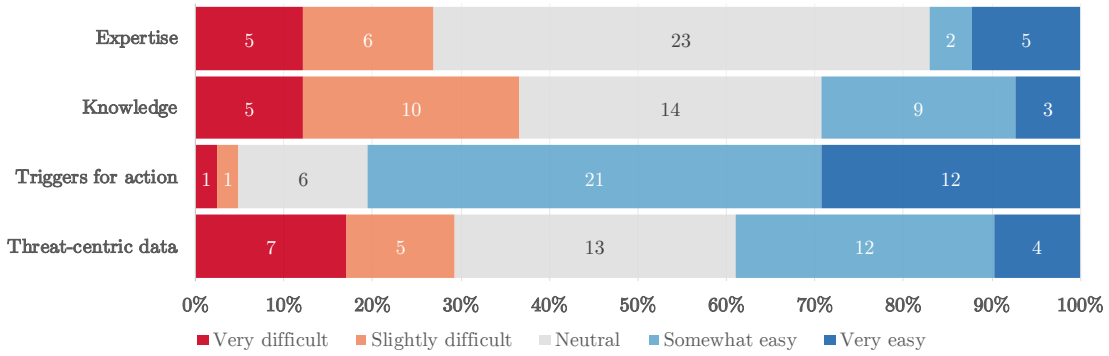



**Figure 4.5:** Survey responses by the difficulty to determine the content quality of each category.

designed for specific sharing functions), others are designed to facilitate several goals at the same time (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. However, it is essential to understand what a sharing effort is trying to achieve in order to decide how to assess its success. Going forward, the dissertation will use the terms introduced in this section to refer to the different types of cyber security information sharing activities.

## 4.4 Determining quality and effectiveness

Despite high levels of participation in some categories of cyber security information sharing such as threat-centric data sharing as shown in Figure 4.2, respondents reported doubts over the usefulness of some of these activities as can be seen in Figure 4.3. This gap is important because as Fleming points out in [148], 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. Without achieving their intended goals, organisations might reconsider their participation in information sharing activities.

In order to further explore the issue of usefulness, the survey was designed to capture the practitioners' perspectives on determining the quality and effectiveness of those activities. This stems from the belief that accurately evaluating the activity and its performance is essential to identifying and remedying any observed shortcomings preventing it from fulfilling its objectives [37, 149].

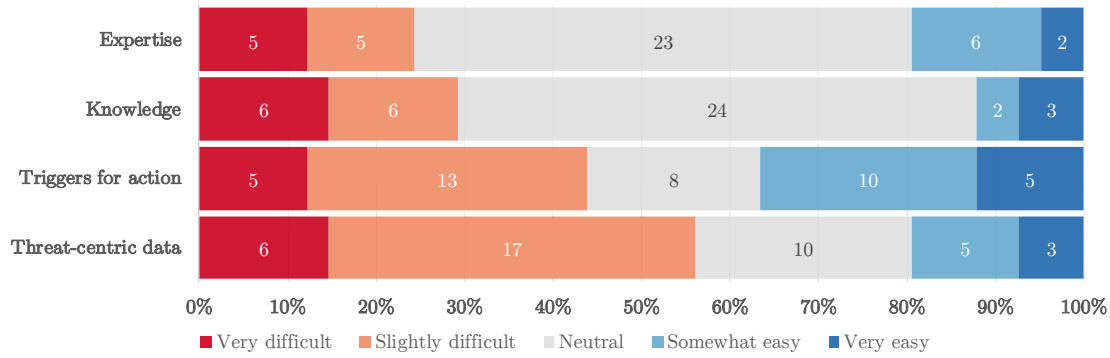



**Figure 4.6:** Survey responses by the difficulty to determine the effectiveness of each category.

We asked the participants several questions to gauge their attitudes towards the difficulty of assessing both the quality of the content, as well as the effectiveness of these activities in terms of their role in decision making. The results are presented as median and interquartile range (IQR) values in Table 4.3 and are illustrated in Figures 4.5 and 4.6.

Most respondents (80.5%) indicated agreement with the idea that determining the content quality in shared *triggers for action* is somewhat or very easy (median=4, IQR=1). There was less agreement among them when asked about the other categories. For example, over half of the participants (56.1%) seemed undecided about the difficulty of assessing the quality in *expertise sharing* (median=3, IQR=1) as can be seen in Table 4.3.

With the exception of *threat-centric data*, where around half of the respondents (56.1%) agreed it was difficult, determining the effectiveness of the other sharing activities seemed less straightforward. Most respondents gave noncommittal answers regarding the difficulty of determining the effectiveness of *expertise* and *knowledge sharing* (median=3, IQR=0; and median=3, IQR=1 respectively).

These results are not surprising as they are in line with general data quality literature [68], as well as previous studies such as [104] in which Sillaber et al. found that the cost and effort required to trace and remedy data quality issues in threat intelligence platforms increase the difficulty of the already complex evaluation process.

| | **How difficult is it to determine the quality of each of the following?* (n=41)** | **How difficult is it to determine the effectiveness of each of the following?* (n=41)** |
|---|---|---|
| Threat-centric data | 3 (2-4) | 2 (2-3) |
| Triggers for action | 4 (4-5) | 3 (2-4) |
| Knowledge | 3 (2-4) | 3 (2-3) |
| Expertise | 3 (2-3) | 3 (3-3) |

**Table 4.3:** Survey responses presented as median with interquartile range (IQR).
* measured on a five-point Likert-type scale: 1 (very difficult) to 5 (very easy).

Despite the perceived difficulty, when asked whether their organisations had methods or metrics in place to determine the effectiveness of their cyber security information sharing programmes and activities, half of the respondents (51.2%) stated that they do not have methods in place, but are interested in establishing them. A further quarter (26.9%) 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 (21.9%) reported having established informal or formal methods.

## 4.5 Summary

Despite the increased recognition of its importance, current research has been slow to address several aspects of cyber security information sharing, with very limited work specifically focusing on the stakeholders' attitudes and understandings. Our first research question therefore set out to examine practitioners' understanding of cyber security information sharing and how they distinguish between its different activities. By collecting and analysing the views of cyber security professionals, this chapter aimed to provide answers to our question by providing insights into their understanding of the current cyber security information sharing practices.

In this chapter we attempted to conceptualise information sharing in cyber security by: (i) addressing the ambiguity surrounding the concept of information sharing and drawing on stakeholders' input to clarify the confusion that arises from the wide use of the term (Section 4.2); (ii) untangling the various types of

information sharing activities by proposing a high-level categorisation that defines the goals each category is trying to achieve, as well as capturing and analysing the participants' views on the usefulness of those categories and their willingness to participate in each (Section 4.3); and (iii) highlighting some of the issues that pertain to evaluating the quality and effectiveness of those efforts (Section 4.4).

The survey showed that *threat-centric data sharing* has dominated cyber security information sharing efforts despite being perceived as the least useful activity. In Chapter 5 we will investigate some of the reasons behind this inconsistency. The survey also revealed that most respondents find it difficult to determine the effectiveness and quality of the data being shared. Nevertheless, they unanimously expressed interest in developing methods to address quality concerns and determine the overall success of information sharing activities. This supports the claim made in [2] that the focus is shifting from creating interoperable sharing tools to operationalising and generating value from those exchanges. This finding will serve as a starting point for the design and development of a success model in Chapters 6 and 7.

The generalisability of these results is subject to several limitations. In addition to the difficulty of verifying self-reported data, due to the time available and resource constraints, our sample size was relatively small. A larger sample size could have yielded deeper insights and allowed for the implementation of further statistical testing and the uncovering of statistically significant relationships.

Although the findings should be interpreted with caution, they provide necessary insights and background information that will guide the discussion in subsequent chapters.

# 5

# Cyber Threat Intelligence Sharing: Perceived Benefits and Barriers

The preceding chapter presented observational data about the current landscape of cyber security information sharing. In addition to providing an insight into how practitioners define and classify various sharing activities, we reported different levels of perceived usefulness and participation in each of them. For example, threat-centric data sharing was the most popular category of sharing among the participants despite being perceived as the least useful.

In this chapter we investigate the reasons behind such inconsistency by examining the extent to which the benefits and barriers suggested in the cyber security information sharing literature are reflected in the attitudes of cyber security professionals. In doing so, we aim to identify the main challenges to the successful implementation of information sharing efforts. We should note that in this chapter, we use the term *cyber threat intelligence*, or *threat intelligence* for short, to refer to both threat-centric data as well as alerts and advisories — two categories of information sharing identified in Chapter 4.

In Section 5.1 we introduce a categorisation of the benefits and barriers found in the literature. In Section 5.2 we explain how these categories were used in designing a questionnaire that captured the views of cyber security professionals towards these

issues. We present the survey's results in Section 5.3 and discuss their implications in Section 5.4. We offer a chapter summary in Section 5.5. The work described in this chapter was previously presented as [150].

## 5.1 Benefits and barriers

A significant amount of the literature has examined the potential benefits of information sharing in cyber security. 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 the subject often highlight "standardisation", "competition" and "trust" among the reasons why organisations struggle to effectively share information pertinent to security incidents and threats [25, 119, 151]. These challenges, as the authors of [13] 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.

While a number of studies have recognised some of the overall opportunities and challenges facing threat intelligence sharing in general, most of what is written in this area is theoretical. Although useful for establishing hypotheses, such contributions do not provide solid grounds for policy making or business decisions. Research has yet to systematically investigate stakeholders' attitudes and perspectives and a limited number of studies have attempted to support the theoretical assumptions with some empirical evidence.

One of the early attempts was [25], in which nine experts from six European countries were interviewed by the European Union Agency for Network and Information Security (ENISA) to identify the most relevant incentives and barriers to effective information sharing, with a view to addressing critical infrastructure protection.

More recently, in 2016, an advisory committee was tasked by the US Federal Communications Commission (FCC) with reviewing the state of cyber security

information sharing within the communications industry [119]. 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 [152], 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 other organisations. However, of the 25 respondents, only 9 firms were active participants in at least one formal information sharing effort. Other notable studies include those conducted by researchers based at the University of Innsbruck who utilised a combination of focus groups and exploratory surveys to examine threat intelligence sharing in practice [10–12, 104].

In this section we present the results of an attempt to explore and structure the benefits and barriers associated with threat intelligence sharing that are found in the literature. The results were grouped into four categories: operational, organisational, economic and policy (Table 5.1). This categorisation was derived and adapted from the frameworks used in [119] and [152]. We should note that given the relatively new use of the term threat intelligence sharing to refer to cyber security information sharing activities, only a small number of studies in the literature have adopted it. Therefore, we considered studies focusing on threat intelligence sharing as well as cyber security information sharing in general. Our classification is not meant to be exhaustive and definitive; rather it is developed to facilitate capturing practitioners' views and the subsequent discussion. It is also important to note that although these benefits and barriers are presented separately, in reality it is often the case that one may affect or overlap with another in dynamic ways.

| Benefits | Barriers |
|---|---|
| **Operational** | |
| • Reduces duplicate information [153]<br>• Supports breach detection [1, 18, 153]<br>• Reduces damage caused by breaches [153]<br>• Supports incident response [154]<br>• Supports deterrence efforts [29] | • Lack of standardisation [151, 155]<br>• Vaguely defined terminology [151, 155]<br>• Capacity limits [119]<br>• Assessing accuracy [119]<br>• Determining quality [1, 51, 104]<br>• Ensuring timeliness [119]<br>• Achieving interoperability [18, 51, 156]<br>• Safeguarding sensitive data [18, 51, 156, 157]<br>• Handling irrelevant data [18, 155] |
| **Organisational** | |
| • Expands professional networks [6, 119]<br>• Supports better defensive agility [18]<br>• Improves overall security posture [18, 151]<br>• Improves situational awareness [18]<br>• Mitigates skills gap [1] | • Proliferation of redundant efforts [119]<br>• Competition [25, 27]<br>• Reputation damage [25, 153]<br>• Establishing trust [25, 119, 156]<br>• Lack of trained staff [119, 158] |
| **Economic** | |
| • Cost savings [25, 28]<br>• Allows governments subsidies [25, 30]<br>• Lowers cyber insurance premiums [25]<br>• Reduces uncertainty associated with cyber security investment decisions [159] | • Free riding [1, 153, 160]<br>• Resource draining [25, 37]<br>• Loss of clients confidence [25, 30, 153] |
| **Policy** | |
| • Strengthens relationship with government entities [161, 162]<br>• Offers liability protection [26, 155] | • Violation of privacy laws [153]<br>• Government over-classification [119, 156, 163]<br>• Upholding public values [161]<br>• Inconsistent legal frameworks [13, 119] |

**Table 5.1:** Summary of the benefits and barriers associated with threat intelligence sharing as reported in the literature.

### 5.1.1 Benefits

Arguments in favour of threat intelligence sharing, in both grey and academic literature, present an extensive list of reasons as to why it could be beneficial to the public and private sectors. In this subsection we explore some of the frequently mentioned benefits (Table 5.1).

**Operational benefits**

**Operational benefit 1: Reduces duplicate information processing**

A common belief in the literature is that by not sharing threat intelligence between them, organisations would end up redoing the same work. If the information is shared however, everyone should in theory benefit from reducing the associated cost and reallocating resources [153].

**Operational benefit 2: Supports breach detection and remediation**

Threat actors often use the same attack vectors and exploit similar vulnerabilities in their campaigns. Threat intelligence sharing could therefore speed up breach discovery and remedy by providing organisations with access to information that might otherwise be unavailable [1, 18, 153].

**Operational benefit 3: Supports incident response**

Sharing threat intelligence increases the efficiency of identifying and responding to security incidents. Security teams can utilise the information received from other organisations in deploying tools and understating the attacker's tactics and techniques [154].

**Operational benefit 4: Supports deterrence efforts**

The claim was first made in the model presented in [29], which builds upon an analysis of ordinary burglaries to make an argument for threat intelligence sharing as a deterrence mechanism. It demonstrates that the regular exchange of threat intelligence with law enforcement and other organisations makes an organisation less attractive for threat actors.

**Organisational benefits**

**Organisational benefit 1: Expands professional networks:**

Successful threat intelligence sharing reinforces existing professionals' relationships and builds new ones between individuals as well as organisations facing similar security challenges [6, 119].

**Organisational benefit 2: Improves overall security posture**

By sharing threat intelligence, organisations gain a deeper understanding into the threat landscape, which, in turn, could inform their cyber security and risk management practices [18, 151].

**Organisational benefit 3: Supports defensive agility and resilience**

Organisations that share information are usually better prepared to detect and respond to threats. As threat actors continue to evolve, the awareness created by intelligence sharing helps reduce the likelihood of successful attacks and increase the cost for the attackers as they are forced to develop new tactics [18].

**Organisational benefit 4: Improves situational awareness**

Sharing threat intelligence creates an environment that allows organisations to leverage the collective knowledge and capabilities of other organisations within the sharing community. Even the smallest observation about a threat actor contributes to increasing the awareness and security of an entire community [18].

**Organisational benefit 5: Mitigates skills gap**

The sharing of threat intelligence and the consequent pooling of knowledge, expertise and capabilities, provide resource-limited organisations with an opportunity to mitigate the impact of skill shortages [1].

**Economic benefits**

**Economic benefit 1: Cost savings**

Efficient allocation of resources and cost saving are often cited as the organisation's main incentives for threat intelligence sharing [25]. Economic models such as the one presented in [28] demonstrate that sharing intelligence reduces the overall cost of achieving the desired level of information security.

**Economic benefit 2: Allows subsidies provision by governments**

Government intervention in the form of subsidies provision or tax benefits is often referred to as an incentive for intelligence sharing with the amount of the financial subsidy closely associated with the level of sharing [25, 30].

**Economic benefit 3: Lowers cyber insurance premiums:**

Some studies have suggested that organisations who exchange threat intelligence could be offered lower insurance premiums assuming that insurers would regard the participation as evidence of good security practice [25].

**Economic benefit 4: Reduces uncertainty associated with cyber security investment decisions**

Based on an analysis of a hypothetical case, the researchers in [159] argue that information sharing can reduce the uncertainty surrounding cyber security investments, which could offset the tendency by organisations to underinvest or defer spending on security activities until a data breach is discovered.

**Policy benefits**

**Policy benefit 1: Strengthens relationship with government entities**

Public-private partnerships are regarded as a key tool in countering cyber attacks. The majority of theses partnerships provide threat intelligence as a core service [161, 162].

**Policy benefit 2: Offers liability protection**

Through government legislation, participants in threat intelligence sharing could be guaranteed reduced liability in exchange for transparent information sharing establishing a regulatory environment that facilitates voluntary sharing of information [26, 155].

### 5.1.2 Barriers

We cannot thoroughly understand the state of threat intelligence sharing or appreciate its benefits without examining the corresponding challenges to the successful implementations of these efforts. In this subsection we list some of the frequently mentioned barriers cited in the literature along the same four categories used earlier (Table 5.1).

**Operational barriers**

**Operational barrier 1: Lack of standardisation**

The absence of standardised and structured representation of the complex information being shared makes it harder to trace and align this information between organisations [54, 151]. This will also increase the cost of consumption of the shared intelligence [155].

**Operational barrier 2: Vaguely defined terminology**

As discussed in Chapters 2 and 4, information sharing in cyber security is a relatively young area. Therefore, consensus on the meaning of many of its evolving concepts and practices is lacking [164]. This according to the literature could result in confusion among practitioners and additional work to extend or harmonise ontologies [151, 155].

**Operational barrier 3: Capacity limits**

The increasing scale and volume of information pose an operational challenge on organisations. With thousands indicators of compromise received daily, security tools and personnel can be overwhelmed [119].

**Operational barrier 4: Determining overall quality**

As threat intelligence sharing continues to spread and gain momentum, quality assurance and validation are necessary in order to obtain the promised benefits of threat intelligence. As suggested by the research published in [104], shared threat intelligence suffers from a number of data quality challenges. The high data volume and velocity, as well as the critical impacts data quality have on the organisation's decision-making processes, raise several unsolved quality issues that threaten to undermine the foundation of any information sharing efforts [1, 51, 104].

**Operational barrier 5: Assessing accuracy**

The accuracy of shared threat intelligence is among a number of quality challenges facing information sharing efforts [1]. Accurate information is often regarded as one of the pillars of effective and actionable intelligence [165].

**Operational barrier 6: Ensuring timeliness**

Real time protection requires timely collection, analysis and dissemination of cyber threat intelligence. Delayed production and sharing of information can render it unusable or ineffective for the receiver. Conversely, hasty production and sharing of information may result in a high percentage of false positives and other undesired outcomes [119].

**Operational barrier 7: Poor interoperability and automation**

Achieving interoperability relies on the development and adoption of standardised data formats and transport protocols. They are also important to facilitate and automate the exchange of threat intelligence between organisations in a frictionless and timely manner [18]. Achieving the desired level of interoperability and automation comes with a cost as it involves considerable time and resources. The value of investing in intelligence sharing can be significantly reduced if other organisations request the use of different formats or protocols [18, 51, 156].

**Operational barrier 8: Safeguarding sensitive data**

Sharing incident or vulnerability information such as logs, configurations or scan results can expose the organisation's protective capabilities and give threat actors visibility into its security architecture. Similarly, any exposure of sensitive information including personal information can lead to legal action and reputation loss among other negative consequences. Both producers and consumers of threat information are therefore expected to design and implement handling policies and technical controls to mitigate the risk of disclosing or compromising the shared information [18, 51, 156, 157].

**Operational barrier 9: Handling irrelevant data**

The high-frequency and high-volume sharing of intelligence could undermine its relevance to the organisation [18]. As the model in [155] demonstrates, only a small fraction of the shared information can answer a particular question. The processing of irrelevant information creates unnecessary workload and lessens the effectiveness of the process [18].

**Organisational barriers**

**Organisational barrier 1: Proliferation of redundant efforts**

The wide array of threat intelligence sharing activities including numerous tools and services dedicated to the sharing of threat-centric data, threaten to dilute resources and overwhelm security teams [119].

**Organisational barrier 2: Competition**

Many intelligence sharing activities and services involve rival firms competing in the same market. The information security economics literature suggests that organisations take competition into consideration when deciding on whether to participate in these efforts or not as withholding information from a competitor could give an organisation a competitive edge [25, 27].

**Organisational barrier 3: The risk of reputation damage**

The reputation of targeted organisations is an asset to protect [160]. If sensitive information about a vulnerability or an incident was to be leaked or widely publicised, an organisation risks hurting or losing its reputation with clients and investors [25, 153].

**Organisational barrier 4: Establishing trust among participants**

Sharing intelligence about incidents and vulnerabilities requires a high level of trust among participants given the sensitive nature of the information [156, 165]. Trust relationships are therefore imperative to the effectiveness of threat intelligence sharing. However they require time and effort to establish and strengthen. The literature often notes that as the number of participants grows, trust decreases, which could limit the effectiveness and quality of the shared intelligence [25, 119].

**Organisational barrier 5: Lack of trained staff**

Organisations continue to voice their concerns over the shortages of skilled personnel in a wide range of security roles including those dedicated to the collection, analysis and dissemination of threat intelligence, which in turn is posing a serious challenge to the successful implementation of threat intelligence capabilities [119, 158].

**Economic barriers**

**Economic barrier 1: Free riding**

An organisation which attempts to benefit from its membership in an intelligence sharing effort without contributing in return is a free-riding member [1]. The information security economics literature has highlighted free-riding as a key barrier to successful cyber security information sharing. If an organisation consistently contributes while not receiving information in return, it may decide to end its membership [153, 160].

**Economic barrier 2: Resource draining**

Collecting and disseminating threat intelligence requires the allocation of human and financial resources [25]. The cost of training analysts, purchasing platforms or subscribing to information feeds, could prevent organisations with limited resources from participating [37].

**Economic barrier 3: Loss of clients confidence and satisfaction**

Research has shown that reports of a data breach or network compromise pose a risk to the organisation's reputation and clients confidence, which in turn can result in reduced revenues [166]. By sharing intelligence pertinent to security incidents, especially one that involves the compromise of customers' private information, an organisation may become a target of regulatory action [25, 30, 153].

**Policy barriers**

**Policy barrier 1: Violation of privacy or antitrust laws**

Several studies have pointed to the reluctance of organisations to share threat intelligence due to some unresolved legal questions surrounding privacy and antitrust issues [153].

**Policy barrier 2: Government over-classification**

Threat intelligence received from government sources is often accompanied by certain security levels [156, 167]. Restrictions placed on this intelligence limits the success of sharing efforts since the recipients cannot gain a full insight into the scope or nature of the threat they are seeking to defend against [119, 163].

**Policy barrier 3: Upholding public values**

With the absence of the government's initial gate-keeping role, the literature recognises the difficulty in making sure private organisations are serving public law values such as accountability, transparency, due process and fairness [161].

**Policy barrier 4: Inconsistent legal frameworks across jurisdictions**
Complex and varying legal regimes prevent or slow down the sharing of threat intelligence. Restrictions on cross-border data flows and different criminal jurisdictions could render the timely sharing of intelligence unfeasible if not impossible [13, 119].

### 5.1.3 Summary

In this section we presented and summarised some of the frequently cited benefits and barriers to successful threat intelligence sharing in the literature. It is important to note that although these benefits and barriers are presented separately, in reality it is often the case that one may affect or intersect with another in dynamic ways. For example, the degree to which an organisation trusts other participants could affect the perceived reliability or quality of the received intelligence. Similarly, the skills shortage could contribute to the increased cost of processing threat intelligence. However, with limited empirical research into this area, most of these claims remain unsupported and shrouded with uncertainty. As a result, organisations might be reluctant to participate in threat intelligence sharing as no empirical evidence is yet to demonstrate its value. It is also more difficult to assess and mitigate the impact of the barriers and risks associated with the process. In the following sections we present and discuss the findings of our empirical study that aimed to validate the claims made in the literature and summarised in Table 5.1.

## 5.2 Questionnaire development

Based on the classification in Section 5.1, we developed a questionnaire to measure practitioners' attitudes towards the benefits and barriers associated with threat intelligence. In the self-reported questionnaire, we asked participants to indicate the extent to which they agreed or disagreed with 28 statements divided equally between the benefits and barriers. The statements were derived from the items of Table 5.1 and covered a range of benefits and barriers mentioned in the literature. Their agreement was measured on a seven-point Likert-type scale with 1 = 'strongly disagree', 7 = 'strongly agree', and 4 = 'neither agree nor disagree.' We also

collected information on each respondent's experience and their organisation's profile. The questionnaire was reviewed by two experts for content validity and readability [168]. The questionnaire was pilot-tested to establish reliability and identify weaknesses by collecting data from five practitioners not included in the study sample. Relevant suggestions were incorporated into the final version of the questionnaire (Appendix B).

The survey was conducted from March to April 2019. In total, 67 cyber security professionals from 41 organisations answered the survey.

## 5.3 Results

Survey respondents represented organisations in a range of sectors with the top three being: information or communication (32.8%); finance or insurance (17.9%); and retail or wholesale (13.4%). A third of these organisations (32.8%) had over 1,000 employees; a further third (29.9%) had between 250 and 1000 employees. Over half of the respondents (56.7%) were security analysts with the rest split across other security-related positions. The majority (65.7%) had between two and five years of working experience in threat intelligence sharing. Over two thirds (67.2%) were directly involved in threat intelligence sharing at the time of the survey. Table 5.2 provides a full description of the respondents' characteristics and their organisations' profiles.

The questionnaire's full set of items along with the responses' median and interquartile range are listed in Tables 5.3 and 5.4. Figure 5.1 shows a box plot of the responses to each of the statements.

Respondents overall agreed that threat intelligence sharing (TIS) has a positive effect on their organisations' security posture as noted in the literature (S07). However, they also highlighted several barriers that can undermine the success of these efforts.

Table 5.3 reveals that the participants expressed strongest agreement with the ideas that threat intelligence sharing supports breach detection and recovery processes (S03), develops and maintains strong professional relationships (S05), and

| Variable | | Frequency (n=67) | Percentage |
|---|---|---|---|
| **Sector** | Information or communication | 22 | 32.8% |
| | Finance or insurance | 12 | 17.9% |
| | Retail or wholesale | 9 | 13.4% |
| | Utilities | 7 | 10.4% |
| | Health or social care | 7 | 10.4% |
| | Public Sector or Defence | 6 | 9.0% |
| | Education | 4 | 6.0% |
| **Number of employees** | >1,000 | 22 | 32.8% |
| | 250–1000 | 20 | 29.9% |
| | 50–249 | 19 | 28.4% |
| | <50 | 6 | 9.0% |
| **Current position** | Security analyst | 38 | 56.7% |
| | Security administrator | 10 | 14.9% |
| | CISO | 9 | 13.4% |
| | Security engineer | 7 | 10.4% |
| | Security researcher | 3 | 4.5% |
| **Experience in cyber security** | <2 years | 16 | 23.9% |
| | 2–5 years | 33 | 49.3% |
| | >5 years | 18 | 26.8% |
| **Experience in threat intelligence** | <2 years | 12 | 17.9% |
| | 2–5 years | 44 | 65.7% |
| | >5 years | 11 | 16.4% |
| **Current involvement in threat intelligence** | Yes | 45 | 67.2% |
| | No | 22 | 32.8% |

**Table 5.2:** Description of the survey respondents and their organisations.

strengthens the organisation's overall security resilience (S08). Weaker agreement was expressed about the ability of threat intelligence sharing to mitigate the impact of skill shortages (S09). Respondents disagreed that threat actors are deterred by threat intelligence sharing among organisations (S01) or that sharing would help lower cyber insurance premiums (S11) and offer liability protection (S14).

On the other hand, Table 5.4 shows an agreement among the respondents that threat intelligence sharing results in redundant data (S20) and incurs expensive infrastructure costs that may divert resources from other activities (S24). They also agreed that determining the overall quality of the shared intelligence is difficult (S17) and that vaguely defined terminology continues to undermine sharing efforts (S16). 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

| Survey statement - Benefits | How strongly do you agree with each of the following?* (n=67) |
|---|---|
| **S01** Threat actors are deterred by TIS among organisations | 3 (1–4) |
| **S02** TIS supports incident response efforts | 4 (3–6) |
| **S03** TIS contributes to breach detection and recovery | 5 (5–6) |
| **S04** TIS reduces duplicate information handling | 3 (2–5) |
| **S05** TIS strengthens and expands professional networks | 5 (4–6) |
| **S06** TIS validates and complements other sources of intelligence | 5 (3–6) |
| **S07** TIS improves overall security posture and situational awareness | 5 (3–6) |
| **S08** TIS enhances defensive agility and resilience | 5 (4–6) |
| **S09** TIS helps mitigate the impact of cyber security skills shortages | 4 (2–6) |
| **S10** TIS reduces overall cyber security costs | 3 (2–6) |
| **S11** TIS lowers cyber insurance premiums | 2 (2–4) |
| **S12** TIS reduces uncertainty surrounding security investment decisions | 4 (2–5) |
| **S13** TIS strengthens relationship with government agencies | 5 (4–6) |
| **S14** TIS offers organisations liability protection | 3 (1–4) |

**Table 5.3:** Survey responses presented as median with interquartile range (IQR).
* measured on a seven-point Likert-type scale: 1 (strongly disagree) to 7 (strongly agree).

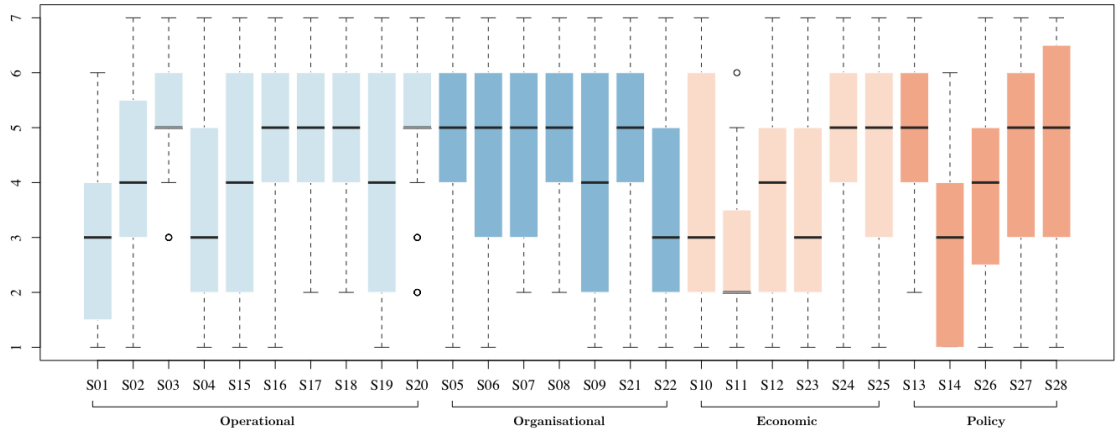



**Figure 5.1:** Box plot of responses to the survey statements on Likert-type scales [1-7].

intelligence (S26 and S27). Respondents disagreed, however, that it is difficult to trust the other participants (S22) or that standardisation is still a major issue hindering threat intelligence (S15).

A correlation matrix was created in R to visualise the correlation of all variables to one another along with their statistical significance (Figure 5.2). Correlations between all 28 questionnaire statements have been calculated using the Spearman's rank correlation coefficient. The use of the non-parametric Spearman's correlation

| Survey statement - Barriers | How strongly do you agree with each of the following?* (n=67) |
|---|---|
| **S15** Standardisation issues continue to hinder TIS | 4 (2–6) |
| **S16** Inconsistent definitions and terminology undermine efficient TIS | 5 (4–6) |
| **S17** It is difficult to determine the overall quality of TIS | 5 (4–6) |
| **S18** It is difficult to ensure the timeliness of TIS | 5 (4–6) |
| **S19** Achieving interoperability and automation of TIS is difficult | 4 (2–6) |
| **S20** TIS results in redundant and irrelevant data | 5 (5–6) |
| **S21** There is a shortage of skilled analysts to handle TIS | 5 (4–6) |
| **S22** It is difficult to trust the other participants in TIS efforts | 3 (2–5) |
| **S23** Free riding will impede TIS efforts | 3 (2–5) |
| **S24** Setting up TIS infrastructure is expensive and resource draining | 5 (4–6) |
| **S25** TIS erodes clients' confidence | 5 (3–6) |
| **S26** Government over-classification undermine effective TIS | 4 (2–5) |
| **S27** Privacy and antitrust legal concerns impede TIS | 5 (3–6) |
| **S28** Inconsistent legal frameworks undermines cross-border TIS | 5 (3–7) |

**Table 5.4:** Survey responses presented as median with interquartile range (IQR).
* measured on a seven-point Likert-type scale: 1 (strongly disagree) to 7 (strongly agree).

was preferred given that the majority of the data did not follow a normal distribution of frequency. The Spearman approach does not assume any assumptions about the distribution of the data and is the appropriate correlation analysis when the variables are measured on an ordinal scale [169]. Significant correlations are labelled with an asterisk in Figure 5.2. We discuss correlations between statements of interest in Section 5.4.

To examine whether there is a statistically significant association between the respondents' job positions or sectors and their attitude towards the benefits and barriers of threat intelligence sharing, we used Kruskal-Wallis test by rank. The test is a rank-based non-parametric method used to examine whether there are statistically significant differences between two or more groups of an independent variable on a continuous or ordinal dependent variable [130]. The technique tested the null hypothesis that all five job positions were identical with respect to average agreement. The test provided a strong evidence of a statistical significant difference between the respondents' job position categories with level of agreement towards statements S11 ($p = .025$), S17 ($p = .015$), S27 ($p = .026$) and S28 ($p = .003$). In

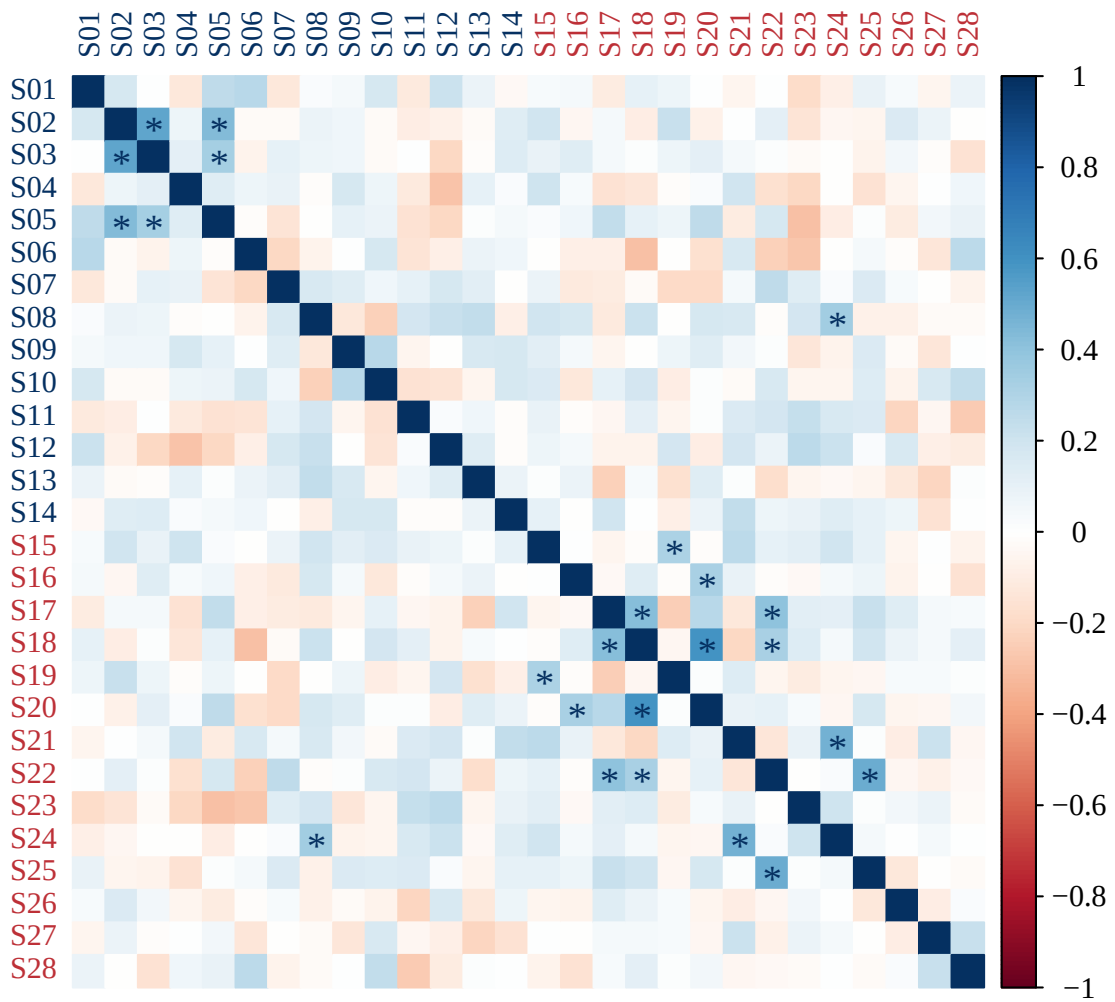



**Figure 5.2:** Spearman's rank correlation matrix of questionnaire statements. The colours of the scale bar denote the strength and nature of the correlation with blue for positive and red for negative relationships. Significant correlations are labelled with an asterisk.

order to determine which categories of job positions are different from others with regard to each of the statements, we conducted Dunn's post-hoc tests on each pair of groups [170]. The test provided a strong evidence that, when compared to other groups, CISOs had significantly different attitudes towards statements S11, S27 and S28 — they disagreed with the notion that threat intelligence sharing would help lower insurance premiums, and agreed that regulatory restrictions and inconsistent legal frameworks undermine the effectiveness of intelligence sharing. As for the organisations' sectors, the tests showed that they did not differ statistically.

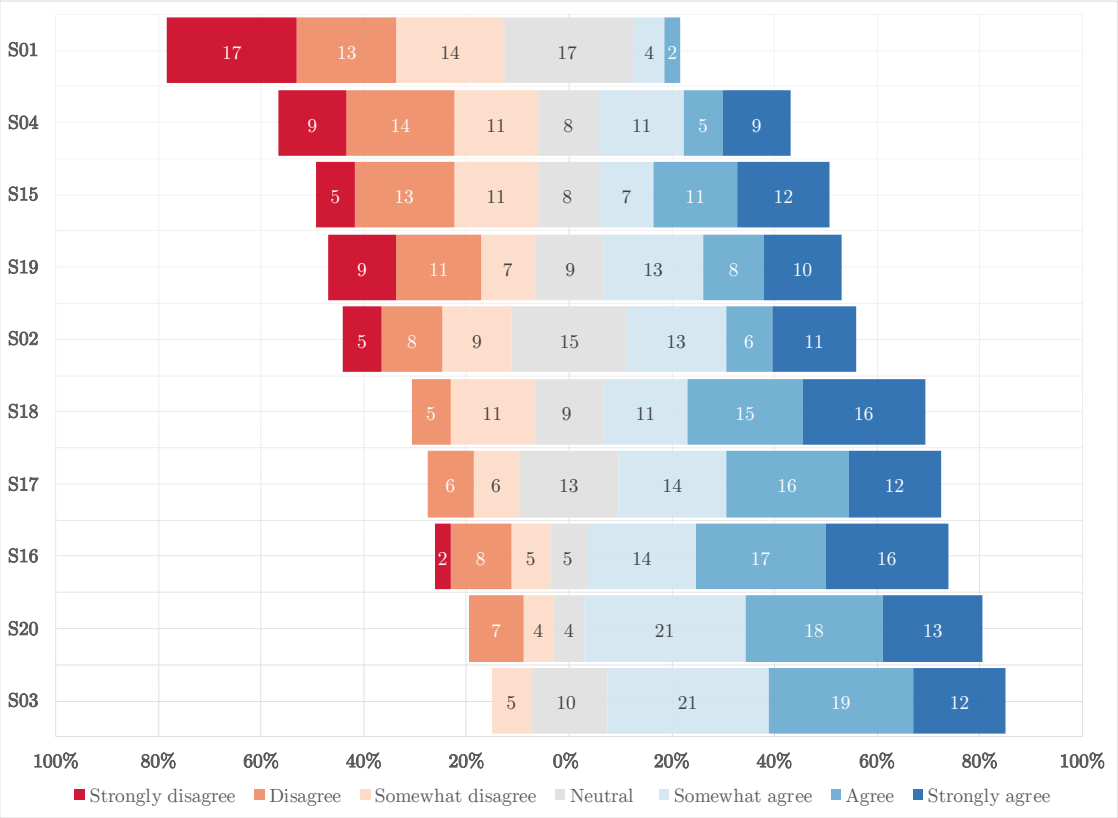



**Figure 5.3:** Attitudes towards the operational benefits and barriers.
**S01** Threat actors are deterred by TIS among organisations.
**S04** TIS reduces duplicate information handling.
**S15** Standardisation issues continue to hinder TIS.
**S19** Achieving interoperability and automation of TIS is difficult.
**S02** TIS supports incident response efforts.
**S18** It is difficult to ensure the timeliness of TIS.
**S17** It is difficult to determine the overall quality of TIS.
**S16** Inconsistent definitions and terminology undermine efficient TIS.
**S20** TIS results in redundant and irrelevant data.
**S03** TIS contributes to breach detection and recovery.

## 5.4 Discussion

Empirical research such as this has the potential to: help determine why cyber threat intelligence 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. With this in mind, we now relate our results (Tables 5.3 and 5.4) to the categories first introduced in Section 5.1.

### 5.4.1 Operational level

The results of threat intelligence sharing depend to a great extent on the effectiveness of implementation from an operational viewpoint [119]. Threat intelligence sharing is still facing fundamental technical and operational challenges (Figure 5.3). Around three quarters of survey respondents (70%) agreed that inconsistent definitions and terminology are undermining efficient threat intelligence sharing. This result is in line with our earlier findings in Chapter 4. The majority of respondents expressed concerns over a number of data quality issues: three quarters (77%) agreed that threat intelligence often result in redundant or irrelevant data processing; two thirds (63%) agreed that ensuring timely dissemination of intelligence is difficult; and the same share (63%) said that determining the overall quality of the intelligence is difficult. According to the Spearman's rank correlation, there is evidence for a strong, positive monotonic correlation between the respondents' levels of agreement with the timeliness and relevance statements ($r_s$ =.596) [171].

On the other hand, standardisation efforts appear to be yielding some practical results. Despite being repeatedly cited as an impediment to effective sharing in the literature, less than half of respondents (45%) agreed that lack of standardisation continues to hinder threat intelligence sharing, and roughly the same number (46%) considered the interoperability and automation of threat intelligence sharing difficult to achieve. This could be partially due to the emergence of several frameworks and ontologies such as OpenIOC, VERIS, MITRE ATT&CK, STIX, and TAXII [23]. As a result, vendors and their clients have begun to incorporate some of these specifications into their solutions, which has helped streamline some of the processes and achieve higher interoperability. These results seem to confirm the argument presented in [2] that the challenge in threat intelligence sharing has shifted from how to develop interoperable systems for data sharing to how to operationalise and generate value from the intelligence received.

Despite the identified shortcomings, the positive role of threat intelligence on an operational level is clear. Respondents acknowledged some of the operational benefits of threat intelligence: over three-quarters (78%) agreed that intelligence

supports breach detection and recovery processes whereas only a third (33%) did not support the idea that threat intelligence supports incident response processes. The Spearman's rank correlation indicates a strong, positive correlation between the two statements ($r_s$ =.528) [171].

As for the role threat intelligence plays in deterring threat actors, the majority (66%) disagreed as they saw little evidence to support this notion, which was presented in [29].

### 5.4.2 Organisational level

Overall, respondents agreed with the positive role of threat intelligence sharing in improving the organisation's security posture and situational awareness (52%), as well as its agility and resilience (72%) (Figure 5.4). This sentiment seems to stem from the constructive role of intelligence sharing on the operational level as expressed by the respondents.

Surprisingly, respondents did not seem concerned about longstanding information sharing challenges such as building trust among participants. Around 57% did not agree that trusting other participants in intelligence sharing efforts is difficult to achieve. This finding is a notable departure from the literature, much of which lists trust and free riding as the most significant barriers to successful information sharing.

However, skills shortages of cyber security professionals with the required skills to process threat intelligence was among the most agreed-on statements with over 64% of the respondents agreeing. These skills are both analytical and technical, including awareness of attack patterns, knowledge of indicators of compromise and familiarity with threat actors and campaigns, as well as critical thinking, intelligence analysis and incident response [158, 172]. As for the potential for threat intelligence to help in mitigating the impact of the current skills gap, respondents were almost equally divided between agreement (45%) and disagreement (46%) with the statement (median=4 , IQR=4). Our finding therefore serves as further evidence of the wider cyber security skills shortages or mismatch as highlighted in [173], and calls for further research into the soft and technical skills required for processing threat

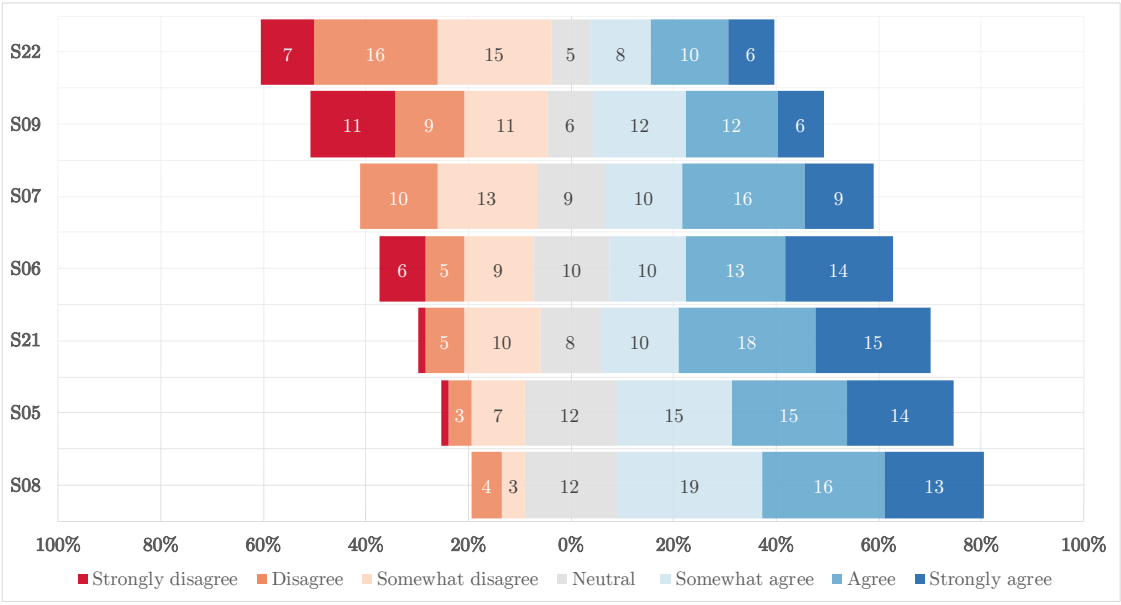



**Figure 5.4:** Attitudes towards the organisational benefits and barriers.
**S22** It is difficult to trust the other participants in TIS efforts.
**S09** TIS helps in combating cyber security skills shortages.
**S07** TIS improves overall security posture and situational awareness.
**S06** TIS validates and complements other sources of intelligence.
**S21** There is a shortage of skilled analysts to handle TIS.
**S05** TIS strengthens and expands professional networks.
**S08** TIS enhances defensive agility and resilience.

intelligence. Finally, two thirds of respondents (66%) were in agreement that threat intelligence sharing contributes to building and maintaining professional networks.

### 5.4.3 Economic level

Financial incentives to information sharing have long been the focus of extensive research in various contexts [28]. 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 (61%) agreed that establishing threat intelligence sharing infrastructure is expensive and could drain resources, a third (36%) supported the idea that, in the long run, intelligence sharing could help bring down the overall security cost (Figure 5.5). Faster response to vulnerabilities and incidents, anticipating network failures and the more efficient allocation of resources are factors that could contribute to cost savings [25]. The associated expenses, as explained in [119], are most acute for small and mid-sized organisations

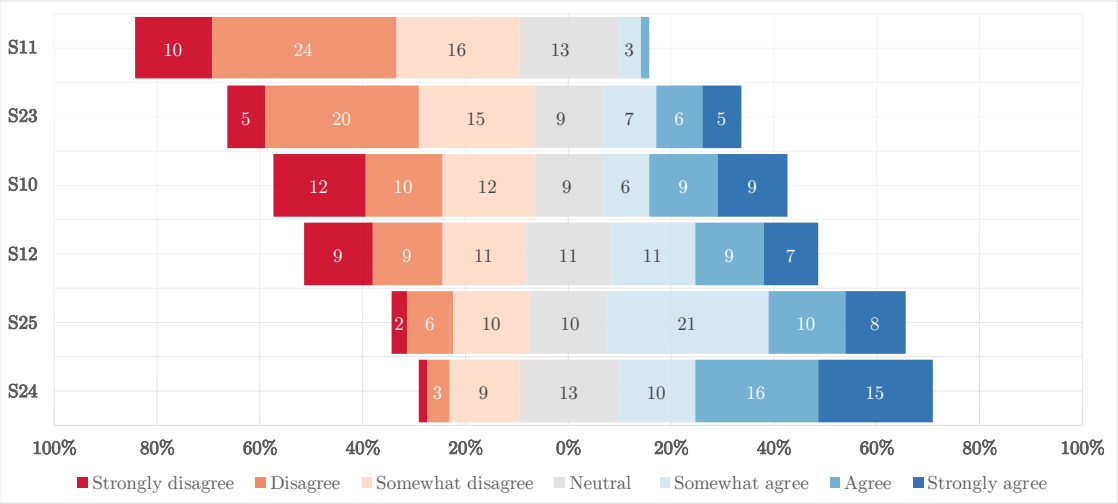



**Figure 5.5:** Attitudes towards the economic benefits and barriers.
**S11** TIS lowers cyber insurance premiums.
**S23** Free riding will impede TIS efforts.
**S10** TIS reduces overall cyber security costs.
**S12** TIS reduces uncertainty surrounding security investment decision.
**S25** TIS erodes clients' confidence.
**S24** Setting up TIS infrastructure is expensive and resource draining.

with limited financial and human resources. A strong positive correlation was found between respondents' agreement with the high price of setting up sharing infrastructure and the skills shortage ($r_s$ =.547) [171].

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 [25, 28, 29]. However, an overwhelming majority (75%) of our respondents did not agree with this notion. This finding is consistent with that of [25] which argues that, in practice, merely sharing cyber threat information is not sufficient to convince insurance companies to lower premiums especially given the paucity of actuarial data on the impact of intelligence sharing on an organisation's security.

As for the risk of other organisations benefiting from the intelligence being shared without sharing the cost or contributing their own threat data (i.e. free riders), the majority of respondents (60%) did not consider it as a significant impediment. Similar to the trust issue discussed earlier, this finding challenges the longstanding

assumption that the free riding problem continues to undermine the effectiveness of intelligence sharing and organisations' willingness to share.

### 5.4.4 Policy level

Cooperation with the government continues to enjoy considerable support among the survey respondents with the majority (58%) agreeing that threat intelligence sharing helps build and strengthen relationships with government agencies (Figure 5.6). This suggests that the positive impact of threat intelligence sharing on establishing strong working relationships is not limited to practitioners operating within the same industry as discussed earlier, but also extends to external partners — especially relevant government entities. However, around half of those who were surveyed (49%) seem to support the idea that government over-classification of data could undermine the usefulness of those efforts. While government entities are expected to consider both public benefit and the potential risks of disclosing sensitive security information, the intelligence community has a tendency to over-classify and be overly cautious when it comes to cyber incidents [174]. This concern among others has led the UK's National Cyber Security Centre (NCSC) for example to implement various forms of public-private initiatives that promote closer collaboration and mitigate the tendency to over-classify. Further research could assess the effectiveness of those different initiatives and determine the ideal method to mitigate the respondents' concerns.

The risk of violating privacy and antitrust laws is a major concern for a considerable share of the respondents (55%) who agreed that this risk could impede threat intelligence sharing. Further legal risks explored in [152] 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.

A quarter of our respondents strongly agreed that inconsistent regulatory frameworks present challenges to cross-border threat intelligence sharing. This finding mirrors the claim of [119] that the complex and vague legal frameworks are thwarting real time sharing of cyber threat information internationally.

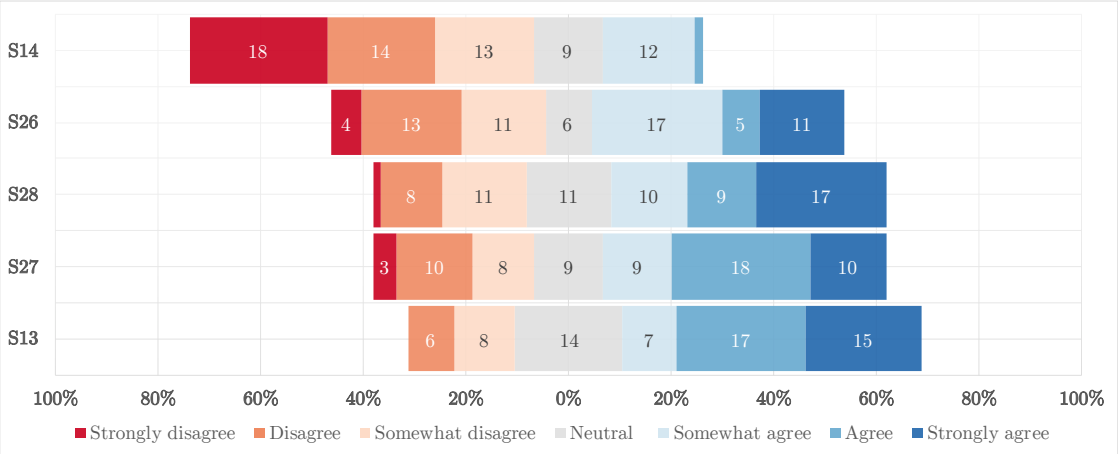



**Figure 5.6:** Attitudes towards the policy benefits and barriers.
**S14** TIS offers organisations liability protection.
**S26** Government over-classification undermine effective TIS.
**S28** Inconsistent legal frameworks undermines cross-border TIS.
**S27** Privacy and antitrust legal concerns impede TIS.
**S13** TIS strengthens relationship with government agencies.

## 5.5 Summary

Threat-centric information sharing, as discussed in Chapter 4, has become the most prevalent type of cyber security information sharing despite increasing doubts among practitioners about its usefulness. The available literature on the benefits of this type of sharing, as well as the barriers contributing to its perceived ineffectiveness, is fragmented and consists largely of theoretical studies.

In this chapter, we aimed to explore some of the potential reasons behind this inconsistency and to gain some empirical insights. As a starting point, we attempted to explore the extent to which the benefits and barriers suggested by the cyber security information sharing literature are reflected in the attitudes of cyber security professionals. In doing so, we aimed to answer our second research question.

We achieved this by: (i) compiling a list of frequently-cited benefits and barriers in the literature and categorising them into four groups: operational, organisational, economic and policy (Section 5.1); (ii) developing a questionnaire that captured practitioners' level of agreement with the findings of the literature reviews (Section 5.2); and (iii) analysing the data and discussing the results of the questionnaire (Sections 5.3 and 5.4).

Our findings confirm the positive role of threat intelligence sharing in improving the organisation's security posture. However they diverge from the literature in how the issue of trust is perceived. Participants' attitudes towards issues such as inconsistent terminology, quality assessment and limited resources come in line with our findings in Chapter 4. In Chapter 6 we investigate the quality challenge in detail and present a set of quality dimensions that incorporates several of this chapter's findings.

We should acknowledge that we have surveyed only a limited number of experts from a handful of sectors in one country. The barriers to threat intelligence sharing might be very specific to country and industry and, therefore, the attitudes towards sharing activities 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 build on in the following chapters.

# 6

# Threat Intelligence Quality Dimensions

The preceding chapter provided an empirical insight into some of the reported benefits and barriers of threat-centric information sharing. Issues surrounding the quality of the information being shared, including its timeliness, relevance and consistency represented the most agreed-on challenges among the participants. Concerns regarding the quality and effectiveness of various forms of information sharing were also captured in Chapter 4.

Data and information quality literature has emphasised the importance of clearly defining the consumer's quality requirements as a foundational step to achieving the desired level of data quality [68, 71]. For example, the Total Data Quality Management (TDQM) methodology proposed by Wang in [175] specifies the definition phase as the first phase in managing the quality of information products.

To this end, the work described in this chapter set out to further investigate the quality challenge in threat-centric information by developing an understanding of the practitioners' quality needs. In doing so, we follow an empirical approach similar to the one used in [71] which elicits and analyses consumers' input to define the attributes they use to determine whether the data is suitable for use in their tasks. We implemented this approach in three steps: (i) addressing the terminological confusion surrounding threat data, information and intelligence; (ii) identifying, defining and verifying a set of quality dimensions consumers use in

assessing the quality of threat intelligence; and (iii) exploring what metrics, if any, organisations use to measure these dimensions.

The methodological approach consisted of a systematic literature review (SLR) followed by a modified two-round Delphi study in an attempt to bridge the gap between theory and practice. Details of the data collection and analysis instruments are provided in Chapter 3. Through the SLR, we identified widely-cited definitions of threat data, information and intelligence, and derived a set of threat intelligence quality dimensions. The preliminary definitions and dimensions served as an input to the Delphi study in which a panel of 30 experts refined and verified our results. The Delphi study was conducted in collaboration with Clemens Sauerwein at the University of Innsbruck, who helped in recruiting and interviewing 11 of the 30 experts. The work described in this chapter was previously presented as [176].

The remainder of this chapter is structured as follows. Section 6.1 draws on the participants' understanding of the terms threat data, information and intelligence, to propose our revised definitions of these terms. Sections 6.2 and 6.3 present and discuss the quality dimensions and their definitions. Section 6.4 outlines the key findings of the chapter and their implications. Finally, Section 6.5 summarises the chapter and links to Chapter 7.

## 6.1 Threat data, information and intelligence

The first goal of our study was to explore the experts' understanding of each of the terms *cyber threat data*, *cyber threat information* and *cyber threat intelligence*. To achieve this, we presented the participants with a widely-cited definition from the literature for each of the terms, and asked them to indicate their level of agreement with each one of them on a five-point Likert-type scale. This was followed by an open-ended discussion regarding the meaning and use of each of the above terms. The three definitions were chosen based on the work of [177] where the researchers synthesise the literature and discuss the strengths and shortcomings of multiple definitions. They are also in line with the commonly accepted depiction of traditional intelligence activity as a progressive refinement of data and information [178].

| Variable | | Frequency (n=30) |
|---|---|---|
| **Sector** | Information or communication | 13 |
| | Finance or insurance | 9 |
| | Manufacturing | 5 |
| | Food or hospitality | 2 |
| | Utilities | 1 |
| **Location** | United Kingdom | 16 |
| | Austria | 4 |
| | Switzerland | 4 |
| | Netherlands | 2 |
| | Germany | 2 |
| | Ireland | 1 |
| | Italy | 1 |
| **Number of employees** | >1,000 | 23 |
| | 250–999 | 2 |
| | 50–249 | 1 |
| | <50 | 4 |
| **Current position** | Security manager | 12 |
| | Security analyst | 5 |
| | Chief information security officer (CISO) | 5 |
| | Security engineer | 4 |
| | Chief information officer (CIO) | 2 |
| | Chief client officer (COO) | 1 |
| | SOC team leader | 1 |
| **Experience in cyber security** | <2 years | 0 |
| | 2–5 years | 8 |
| | >5 years | 22 |
| **Experience in threat intelligence** | <2 years | 2 |
| | 2–5 years | 18 |
| | >5 years | 10 |
| **Organisation's threat intelligence activity** | Threat intelligence producer | 0 |
| | Threat intelligence consumer | 8 |
| | Threat intelligence producer & consumer | 22 |
| **Does your organisation operate a SOC?** | Yes | 20 |
| | No | 10 |
| **Does your organisation use a TIMP?** | Yes | 22 |
| | No | 8 |

**Table 6.1:** Overview of the Delphi panel experts and their organisations.

| Definition | Strongly disagree | Disagree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| **Threat data** | 1 (3.30%) | 1 (3.30%) | 6 (20.0%) | 19 (63.3%) | 3 (10.0%) |
| **Threat information** | 1 (3.30%) | 5 (16.7%) | 4 (13.3%) | 18 (60.0%) | 2 (6.70%) |
| **Threat intelligence** | 0 (0.00%) | 3 (10.0%) | 5 (16.7%) | 15 (50.0%) | 7 (23.3%) |

**Table 6.2:** Experts' agreement with each of the literature-derived definitions.

As shown in Table 6.2, the majority of the experts either agreed or strongly agreed with the literature-based definitions of threat data, information and intelligence (73.3%, 66.7% and 73.3% respectively). However, during the discussion a number of experts highlighted aspects of the definitions that they did not agree with and suggested some changes.

### 6.1.1 Cyber threat data

The authors of [177] define threat data as: "lower-level raw logs that have been produced by sensors such as payloads hash values, network artifacts, internet protocol (IP) addresses and uniform resource locators (URLs)."

Participants generally agreed with this definition albeit with three caveats. First, although threat data is primarily raw, lower-level data points such as indicators of compromise (IoCs), it does not always have to be produced by sensors. Secondly, in order for the data to be considered as threat data it has to be related to some sort of malicious activity. Finally, according to the participants, threat data is predominantly machine-readable. Examples of threat data include SHA1 and MD5 hashes that correspond to specific suspicious files or samples of malware; IP addresses of suspected command and control servers; and network artifacts that identify malicious activity from that of legitimate users [179].

Based on the participants' comments and suggestions, we propose the following revised definition of threat data:

> **Revised definition:** Cyber threat data is a machine-readable set of raw recorded facts that can help in identifying or mitigating malicious activity in a system or network. It includes indicators of compromise such as malware signatures, IP and URL addresses, file and domain names, or registry keys.

### 6.1.2 Cyber threat information

In the same report [177], threat information is defined as: "data that have undergone additional processing to provide enhanced high-level insight that may help decision makers in reaching a well informed decision."

Overall, participants agreed with the notion that threat information is data enriched with context. However, they stated that it does not necessarily provide high-level insights or allow for well-informed decisions. They also challenged the idea that threat information is strictly the result of extra processing of the data stating that threat data grouped together or with some context is usually enough to make the information relevant to the organisation. For example, a series of raw logs (threat data) collated together indicates a spike in suspicious activity (threat information) [180].

A couple of experts stated that it is difficult to differentiate between data and information and therefore did not see value in distinguishing between the two in practice. Instead they offered a simpler model that only differentiates between intelligence inputs and outputs. In light of the discussion above, we adopt the following definition for threat information:

> **Revised definition:** Cyber threat information is information pertaining to a threat to, or vulnerability of, a system or network. It is the result of contextualising and interpreting threat data.

### 6.1.3 Cyber threat intelligence

A widely-cited definition of threat intelligence in the literature is the one presented in [181], where the term is defined as: "evidence-based knowledge, including context, mechanisms, indicators, implications, and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject's response to that menace or hazard."

The majority of the experts agreed with this definition noting that it adequately captures the meaning and function of intelligence in practice. Nevertheless, they stressed the importance of manual analysis and therefore the analyst's role in

vetting, analysing, interpreting and applying hypotheses to the information. A number of participants referred to the forward-looking nature of threat intelligence, emphasising that threat intelligence involves not only impact assessments and recommendations but also requires deduction and prediction. One participant raised doubt about using the word "knowledge" in the definition saying that intelligence is more about reaching a hypothesis that one could agree or disagree with and that it does not have to be 100% knowledge or truth per se. For example, indication of a suspicious activity, when contextualised with information on prior incidents involving similar activity, could allow for the development and deployment of a mitigation strategy to stop the incident [180].

In reflecting on the experts' feedback we build on the definition introduced in [181] to formulate the following definition:

> **Revised definition:** Cyber threat intelligence is evidence-based forward-looking assessment including context, implications, and action-oriented advice about a threat to, or vulnerability of, a system or network. This intelligence is produced through the application of individual or collective cognitive methods, and can be used to inform decisions regarding the subject's response to that threat or vulnerability.

## 6.2 Identifying threat intelligence quality dimensions

In this section we first report the results of the systematic literature review in the form of a set of literature-based quality dimensions in Section 6.2.1. These results were fed into the modified two-round Delphi study where the experts panel reviewed and refined the quality dimensions. We discuss their adjustments in Sections 6.2.2 and 6.2.3. The panel reached consensus in the second round resulting in a final set of quality dimensions presented in Section 6.2.3.

### 6.2.1 Results of the systematic literature review

The systematic literature review, described in Chapter 3, delivered a final set of 22 papers discussing quality dimensions in the context of cyber security. We

extracted 32 quality dimensions in total as listed in Table 6.3. The most common dimensions were: timeliness (n=14), completeness (n=13), accuracy (n=12), consistency (n=8), relevance (n=8) and reliability (n=7). Both uniqueness and understandability were mentioned in four different studies, whereas the remaining quality dimensions were mentioned once or twice. Table 6.3 also records whether the dimensions were mentioned in the context of data, information, intelligence, or any combination of the three.

In order to simplify the final set of dimensions, we decided to only include the dimensions that were mentioned in all three contexts: data, information and intelligence. Figure 6.1 shows the intersections of the three groups of dimensions, with the grey box showing those mentioned in all of them. With the exception of uniqueness and interoperability, the other five dimensions were among the ones mentioned most frequently. The preliminary set of dimensions along with their definitions as stated in the ISO/IEC 25012 standard [182] are as follows:

- **Accuracy:** The degree to which threat intelligence has attributes that correctly represent the true value of the intended attribute of a concept or event in a specific context of use.
- **Completeness:** The degree to which threat intelligence contains all expected information and ensures that no information is missing.
- **Interoperability:** The degree to which threat intelligence is in a form that allows it to be imported, replaced and moved into an organisation's information management systems while preserving its existing quality.
- **Relevance:** The degree to which threat intelligence is useful for the purposes for which they were collected.
- **Reliability:** The degree to which threat intelligence comes from legitimate sources and has not been tampered with.
- **Timeliness:** The degree to which threat intelligence has attributes that are of the right age in a specific context of use.

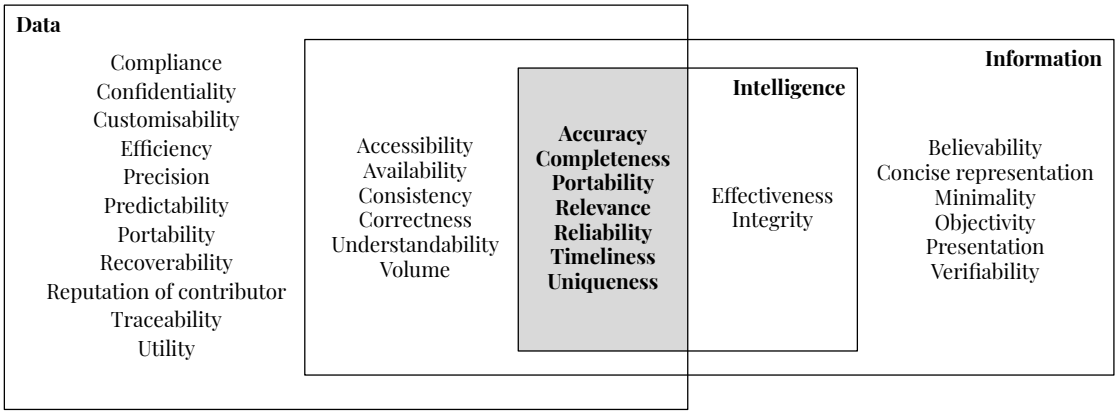



**Figure 6.1:** Literature-based quality dimensions grouped by scope.

- **Uniqueness:** The degree to which threat intelligence is similar to previously seen threat intelligence from other sources.

### 6.2.2 Results of Delphi round 1

The aforementioned set of literature-based quality dimensions served as a starting point for the first round of the modified Delphi study. The results of this round are manifested in the following three modifications.

**Dropping the uniqueness and completeness dimensions:**

After careful examination of the proposed literature-based quality dimensions, almost all of the experts saw little importance in including the uniqueness and completeness dimensions.

Threat intelligence received from one source only often calls for further investigation to ensure that it is not the product of faulty analysis. Despite being promoted as a selling point by some vendors, for consumers, unique data or intelligence plays little, if any, role in determining the overall quality of the product. Truly unique and reliable intelligence according to the panel can only be delivered if a provider has access to unique sources or capabilities, which is applicable mostly to government intelligence agencies. The experts also stressed that unique intelligence should not be confused with bespoke intelligence products resulting from a specific request by the client.

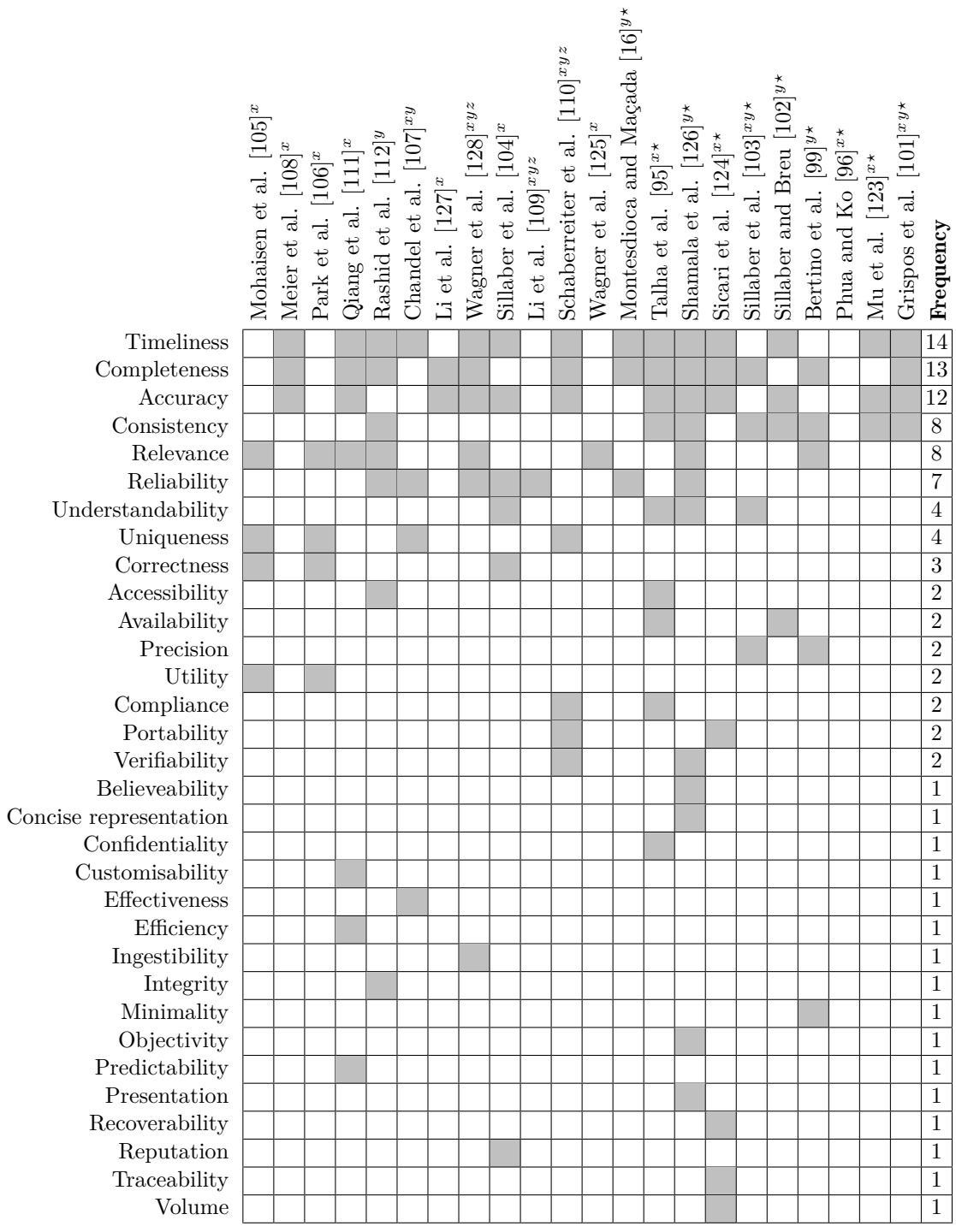



**Table 6.3:** Quality dimensions extracted from the literature.
*Scope: [x] data; [y] information; [z] intelligence; [⋆] non-TI.*

Similarly, completeness in an absolute sense is difficult to determine, attain or measure. Alternatively, intelligence completeness according to the experts is mainly about the totality of the assessment, in terms of how methodical and rigorous the analysis is. This is usually accomplished by following a certain model like the kill chain [183] to provide a reasonable amount of coverage. Pursuing intelligence completeness according to the panel could undermine its timeliness and actionability. By the time more information is collected and a comprehensive analysis is conducted, the intelligence might become less actionable. As for lower-level data like IoCs, all else being equal, a feed with more data is potentially better than others, but no one expects one source to provide a 100% complete picture. Organisations with more resources minimise these limitations by purchasing or subscribing to more than one service.

Given their minimal impact on determining intelligence quality and following the experts' recommendations, we decided to exclude *uniqueness* and *completeness*.

**Adding the actionability and provenance dimensions**

When asked about what quality dimensions are missing from the initial set of dimensions, the majority of experts referred to two main dimensions: actionability and provenance. Further discussion with the panelists highlighted the importance of these two dimensions in evaluating the quality of threat intelligence and therefore were added to the modified set of dimensions in the second round. We discuss the actionability and provenance dimensions in Section 6.2.3.

**Distinguishing between threat data and threat intelligence**

In commenting on the validity of the literature-based quality dimensions, the experts highlighted the need to differentiate between threat data and threat intelligence when it comes to determining quality dimensions. This is in line with our discussion in Section 6.1 where we distinguished between the two terms and the different purposes they serve. Threat information, on the other hand, was excluded as the experts did not see a practical need to evaluate its quality separately. Therefore, the next round sought to capture the participants' agreement with the modified

| Dimension | Threat Data | | | | | Threat Intelligence | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | $N_d$ | $N_a$ | $LA$ | $M$ | $IQR$ | $N_d$ | $N_a$ | $LA$ | $M$ | $IQR$ |
| **Accuracy** | 0 | 26 | 86.7% | 5 | 1 | 0 | 30 | 100% | 5 | 1 |
| **Actionability** | 1 | 23 | 76.7% | 4 | 1 | 1 | 29 | 96.7% | 5 | 1 |
| **Interoperability** | 3 | 25 | 83.3% | 4 | 1 | 6 | 20 | 66.7% | 4 | 2 |
| **Provenance** | 0 | 23 | 76.7% | 4 | 1 | 0 | 21 | 70.0% | 4 | 1 |
| **Relevance** | 2 | 24 | 80.0% | 5 | 1 | 0 | 29 | 96.7% | 5 | 1 |
| **Reliability** | 0 | 26 | 86.7% | 4 | 1 | 0 | 25 | 83.3% | 4 | 1 |
| **Timeliness** | 0 | 29 | 96.7% | 5 | 1 | 1 | 26 | 86.7% | 5 | 1 |

**Table 6.4:** Experts' agreement with the dimensions in Delphi round 2.

$N_d$ : Number of experts who disagreed or strongly disagreed.
$N_a$ : Number of experts who agreed or strongly agreed.
$LA$ : Level of agreement ($LA = N_a/n * 100, n = 30$).
$M$ : Median, $IQR$ : Interquartile range.

set of quality dimensions in the context of threat data and threat intelligence independently of each other.

### 6.2.3 Results of Delphi round 2

All 30 experts from the previous round participated in the second round. The experts were asked whether they agreed with the modified set of dimensions from the first round. They were also asked to rank the dimensions in order of importance for each of threat data and threat intelligence. The responses to each of the dimensions were tested against our predefined definition of consensus: LA $\geq$ 66.7%. As shown in Table 6.4, a third Delphi round was not required because consensus was achieved on all dimensions. Consequently, the final set of threat data and intelligence quality dimensions are: *accuracy*, *actionability*, *interoperability*, *provenance*, *relevance*, *reliability* and *timeliness*. In the following section we discuss each of these dimensions and their significance to threat intelligence practice.

## 6.3 Threat intelligence quality dimensions

In this section we discuss our threat intelligence quality dimensions. The final set of quality dimensions and their definitions are presented in Table 6.5.

| Dimension | Definition |
|---|---|
| **Accuracy** | The degree to which threat data or intelligence is correct, objective or without false-positives. |
| **Actionability** | The degree to which threat data or intelligence allows a decision to be made or action to be taken without the need for further analyses. |
| **Interoperability** | The degree to which the formats of threat data or intelligence is compatible with consumers' internal systems allowing it to be accessed and integrated seamlessly. |
| **Provenance** | The degree to which a threat intelligence consumer is able to track the evolution of a piece of threat data or intelligence including its origins and the process through which it was produced. |
| **Relevance** | The degree to which threat data or intelligence meets the consumer's specific requirements and is useful for the purpose for which it was produced. |
| **Reliability** | The degree to which the source of threat data or intelligence is trustworthy, authentic and competent. |
| **Timeliness** | The degree to which threat data or intelligence is available without delay in a specific context of use. |

**Table 6.5:** Final set of quality dimensions for threat data and intelligence.

### 6.3.1 Accuracy

In an absolute sense, accuracy is the degree to which information has attributes that correctly represent the true value of the intended attribute of a concept or event in a specific context of use. In the context of threat intelligence, inaccurate and false-positive attributes might result in undesired effects and wasted resources [46]. However, the experts stated that, in practice, determining the absolute truth is difficult if not impossible. Accordingly, alternative interpretations of accuracy were elicited.

For threat intelligence producers, accuracy means ensuring the objectivity of the analysis and that the way the product was communicated enables the message to arrive and be understood the way that it was meant to. Although a low number of false-positives in IoCs is one indication of the accuracy of threat data, the panel agreed that consumers do not expect a vendor to provide 100% accurate information in an absolute sense. However, in order to determine the relative accuracy of the intelligence product, they ask how the data and intelligence were collected, whether the analyst has come up with the right hypothesis, and what evidence supports the

conclusions. Analysts have some latitude based on their own experiences but it is crucial to ensure that their analysis is logical and they do not leap to conclusions.

The need to distinguish between assessments and facts is crucial, prompting practitioners to adopt traditional intelligence language that conveys confidence levels such as the NATO or Admiralty coding [84] that is used by some vendors to indicate what they perceive as accurate and reliable information.

### 6.3.2 Actionability

According to the panel of experts, actionability is the extent to which threat data or intelligence allows a decision to be made or action to be taken without the need for further analysis.

The production of actionable intelligence in practice usually requires an analyst to provide some recommendations or courses of action. And there is always one course of action, which is to do nothing. So, in reality, what one is asking intelligence analysts to do is to make calls, right or wrong. This allows the consumer to use or deploy the intelligence directly before it loses its value. In practice, what makes intelligence actionable can take a range of forms. For high-level analytical reports it could mean that the consumer is going to use that intelligence the next time they make an important decision about security architecture. For lower-level threat data, it could mean using these indicators to block a threat, prioritise patching or develop mechanisms to detect specific adversary tactics, techniques and procedures (TTP).

However, in reality according to some experts, if the intelligence producer understands their client's requirements, then everything they produce should be actionable in one way or another.

### 6.3.3 Interoperability

The increasing volumes of threat data and diversity of sources have elevated the importance of interoperability in threat intelligence. For organisations using more than one service or vendor, it is vital to be able to access and process all of the data in one place and in a timely manner. Similarly, vendors realise that offering

products that are aligned to particular standards is important to allow consumption across their clients' different platforms.

The importance of interoperability varies depending on the exact nature of the intelligence. For machine-readable threat data like IoCs, it is crucial to be able to ingest them smoothly and with minimal analyst effort. However, for higher-level analytical reports, recommendations or assessments, the importance of being able to ingest that into a platform is less critical.

The panel also reinforced the importance of standardised formats in ensuring data is exchanged in consistent and machine-readable manner. The Structured Threat Information Expression (STIX) language [54] continues to attract traction and support.

Threat intelligence platforms and APIs continue to evolve and provide new capabilities including auto-scrubbing, and auto-validation of indicators in order to prevent false positives or neutral indicators from being added automatically. However, despite the increasing reliance on platforms and APIs, a number of experts on the panel stated that some of the APIs of commercial vendors are not well documented (or not as well as the consumers would like them to be), which in some cases makes it very complex to pull files and generate reports.

### 6.3.4 Provenance

Provenance according to the experts panel is the extent to which a threat intelligence consumer is able to track the evolution of a piece of threat data or intelligence including its origins and the process through which it was produced. Good provenance allows the consumer to trace the intelligence in the same way the author did based on the evidence provided. This includes the source of information at granular level and detailed documentation of the processes through which it was produced. A provenance chain would also show what analytical models were used and what hypotheses were tested in formulating the conclusion or assessment.

Provenance is also seen as an important factor in establishing trust and determining usefulness of a vendor. It allows the consumer to identify vendors that merely serve as information aggregators giving rise to issues such as circular reporting.

However, establishing provenance is a complex problem, and the community is yet to establish a standardised provenance process, which could be the reason why this dimension is often overlooked.

### 6.3.5 Relevance

Overall, the experts agreed that relevance is an important dimension in evaluating the quality of threat intelligence. Increased noisy and irrelevant data result in wasted resources and time. However determining what makes a particular piece of data relevant or not cuts across the organisation's industry, sector, geography, technologies in use, its assets etc.

In addition to the organisation's business activity, the amount of allocated resources for its threat intelligence programme plays a vital role in determining how tailored the received intelligence needs to be. In big organisations including those operating in multiple sectors, a dedicated internal team collects as much data, information and intelligence as possible before translating it into intelligence that is relevant for the organisation's different business entities.

Our experts agreed that irrelevant intelligence can often be attributed to a failure to understand the consumer's requirements. However, intelligence producers sometimes face cases where their clients have an immature threat intelligence programme and the clients themselves are unable to identify their intelligence needs, which further complicates things for the producers.

### 6.3.6 Reliability

According to the Delphi experts, determining the reliability of a source is critical in deciding whether to rely on the information received or not. The inferential value of the assessments or conclusions is constantly considered with the reliability of their source in mind. The experts stated that the reliability of a source encompasses other factors including its trustworthiness, authenticity, competence and objectivity.

Assessing a source's reliability in the context of threat intelligence is currently a multi-layered process and involves subjective elements. The process, according

to the experts, should take into account the following three considerations: the historical reliability of the source for similar incidents or topics including its own confidence in the intelligence; the intelligence's consistency with known facts or confirmed post-mortem findings; the intelligence's consistency with information gleaned from other sources. Therefore, perceived reliability in a source is established over time, throughout the progression of the analyst's experience and encounter with the source, as well as the organisation's overall experience. A source with a demonstrated track record of accurate and credible reporting is perceived as more reliable than an unknown source. For example, experts reported high levels of perceived reliability of official sources such national intelligence agencies and national CERTs, as opposed to a new or untested vendor.

It should be noted that despite the importance of source reliability, the experts pointed to the challenge of ensuring source anonymity in some cases as highlighted by Murdoch and Leaver [157]. They also noted that the reliability of a source is not constant and therefore continuous re-evaluation might be required. This is in line with the findings of Schaberreiter and colleagues who present a method that allows an organisation to re-evaluate trust in one or more sources every time it receives new threat intelligence [110].

### 6.3.7 Timeliness

Timely decision-making is imperative for an organisation's security [51]. Accordingly, the experts overwhelmingly agreed that timeliness is one of the most important dimensions in evaluating the quality of threat data and intelligence. Organisations are constantly looking for new ways to reduce the delay in receiving important information and in acting upon it.

Although the value of intelligence does not drop to zero if it is late, it could diminish significantly. The shelf life of the intelligence also depends on the exact type of the information being shared. For example, threat data like malware signatures have a relatively short shelf life as they are constantly evolving. An organisation responsible for providing those to a consumer needs to ensure they are delivered in

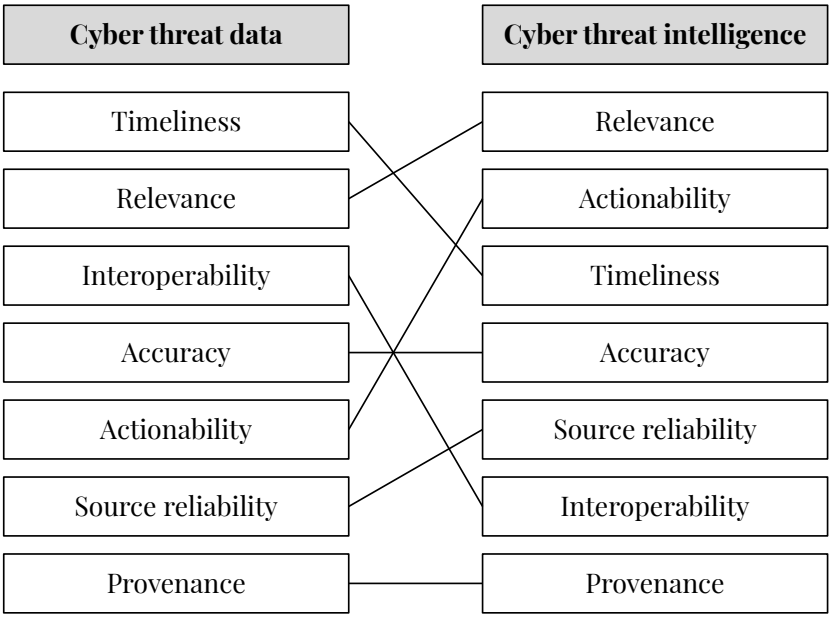



**Figure 6.2:** Experts' ranking of dimensions in order of importance from high to low.

a timely manner. However, a more strategic intelligence assessment that looks at 3–6 months of the threat landscape is still timely but could be delivered on a later deadline. The experts also pointed to the inconsistency in the metadata surrounding the intelligence received by some sources. While some sources state both when the data was observed and when it was reported, others might fail to do so.

## 6.4 Discussion

The analysis of the results of the systematic literature review and the modified Delphi study provided insights on certain dimensions and metrics used to assess the quality of cyber threat data, information and intelligence. In this section we discuss the key findings and critically reflect on the limitations of our research.

#### Quality priorities vary

For each of threat data and threat intelligence, we asked the panel's experts to rank the final set of quality dimensions in order of importance. The results as depicted in Figure 6.2 show that the importance of a dimension varies depending on whether it is being used to assess the quality of threat data or threat intelligence.

Threat data as discussed in Section 6.1 is used to monitor and detect threats and vulnerabilities. The shelf life of threat data is short and its value diminishes considerably with time. Data feeds are predominantly machine-readable and are expected to be easily processed and integrated into different platforms. Therefore, it is not surprising that the panel considered timeliness, relevance and interoperability as the three most important quality dimensions.

On the other hand, the three most important threat intelligence quality dimensions are relevance, actionability and timeliness. As examined in Section 6.1, many experts stressed that threat intelligence by definition is forward-looking and involves applying hypotheses and making recommendations. Actionable, relevant and timely intelligence therefore is understandably key to avoid waste of resources and overburdening security operation centres.

**Measuring intelligence quality remains a challenging issue**

As part of the cost-benefit analysis of their threat intelligence programmes, organisations would ultimately like to know how intelligence products are being used and which paid source is providing good quality intelligence products. Discussions with the experts revealed that, despite growing interest in the idea, stakeholders are yet to identify and develop suitable metrics to measure any of the quality dimensions and most of them do not have a specific process to filter and evaluate threat intelligence based on these dimensions.

Simple quantitative metrics like the number of intelligence reports received or the number of IoCs fed into a platform are considered unhelpful in measuring intelligence quality. They are however useful for the consumers to know how much data they will receive and how much resources it requires to process. Traditional intelligence evaluation frameworks like the Admiralty System are used in some cases to indicate the reliability of the source and the credibility of the intelligence. Whether the intelligence has been validated by other sources, or the threat has materialised, inaccurate elements as well as the source reputation and history are factors that can negatively or positively affect the evaluation of the source.

The experts also stated that consumer feedback is essential for vendors in order to identity areas for further improvement. Feedback collection ranges from informal conversations to more rigorous and regular processes such as questionnaires attached to intelligence reports. Through these processes, vendors solicit feedback on the quality of their products, systems and services. Metrics integrated into the platforms (e.g. number of times a report was read or downloaded) would also be considered. However, despite being an essential part of the traditional intelligence cycle [178], the feedback loop according to some experts does not exist in commercial intelligence since only few vendors actually implement it, and, where it does, it is slow and inefficient.

From a consumer point of view, measuring the quality of a threat intelligence product is intertwined with determining its effectiveness. This is typically achieved by examining the decisions that were made based on the received intelligence and the impact of these decisions on preventing exploitation or reducing vulnerability. The percentage of intelligence that has led to control changes (e.g. deciding to monitor or stop monitoring a specific part of the network), or the number of incidents detected or foiled because of intelligence received from a specific source, are examples of metrics that could be employed to determine the effectiveness of a threat intelligence service. One way to achieve this is by using a tagging system that enables an organisation to track the number and nature of actions and provide it with a direct link back to the source of the intelligence. This would allow it to identify the most used sources and compare their impact to their cost.

The panelists stated that threat intelligence vendors and their clients should work together to develop and implement some of these metrics. However they warned that issues such as privacy, confidentiality and willingness can hinder the progress of the collaboration. Metrics development and tracking also requires dedicated efforts and resources adding more work to already stretched and understaffed cyber security teams.

**Determining quality is intertwined with defining requirements**

A common view amongst the panel experts is that a high-quality intelligence product is one that aligns closely with the consumer's requirements. An organisation does not necessarily need to know which of the vendors provide the most accurate intelligence, but rather which one of them is the most useful, as in which vendor's services satisfy the organisations' requirements and business area. The experts also argue that in reality if the provider knows their client's requirements well then most intelligence products should be of suitable quality. Consequently, producing an irrelevant or unactionable intelligence product is mostly attributed to a failure at the requirements level.

Requirements are ideally captured at the beginning of the interaction and reviewed regularly through ongoing conversations and requirement exercises. Establishing the requirements entails understanding what the business wants from the threat intelligence products. This requires vendors to understand the risks and the worries the client has, the industry's threat landscape, infrastructure, and what they can do to try alleviate some of these concerns or allow the client to make more informed decisions.

However, given that it is a new area, most organisations still do not fully understand how to consume threat intelligence and are therefore unable to accurately identify and convey their needs. Organisations with no existing threat intelligence programme expect the provider to fully understand the organisation's environment including its critical asset, personnel, systems, third party suppliers and so on. A number of experts also pointed out that expectations from threat intelligence vendors are high and somewhat unrealistic, and cautioned that threat intelligence services are not a panacea.

## 6.5 Summary

As the interest in threat-centric information sharing continues to grow, questions about its quality and effectiveness have surfaced. Chapter 5 highlighted data quality

issues as a concern for threat intelligence stakeholders. In this chapter, we provided a deeper empirical understanding of threat intelligence quality with the aim to clearly define the consumers' most important quality needs. A systematic review of relevant literature, followed by a modified Delphi study, resulted in identifying seven quality attributes: accuracy, actionability, interoperability, provenance, relevance, reliability and timeliness. It also examined the literature definitions of threat data, information and intelligence, and suggested areas for improvement. We found that practitioners' quality priorities vary depending on the nature of the intelligence. We have also observed that, despite increasing awareness of their potential value, organisations are yet to develop concrete metrics to measure any of the quality dimensions, and that they largely rely on consumer feedback and anecdotal evidence. We therefore hope that the quality requirements identified in this chapter could contribute to mitigating some of the concerns surrounding the quality of information sharing by serving as a foundational framework for measuring, analysing and improving threat intelligence quality.

The next chapter incorporates the findings of this chapter in investigating the success of threat intelligence management platforms as a whole.

# 7

# A Model for Measuring Threat Intelligence Success

Commercial threat intelligence management platforms (TIMPs) have been widely adopted to assist organisations in engaging with wider cyber security information sharing efforts. Measuring the effectiveness or success of these platforms is critical to understanding how such products and services should be designed, built, implemented and used. The success of a threat intelligence management platform at an organisation could also be indicative of the success of this organisation's overall threat intelligence sharing practice.

In the previous chapter we identified the main quality dimensions users consider when evaluating the quality of threat intelligence. However, in order to assess the success of the threat intelligence management system as a whole, we need to examine aspects of the system besides the quality of its content.

Although measuring traditional information system success has been discussed at length in the literature, there have been no attempts to model the success of TIMPs. In this chapter we build on the findings of earlier chapters in developing and validating a comprehensive multi-dimensional model for determining the success of a TIMP. To this end, we draw inspiration from DeLone and McLean (D&M) whose interdependent and multi-construct view of information systems success is

widely accepted and has been applied to a variety of contexts including information security practices [14–16]. We discuss relevant aspects of this model in Section 7.1.

Two main considerations guide the design and operationalisation of our model. First, to maximise its usefulness, it has to be complete and concise, as in it should consolidate previous work in the field, while remaining simple enough to preserve its explanatory value regardless of the complexity of its real-world applications [15]. Secondly, the model has to capture and integrate the characteristics of threat intelligence managements platforms while retaining as much as possible of the richness of the D&M model.

Section 7.2 provides a characterisation of the TIMP as an information system before introducing our theoretical model and the associated hypotheses in Section 7.3. Section 7.5 presents the results of the model's measurement and structural evaluation. Section 7.6 examines those results and discusses their implications for theory and practice. Section 7.7 offers a summary of this chapter.

## 7.1 D&M information systems success model

Early attempts to define what makes some information systems successful failed to capture the complex, interdependent and multi-dimensional nature of IS success [56]. With this in mind, DeLone and McLean (D&M) built upon a comprehensive review of relevant literature to propose a model for IS success that consisted of six interrelated constructs: *system quality*, *information quality*, *use*, *user satisfaction*, *individual impact* and *organisational impact* [14]. The model suggested that both system and information quality influence use and user satisfaction while the latter two influence each other and the individual impacts of the use of the system. Individual impacts, in turn, were proposed to influence organisational impacts of the information system. The model was subsequently subjected to close scrutiny including a number of modifications [57, 58]. In their follow-up work, DeLone and McLean examined these suggestions and revised their original model accordingly [15]. The updated version, as shown in Figure 7.1, extended the concept of quality to include *service quality* in addition to information and system quality as antecedents of use and

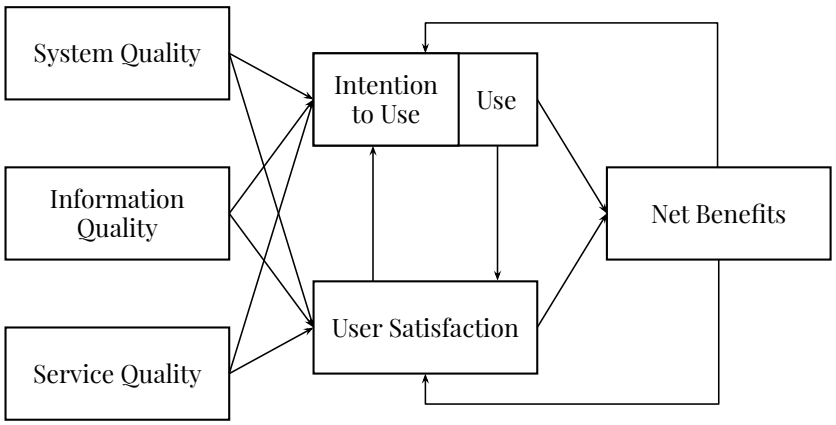



**Figure 7.1:** DeLone and McLean's updated information systems success model [15]

user satisfaction. The use construct was also further clarified in the new model by adding the *intention to use* construct to measure the user's attitude. A third and final refinement to the model stemmed from the argument that the impact of an information system can stretch beyond the individual and organisational levels [59]. The revised model therefore substituted individual impact and organisational impact with *net benefits* to account for benefits occurring on multiple levels of analysis [56].

The revised model has since been utilised as a framework to guide and organise measuring success factors in information systems [56]. In various applications of the model, researchers derive variables that describe the success of the system in accordance with the six main success constructs of the updated model, which include [15]:

1. *information quality*, capturing the desirable characteristics of the system's output or content;

2. *system quality*, referring to the desirable characteristics of the information system itself;

3. *service quality*, referring to the quality of the support users receive from the provider's support personnel;

4. *use*, denoting the extent to which the system's capabilities has been adopted by the staff or customers;

5. *user satisfaction*, referring to the users' level of satisfaction throughout their interaction with the system; and

6. *net benefits*, referring to the degree to which the system is contributing to the overall success of its users, departments, organisations, industries or societies depending on the context and level of analysis.

Practical application of the success model requires an understanding of the information system and its organisational context. This allows for the selection of appropriate dimensions that are used to measure each of the success constructs [56]. Determining success constructs and the associated metrics depend on the specific nature and objectives of the system being assessed [60]. In the following sections we discuss the model and its applicability to threat intelligence management platforms.

## 7.2 TIMP characterisation

A threat intelligence management platform (TIMP), as discussed in Chapter 2, is a cloud or on-premise information system that is used by organisations to detect and thwart cyber security threats. The software package usually includes pre-configured dashboards or templates allowing the users to customise the platform in accordance with their business needs. Commercial TIMPs allow personnel throughout an organisation to handle external feeds and intelligence, analyse threat data and conduct processes, including triaging and incident response. The platform could also be used to identify trends and provide real-time updates. It typically allows the integration of different types of data and offer all stakeholders with a mechanism to work together as a team [184].

While TIMPs vary considerably from vendor to vendor, their core features are best summarised by Dandurand and Serrano as the ability to: facilitate information sharing; assist with automation; and enable the generation, processing and validation of data [51].

As with other information systems that involve multiple stakeholders, evaluating the success of a TIMP requires answering the question of "from whose perspective is

success being evaluated?" [185]. Different actors view the success of an information system differently. For example, from a vendor's perspective, a TIMP's success might be associated with profitability, which includes traditional metrics such as units sold, market share, customer retention and satisfaction. From an end user's perspective, the platform is expected to ultimately enhance job performance and facilitate daily tasks while being easy to use and navigate. From a manager's perspective, the TIMP should meet business requirements, ensure efficient use of resources, effectively support business objectives, etc.

Various models have been developed to capture how business leverage information technology capabilities [186]. They all focus on the underlying rationale of technology adoption. However the D&M success model, examined in Section 7.1, provides a holistic understanding of adoption success given its flexible, multi-dimensional and interdependent nature. This is evident in the model's utilisation in evaluating the success of various information systems, including knowledge management systems [61, 62], e-commerce systems [63], e-government systems [64] and employee portals [65]. Therefore, we utilise the D&M model as a theoretical basis for studying and developing a TIMP success model from a user's perspective.

## 7.3 Theoretical model and hypotheses

In this section we outline and discuss a TIMP success model that builds on and adapts the refined DeLone and McLean model [15]. The model as shown in Figure 7.2 consists of seven main success constructs: *content quality*, *system quality*, *service quality*, *perceived trust*, *use*, *user satisfaction* and *net benefits*. The arrows between the constructs represent temporal and causal relationships, with each of them corresponding to a hypothesis. Section 7.3.1 examines the construct and their operationalisation, while Section 7.3.2 presents the hypothesised relationships in the model and the rationale behind them.

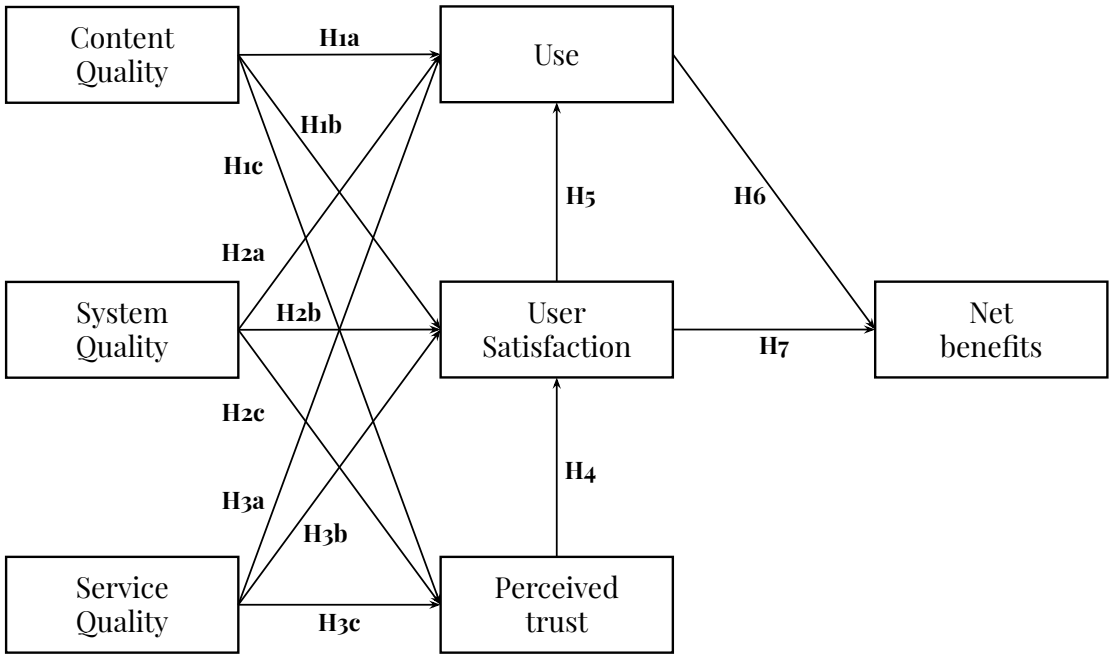



**Figure 7.2:** Our proposed research model.

### 7.3.1 Constructs

In developing our model's constructs, we examined the definition of each of the success factors in the D&M model, contrasted them with the specific features and objectives of threat intelligence management platforms, and incorporated the relevant concepts in the literature, as well as the findings of earlier chapters. This process resulted in a theoretical model that comprises of the following seven constructs (Table 7.1):

**Construct 1: Content quality**

In the D&M model, the information quality construct refers to the extent to which information retrieved from the system is in line with the user's requirements and satisfaction [189]. Previous studies have strongly stressed the role of information quality as an important determinant of a user's satisfaction and willingness to use a particular system [65, 187].

Guided by DeLone and McLean's characterisation of information quality as a content issue, our model attempts to capture the quality of threat intelligence in a construct labelled *content quality*. This is the quality of the information

| Construct | Operational definition | Dimensions |
|---|---|---|
| **Content quality (CONQ)** | The extent to which data and intelligence retrieved from the TIMP meets the requirements and expectations of the user. | Accuracy[a]<br>Actionability[a]<br>Provenance[a]<br>Relevance[a]<br>Reliability[a]<br>Timeliness[a] |
| **System quality (SYSQ)** | The extent to which the TIMP itself possesses desired characteristics and is technically sound. | Interoperability[a]<br>Functionality [65]<br>Reliability [65]<br>Usability [65] |
| **Service quality (SERQ)** | The extent to which the services provided by the TIMP vendor meet the user's needs or expectations. | Assurance [15, 56]<br>Empathy [15, 56]<br>Reliability [15, 56]<br>Responsiveness [15, 56] |
| **Perceived trust (PT)** | The extent to which the user believes that the TIMP is safe and secure. | Compliance [187]<br>Security [187]<br>Overall Trust [187] |
| **Use (USE)** | The extent to which the users actually use TIMP in performing their tasks. | Analysis [51]<br>Collection [51]<br>Dissemination [51] |
| **User satisfaction (USAT)** | The extent to which the user is satisfied with their interaction with the TIMP. | Adequacy [188]<br>Effectiveness [188]<br>Efficiency [188]<br>Overall satisfaction [188] |
| **Net benefits (NETB)** | The extent to which the use of the TIMP benefits the organisation as a whole. | Improved breach detection[b]<br>Enhanced resilience[b]<br>Improved intelligence validation[b]<br>Improved incident response[b]<br>Improved situational awareness[b] |

**Table 7.1:** The definition and operationalisation of the proposed model's constructs.
[a] adopted from Chapter 6.
[b] adopted from Chapter 5.

available through the platform, which includes indicators of compromise, incident reports, country and threat actor profiles, lessons learnt, and so forth, in structured and unstructured formats.

Despite its similarity to the information quality construct in D&M's model, the content quality construct in our model is adapted to be a broader construct and aimed at capturing the richness and diversity of the TIMP's content.

We measure the content quality construct using the findings of the previous chapter. In Chapter 6, we reported that a Delphi panel of 30 threat intelligence

practitioners agreed on seven dimensions to measure the quality of threat data and intelligence. Six of these dimensions are content-related: accuracy, actionability, provenance, relevance, reliability and timeliness.

**Construct 2: System quality**

The *system quality* construct captures the performance and functionality of the system itself by measuring the extent to which it is technically sound and has the desirable characteristics [56]. This is usually determined by the quality of the system's hardware or software components such as the number of bugs in the system, the ease of use, response time, the quality of user interface and the quality of documentation [58]. When the users are the vendor's customers as opposed to its employees, as is the case with most threat intelligence management solutions, their use of the system is usually volitional [15]. This means that unsatisfactory usability, functionality or responsiveness could discourage customer usage of that system.

Although system quality has been commonly determined using the simplified ease of use measure, some studies have found that perceived ease of use does not fully represent the system quality construct [56]. Instead, an increasing number of researchers have developed and tested their own instruments using dimensions adapted from DeLone and McLean's original model [14] or through an independent review of relevant system quality literature [56].

Based on our review of the literature concerning the function and characteristics of threat intelligence management platforms, our system quality scale includes the interoperability, functionality, reliability and usability of the system. Interoperability was included as system quality dimension based on the findings of Chapter 6, whereas functionality, reliability and usability were adapted from [65].

**Construct 3: Service quality**

*Service quality* is generally described as how well a delivered service matches customer expectations [190]. It has traditionally been considered as a subset of the model's systems quality. However, the rise of end-user computing services and the resulting change in the role of information system providers have strengthened

the argument for adding service quality as a separate construct [15]. Following an extensive debate surrounding the role it plays in determining the success of information systems, DeLone and McLean decided to add service quality to their model as a third quality antecedents as shown in Figure 7.1.

In our context, service quality is a subjective assessment of the quality of the user-vendor interaction including the extent to which specific service needs have been met [16]. Discussions with practitioners in Chapter 6 revealed that TIMP users expect a certain level of support from the vendors. Measures of information system effectiveness usually focus on the products instead of the services of the information system function [57]. Therefore, adding service quality to the assessment model could result in a more accurate and balanced measure of the system's effectiveness.

The multi-dimensional nature of the service quality construct is often captured using the SERVQUAL instrument [191]. The instrument is adapted from marketing research and is designed to measure the consumer's expectations and perceptions of a service. SERVQUAL has been found to be a valid and satisfactory measure of IS service quality [192]. Therefore, our model adopts the SERVQUAL approach by measuring the service quality construct along SERVQUAL's dimensions: reliability, responsiveness, assurance, and empathy [15, 56].

**Construct 4: Perceived trust**

In addition to the quality of the content, system and service, discussions with practitioners during the Delphi study revealed that the users' disposition towards security and compliance issues such as privacy and data protection could influence their overall satisfaction with the TIMP. The extent to which a vendor is able to ensure that TIMP installation and utilisation can be carried out securely without any intrusion or disruption is an important consideration that might affect the customers' satisfaction. This observation is in line with Molla and Licker's argument in [187] that user trust in information systems usually refers to two main issues: security and privacy. Security refers to the protection of the system's information

or processes from unauthorised access or disruption, whereas privacy refers to the users' ability to keep their data confidential during the interaction with the system.

The literature on trust in threat intelligence focuses on the establishment of trust between members of a sharing group [45, 165]. In the context of our research, the *perceived trust* construct refers to the confidence TIMP users have that the system and the party behind the system have adequate security and are compliant with relevant data protection regulations such as GDPR. Therefore, in our study we adopted a scale that consisted of three dimensions: security, compliance and overall trust in the platform.

**Construct 5: Use**

The *use* of an information system has been widely accepted as an important success measure in IS research [15]. However, the actual use, as an indicator of success, only makes sense when the use of the system is voluntary. When the system use is mandatory, researchers have suggested replacing the use construct with usefulness as a surrogate for system use [56, 187]. The use of threat intelligence platforms a discussed in previous chapters is largely voluntary and therefore we decided to adopt the construct in our model in its original form. Due to the complex nature of the use construct, empirical studies have employed a range of subjective and objective measures including frequency of use, intention to use, self-reported use and actual use [15, 56]. However, as Doll and Torkzadeh note in [193], a multi-dimensional measure of system use that is based on the nature or purpose of the system, provides a better understanding of how a system is utilised.

We follow Doll and Torkzadeh's recommendation in operationalising the use construct in our model. The dimensions were extracted from Dandurand and Serrano's summary of a threat intelligence management platform objectives as discussed in Chapter 2. According to their characterisation, a TIMP facilitates information sharing, enables automation and facilitates the generation, refinement and vetting of data through burden sharing collaboration or outsourcing [51]. This depiction is confirmed by Brown and colleagues who describe the aim of a TIMP as

to manage, synthesise and deliver threat data to different tools and stakeholders [2]. They also note how threat intelligence commercial solutions have evolved to satisfy these requirements, which manifests in the industry's shift from simple content aggregation tools towards offering threat intelligence management capabilities.

Therefore, in our study we adopt a scale for measuring use that is consistent with the literature and that consists of three dimensions: collection, analysis and dissemination.

**Construct 6: User satisfaction**

*User satisfaction* generally refers to the extent to which the users believe that a particular system they use meets their information requirements [194]. In other words, it captures the users' net feeling of pleasure or displeasure that arises from adding together all the benefits that they hope to receive from the information system [195]. Given that determining the effectiveness of information systems is in most cases difficult to measure, user satisfaction with the system has been widely accepted as a potentially measurable substitute for evaluating the utility and effectiveness of the system in decision making [194]. The majority of usability studies have also included user satisfaction measures [196]. Discussions with threat intelligence practitioners (as discussed in Chapter 6) suggested that customer feedback is commonly used by vendors as an indicator of their product's success. Practitioners acknowledged that a technically solid and well-constructed threat intelligence product is of little value if users deem its use to be unsatisfactory. Several approaches have been used to measure the user satisfaction construct. The first approach uses single-item rating to measure overall satisfaction with an information system [197]. This approach has been found to provide limited information about what the user finds dissatisfying or satisfying and has therefore been deemed unreliable. Conversely, the second approach employs multiple-item semantic differential scale and have become increasingly common [194]. In our study we adopt the latter approach by employing a scale proposed by Seddon and

Yip in [188] and consists of four dimensions: adequacy, efficiency, effectiveness, and overall satisfaction with the platform.

**Construct 7: Net benefits**

The *net benefits* construct is the final dependent variable in our model and aims to capture the overall beneficial outcomes of the use of an information system [60]. The construct was first introduced by DeLone and McLean in their revised success model [15] in order to group individual and organisational impact measures into a single impact or benefit construct. As discussed in Section 7.1, this refinement to the model stemmed from their belief that the impacts of information systems are no longer limited to the immediate user, but they include other entities such as the industry and society. The level and scope of impact measurement, therefore, depends on the system being evaluated and its objectives.

In Chapter 5, following a synthesis of the literature, we grouped the benefits of threat-centric information sharing into four categories: operational, organisational, economic and policy. This was followed by a survey that measured the extent to which these benefits and barriers are reflected in the attitudes of practising information security practitioners. In developing the net benefits measuring instrument, we rely on the findings of Chapter 5. This was achieved by selecting the questionnaire statements that focused on the benefits of threat-centric sharing and achieved more than 50% agreement by the participants after excluding neutral responses. Seven statements met the criteria. However, it is important to make sure that the person assessing the benefits is in a position and has the required knowledge to answer the questions [56]. Therefore, we decided to exclude two of the seven statements since only managers or highly experienced professionals would be able to evaluate them accurately. The process resulted in the adoption of the following set of statements:

**S02** TIS supports incident response efforts.
**S03** TIS contributes to breach detection and recovery.
**S08** TIS enhances defensive agility and resilience.
**S06** TIS validates and complements other sources of intelligence.

**S07** TIS improves overall security posture and situational awareness.

### 7.3.2 Hypotheses

Using the findings of DeLone and McLean [15] and related studies [56, 187, 188, 191], as well as the additional success dimensions, we present a theoretical model which assumes that content, system, and service quality, as well as perceived trust are associated with the TIMP's user satisfaction and usage. We also propose that the latter two, in turn, have an impact on the platform's net benefits to the organisation.

Our model's hypothesised relationships are mostly based on the D&M success model. We also expect the newly added success dimension *perceived trust* to have an impact on some of the model's other constructs.

The decision to add the trust construct came as a result of our discussion with threat intelligence practitioners as explained in Chapter 6. Based on these discussions, we hypothesise that the more trust users have in the platform, the more satisfied they are with it. The discussion also revealed that each of content, system and service quality has a role to play in establishing and maintaining users' trust in the platform. We therefore hypothesise that the higher the platform's content, system and service quality are, the more trust users have in the platform. This results in a set of hypotheses that we aim to test, as shown in Table 7.2.

Our proposed theoretical model for assessing TIMP success is shown in Figure 7.2. Each of the arrows represents one of the hypotheses to be tested. We transformed the theoretical model into a structural equation model (SEM), which we tested empirically.

## 7.4 Data collection

The data collection period was from September to November 2020. The target group consisted of users of threat intelligence management platforms in all sectors. Invitations were sent to users primarily located in the United Kingdom and Europe.

An invitation to participate in the the self-administered online questionnaire was posted on several online threat intelligence interest groups and forums. It

| | |
|---|---|
| **H1.a** | Content quality has a positive influence on the use of a TIMP. |
| **H1.b** | Content quality has a positive influence on user satisfaction with a TIMP. |
| **H1.c** | Content quality has a positive influence on user trust in a TIMP. |
| **H2.a** | System quality has a positive influence on the use of a TIMP. |
| **H2.b** | System quality has a positive influence on user satisfaction with a TIMP. |
| **H2.c** | System quality has a positive influence on the perceived trust. |
| **H3.a** | Service quality has a positive influence on the use of a TIMP. |
| **H3.b** | Service quality has a positive influence on user satisfaction with a TIMP. |
| **H3.c** | Service quality has a positive influence on the perceived trust. |
| **H4** | Perceived trust has a positive influence on user satisfaction with a TIMP. |
| **H5** | User satisfaction has a positive influence on the use of a TIMP. |
| **H6** | TIMP use has a positive influence on the net benefits of the platform. |
| **H7** | User satisfaction has a positive influence on the net benefits of the TIMP. |

**Table 7.2:** Research hypotheses.

was also sent by email to a number of connections and security-focused mailing lists. The invitation included a description of the purpose of the study and instructions to access the online questionnaire. We encouraged participants to share the questionnaire with all or a subset of their platform's users.

We emphasised in the invitations, as well as in the questionnaire's preamble, that we will use all reasonable endeavours to keep the responses confidential and that the respondent's identity could not be inferred. This was done in order to ensure best possible response rate. A total of 152 completed questionnaires were collected.

## 7.5 Analysis and results

We used the empirical data collected through the survey in testing the research hypotheses. To do so, we followed the partial least squares (PLS) approach [198] to analyse the data and assess the measurement properties of the model. The PLS, or variance-based SEM, is better suited for complex models with large number of indicators and relatively small data samples [199]. It is also useful for models where the measures are not well established [200].

The analysis is presented in three parts. Section 7.5.1 describes the survey respondents and their organisations, and provides descriptive statistics of the responses. Section 7.5.2 evaluates the latent variable constructs to ascertain whether

| Variable | | Frequency (n=152) | Percentage |
|---|---|---|---|
| **Sector** | Information or communication | 77 | 50.6% |
| | Finance or insurance | 37 | 24.3% |
| | Manufacturing | 13 | 9.2% |
| | Utilities | 9 | 6.0% |
| | Public Sector or Defence | 7 | 4.6% |
| | Retail or wholesale | 3 | 2.0% |
| | Education | 4 | 2.6% |
| | Health or social care | 1 | 0.7% |
| **Number of employees** | >1,000 | 60 | 39.5% |
| | 250–1000 | 31 | 20.4% |
| | 50–249 | 43 | 28.3% |
| | <50 | 18 | 11.8% |
| **Experience in threat intelligence** | <2 years | 53 | 34.9% |
| | 2–5 years | 55 | 36.2% |
| | >5 years | 44 | 28.9% |

**Table 7.3:** Description of the survey respondents and their organisations.

measurements used are valid and adequately describe the latent variables in this research. There are seven latent variables in this study: content quality (CONQ), system quality (SYSQ), service quality (SERQ), perceived trust (PT), use (USE), user satisfaction (USAT) and net benefits (NETB). Section 7.5.3 examines the structural model to assess the relationships between the latent variables in this study. We used the software package SmartPLS for statistical calculations [201].

### 7.5.1 Demographics and descriptive statistics

By the end of the survey period, data had been collected from 152 cyber security professionals representing organisations in a range of sectors. Half of the respondents (50.6%) were working at organisations in the information or communication sectors; a quarter (24.3%) at finance or insurance organisations; and the remaining quarter (25.1%) were spread across six other sectors as shown in Table 7.3.

The respondents' organisations also varied in size, including companies with over 1,000 employees (39.5%), between 250 and 1000 employees (20.4%), between 50 and 249 (28.3%), and fewer than 50 (11.8%).

Less than a third of the respondents (28.9%) had over five years of experience in threat intelligence, whereas the rest were split almost equally between those

with two to five years of experience (36.2%) and those with less than two years of experience (34.9%). Table 7.3 provides a full description of the respondents' profiles.

The mean and standard deviation were used to summarise the distribution of the indicators and latent variables. None of the included indicators had missing values. Skewness and kurtosis of the seven latent variables were also tested. The two measures illustrate the deviation of the observational data from the normal distribution. The skewness measures the asymmetry of the distribution, whereas the kurtosis estimates how sharp the distribution's peak is relative to its width. Skewness and kurtosis values between -1 and +1 are considered excellent. Values that fall outside this range but do not exceed -2 to +2 are considered acceptable [202]. As demonstrated in Table 7.4, we observed a fairly normal distribution for our indicators of latent factors. The skewness value for 28 out of 29 indicators fell between -1 and +1, which is considered excellent. Kurtosis values were also excellent for 25 indicators, and did not exceed the -2 to 2 range for the remaining four which is acceptable.

### 7.5.2 Measurement model evaluation

An evaluation of the constructed theoretical model was conducted to determine whether the manifest variables measured the latent variables reliably and adequately. In line with the validation guidelines proposed in [203] and [204], we carried out several tests to assess the measurement model's unidimensionality, multicollinearity, internal consistency, indicator reliability, as well as convergent and discriminant validity.

#### Unidimensionality test

A set of measurement items is described as unidimensional if it measures one and only one latent variable [205]. We conducted an exploratory factor analysis (EFA) to determine whether the indicators converge in the assigned constructs, each indicator has a high loading on one factor only, and this factor is the same for the indicators that are expected to measure it. Seven factors had an Eigenvalue

| Item | Mean | Median | Min | Max | Standard Deviation | Excess Kurtosis | Skewness |
|---|---|---|---|---|---|---|---|
| CONQ1 | 3.520 | 4 | 0 | 6 | 1.347 | -0.345 | -0.556 |
| CONQ2 | 3.454 | 4 | 0 | 6 | 1.601 | -0.463 | -0.479 |
| CONQ3 | 3.796 | 4 | 0 | 6 | 1.553 | -0.774 | -0.453 |
| CONQ4 | 3.625 | 4 | 0 | 6 | 1.337 | -0.335 | -0.455 |
| CONQ5 | 3.724 | 4 | 0 | 6 | 1.553 | -0.837 | -0.350 |
| CONQ6 | 3.355 | 4 | 0 | 6 | 1.462 | -0.574 | -0.381 |
| SYSQ1 | 4.342 | 5 | 1 | 6 | 1.107 | 0.194 | -0.770 |
| SYSQ2 | 4.191 | 5 | 0 | 6 | 1.213 | 0.954 | -1.133 |
| SYSQ3 | 4.184 | 5 | 0 | 6 | 1.305 | 0.138 | -0.831 |
| SYSQ4 | 4.171 | 4 | 0 | 6 | 1.224 | 0.170 | -0.746 |
| SERQ1 | 4.184 | 4 | 1 | 6 | 1.172 | -0.252 | -0.315 |
| SERQ2 | 4.039 | 4 | 1 | 6 | 1.175 | -0.342 | -0.348 |
| SERQ3 | 4.053 | 4 | 0 | 6 | 1.191 | -0.028 | -0.457 |
| SERQ4 | 4.211 | 4 | 1 | 6 | 1.168 | -0.314 | -0.318 |
| PT1 | 4.059 | 4 | 1 | 6 | 1.182 | -0.834 | -0.188 |
| PT2 | 3.954 | 4 | 1 | 6 | 1.388 | -0.738 | -0.260 |
| PT3 | 3.961 | 4 | 0 | 6 | 1.499 | -0.667 | -0.441 |
| USE1 | 3.947 | 4 | 1 | 6 | 1.385 | -0.891 | -0.160 |
| USE2 | 3.717 | 4 | 0 | 6 | 1.575 | -0.329 | -0.371 |
| USE3 | 3.704 | 4 | 0 | 6 | 1.534 | -0.475 | -0.275 |
| USAT1 | 3.618 | 4 | 0 | 6 | 1.701 | -1.197 | -0.319 |
| USAT2 | 3.447 | 4 | 0 | 6 | 1.780 | -1.266 | -0.125 |
| USAT3 | 3.289 | 4 | 0 | 6 | 1.809 | -1.222 | -0.123 |
| USAT4 | 3.546 | 4 | 0 | 6 | 1.802 | -1.272 | -0.287 |
| NETB1 | 3.849 | 4 | 0 | 6 | 1.463 | -0.538 | -0.459 |
| NETB2 | 3.776 | 4 | 0 | 6 | 1.518 | -0.453 | -0.515 |
| NETB3 | 3.730 | 4 | 0 | 6 | 1.509 | -0.470 | -0.530 |
| NETB4 | 3.842 | 4 | 0 | 6 | 1.496 | -0.364 | -0.560 |
| NETB5 | 4.204 | 5 | 1 | 6 | 1.475 | -0.694 | -0.519 |

**Table 7.4:** Descriptive statistics of the survey items.

greater than 1.0, which, according to Kaiser criterion, meant that we can select seven factors for the EFA [206].

Using R software package version 3.6.0 [207], we conducted an EFA with principal component analysis and varimax rotation. The results, as shown in Table 7.5, demonstrate a high level of unidimensionality. All items loaded highly (coefficient $\geq 0.6$) on one factor only [208].

| Item | Component | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| CONQ1 | **0.774** | 0.230 | 0.166 | 0.197 | 0.174 | 0.119 | 0.163 |
| CONQ2 | **0.703** | 0.207 | 0.196 | 0.208 | 0.252 | 0.199 | 0.177 |
| CONQ3 | **0.757** | 0.217 | 0.166 | 0.204 | 0.187 | 0.159 | 0.136 |
| CONQ4 | **0.764** | 0.232 | 0.147 | 0.215 | 0.251 | 0.123 | 0.187 |
| CONQ5 | **0.776** | 0.269 | 0.172 | 0.213 | 0.197 | 0.125 | 0.127 |
| CONQ6 | **0.732** | 0.269 | 0.232 | 0.229 | - | 0.177 | 0.135 |
| SYSQ1 | - | 0.148 | 0.248 | 0.101 | **0.673** | 0.152 | 0.143 |
| SYSQ2 | 0.237 | 0.226 | 0.177 | 0.159 | **0.759** | - | 0.101 |
| SYSQ3 | 0.277 | 0.281 | 0.192 | 0.170 | **0.742** | 0.182 | 0.135 |
| SYSQ4 | 0.273 | 0.169 | 0.137 | 0.219 | **0.740** | - | 0.128 |
| SERQ1 | 0.165 | 0.224 | **0.843** | 0.180 | 0.124 | 0.107 | 0.102 |
| SERQ2 | 0.148 | 0.189 | **0.707** | - | 0.240 | 0.197 | 0.141 |
| SERQ3 | 0.282 | 0.172 | **0.719** | 0.179 | 0.180 | 0.112 | 0.177 |
| SERQ4 | 0.227 | 0.168 | **0.774** | 0.230 | 0.236 | 0.167 | 0.131 |
| PT1 | 0.180 | 0.202 | 0.172 | 0.150 | 0.168 | **0.801** | 0.216 |
| PT2 | 0.160 | 0.107 | 0.185 | 0.174 | 0.181 | **0.764** | 0.220 |
| PT3 | 0.299 | 0.249 | 0.191 | 0.232 | 0.135 | **0.784** | 0.224 |
| USE1 | 0.184 | 0.126 | 0.196 | 0.166 | 0.190 | 0.161 | **0.708** |
| USE2 | 0.218 | 0.228 | 0.213 | 0.151 | 0.119 | 0.249 | **0.738** |
| USE3 | 0.224 | 0.236 | - | 0.187 | 0.156 | 0.254 | **0.764** |
| USAT1 | 0.300 | 0.137 | 0.182 | **0.800** | 0.181 | 0.139 | 0.138 |
| USAT2 | 0.281 | 0.326 | 0.162 | **0.678** | 0.126 | 0.195 | 0.155 |
| USAT3 | 0.276 | 0.190 | 0.168 | **0.787** | 0.196 | 0.170 | 0.124 |
| USAT4 | 0.252 | 0.309 | 0.138 | **0.730** | 0.241 | 0.171 | 0.244 |
| NETB1 | 0.265 | **0.717** | 0.209 | 0.193 | 0.227 | 0.133 | 0.195 |
| NETB2 | 0.290 | **0.801** | 0.220 | 0.185 | 0.179 | 0.164 | 0.134 |
| NETB3 | 0.297 | **0.708** | 0.210 | 0.216 | 0.184 | 0.194 | - |
| NETB4 | 0.216 | **0.758** | - | 0.176 | 0.228 | - | 0.211 |
| NETB5 | 0.278 | **0.805** | 0.243 | 0.190 | 0.189 | 0.145 | 0.161 |

**Table 7.5:** Assessment of unidimensionality of measured constructs using EFA.

### Multicollinearity test

Multicollinearity points to a strong correlation between latent variables. High multicollinearity can affect the results of the model. We used the Variance Inflation Factor (VIF) method to test multicollinearity between the model's latent variables. The VIF value of an independent variable indicates how well the variable is explained by other constructs' indicators [209]. Values $\geqslant 5$ indicate collinearity between the

| | CONQ | SYSQ | SERQ | PT | USE | USAT | NETB |
|---|---|---|---|---|---|---|---|
| **CONQ** | - | - | - | 1.702 | 2.072 | 1.863 | - |
| **SYSQ** | - | - | - | 1.668 | 1.751 | 1.717 | - |
| **SERQ** | - | - | - | 1.612 | 1.658 | 1.694 | - |
| **PT** | - | - | - | - | - | 1.59 | - |
| **USE** | - | - | - | - | - | - | 1.393 |
| **USAT** | - | - | - | - | 1.909 | - | 1.393 |
| **NETB** | - | - | - | - | - | - | - |

**Table 7.6:** Multicollinearity test using VIF.

independent variables [210].

Table 7.6 shows the VIF value of our model's exogenous variables. All of the VIF values are less than 5, which confirms that there is no multicollinearity between independent variables.

### Internal consistency

Internal consistency is usually determined according to Cronbach's alpha (CA) criterion. A high CA value indicates that all the items of one constructs have the same range and meaning [211]. However, composite reliability (CR) is used as an alternative measure to latent variables' reliability since it overcomes some of CA's shortcoming and provides more reliable results [210]. CA and CR scales range from 0 to 1, with a higher value indicating higher reliability level. Values greater than 0.7 for both scales denote acceptable construct reliability [212]. Internal consistency test results are summarised in Table 7.7. CA and CR values of all latent variables in our model were greater than the recommended minimum of 0.7, indicating good reliability of the study's constructs.

### Indicator reliability

Indicator reliability represents the proportion of indicator variance that is explained by the latent variable. It denotes the extent to which the set of variables is consistent in terms of what it intends to measure.

We used a confirmatory factor analysis (CFA) within PLS to evaluate indicator reliability. The number of factors was specified a priori. Each construct's reliability is calculated on its own independent of the others. Indicators with a loading

| Construct | CA | CR | AVE |
|---|---|---|---|
| Content quality (CONQ) | 0.954 | 0.954 | 0.776 |
| System quality (SYSQ) | 0.906 | 0.908 | 0.714 |
| Service quality (SERQ) | 0.924 | 0.925 | 0.755 |
| Perceived trust (PT) | 0.937 | 0.939 | 0.839 |
| Use (USE) | 0.900 | 0.901 | 0.752 |
| User satisfaction (USAT) | 0.944 | 0.944 | 0.807 |
| Net benefit (NETB) | 0.955 | 0.955 | 0.809 |

**Table 7.7:** Internal consistency and convergent validity.
CA: Cronbach's alpha
CR: Composite Reliability
AVE: Average Variance Extracted

below 0.7 are considered unreliable [198]. Table 7.8 shows that, in our model, all loadings are above the 0.7 threshold, which indicates that more than 50% of each item's variance is caused by the respective construct. The results confirm the validity of the study's indicators.

### Convergent validity

Convergent validity measures the degree to which a set of items, reflecting a construct, converge, compared to items measuring different constructs. To assess convergent validity, each latent variable's Average Variance Extracted (AVE) is calculated as suggested by Fornell and Larcker in [213]. A value of 0.5 or greater is considered acceptable [212].

Table 7.7 shows that the AVE value for each of the latent variables in our model is above 0.5, confirming that the constructs' variance is larger than the variance caused by the associated measurement errors. This result confirms that our theory that each set of items is related to the same corresponding construct.

### Discriminant validity

Discriminant (or divergent) validity refers to the extent to which the constructs differ from one another empirically. It ensures that a construct has the strongest relationships with its own indicators [130].

Discriminant validity is evaluated by comparing an indicator's loading with its cross-loadings on other constructs in the model. If the indicator's outer loading on

its assigned construct is greater than any of its cross-loadings on other construct, good discriminant validity is achieved [210].

The second test of discriminant validity is the Fornell-Lacker criterion, which compares the correlations between latent variables to the square root of the average variance extracted (AVE). Therefore, the square root of each construct's AVE should have a greater value than the correlations with other latent constructs [7] since it should better explain the variance of its own indicator rather than the variance of other latent constructs.

Table 7.8 shows that each indicator's loading is higher for its assigned construct than any of its cross-loadings on all other constructs in the research model. Table 7.9 shows that the square root of AVE for each of the latent variables was greater than its corresponding correlation with any of the other latent variables. The results from both tables indicate that all of our model's constructs are sufficiently dissimilar indicating good discriminant validity.

### 7.5.3 Structural model evaluation

Our assessment of the measurement model confirmed that it meets the criteria of convergent validity, discriminant validity, and construct reliability. We therefore moved to evaluating the structural model (inner model). Evaluating the structural model was done to examine the relationship between latent constructs by looking at the estimated results of the path parameter coefficients and their significance level. We also reviewed the extent to which the model can explain the relationship between the exogenous variables and the endogenous variables. We used bootstrapping with 1000 resamples to test regression coefficients for statistical significance and to determine the significance of the paths within the structural model. The results are depicted in Figure 7.3.

#### Model fit

The coefficient of determination ($R^2$) measures the overall effect size, or the variance explained in the structural model's endogenous construct. $R^2$ is therefore considered

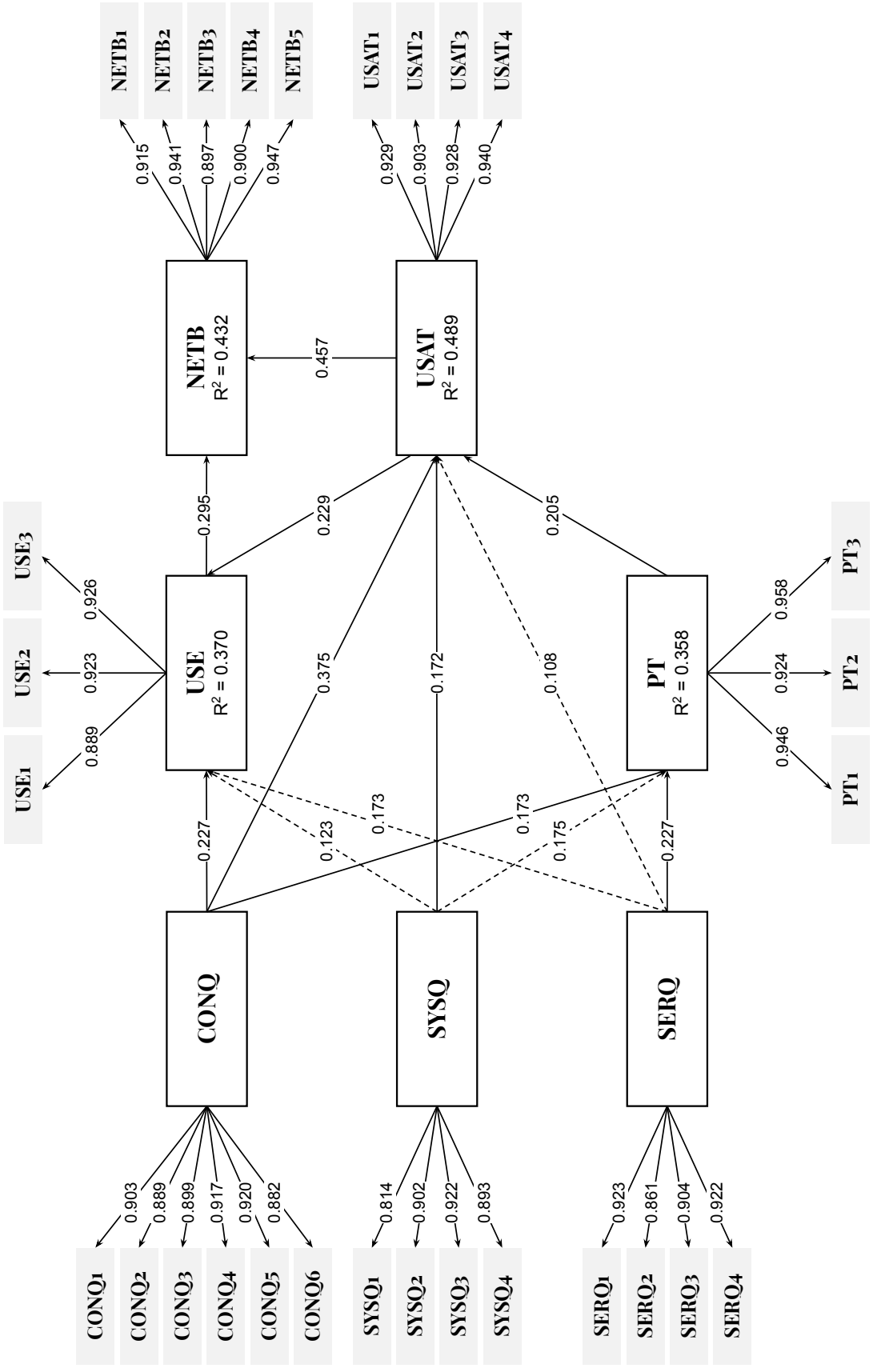



**Figure 7.3:** Path coefficients of Partial Least Square (PLS) analysis.

| | Factor | | | | | | |
|---|---|---|---|---|---|---|---|
| | **CONQ** | **SYSQ** | **SERQ** | **PT** | **USAT** | **USE** | **NETB** |
| CONQ1 | **0.903** | 0.506 | 0.477 | 0.462 | 0.485 | 0.567 | 0.574 |
| CONQ2 | **0.889** | 0.567 | 0.522 | 0.530 | 0.515 | 0.588 | 0.578 |
| CONQ3 | **0.899** | 0.513 | 0.482 | 0.482 | 0.461 | 0.570 | 0.559 |
| CONQ4 | **0.917** | 0.567 | 0.487 | 0.489 | 0.519 | 0.594 | 0.605 |
| CONQ5 | **0.920** | 0.530 | 0.500 | 0.479 | 0.473 | 0.591 | 0.615 |
| CONQ6 | **0.882** | 0.415 | 0.520 | 0.501 | 0.473 | 0.579 | 0.597 |
| SYSQ1 | 0.353 | **0.814** | 0.467 | 0.382 | 0.376 | 0.376 | 0.410 |
| SYSQ2 | 0.519 | **0.902** | 0.476 | 0.402 | 0.401 | 0.482 | 0.517 |
| SYSQ3 | 0.587 | **0.922** | 0.524 | 0.496 | 0.469 | 0.531 | 0.606 |
| SYSQ4 | 0.542 | **0.893** | 0.442 | 0.408 | 0.413 | 0.518 | 0.496 |
| SERQ1 | 0.467 | 0.437 | **0.923** | 0.420 | 0.404 | 0.464 | 0.516 |
| SERQ2 | 0.420 | 0.486 | **0.861** | 0.445 | 0.404 | 0.333 | 0.459 |
| SERQ3 | 0.552 | 0.481 | **0.904** | 0.438 | 0.464 | 0.488 | 0.499 |
| SERQ4 | 0.542 | 0.541 | **0.922** | 0.492 | 0.461 | 0.535 | 0.516 |
| PT1 | 0.477 | 0.445 | 0.452 | **0.946** | 0.543 | 0.478 | 0.489 |
| PT2 | 0.441 | 0.432 | 0.436 | **0.924** | 0.528 | 0.465 | 0.413 |
| PT3 | 0.605 | 0.478 | 0.512 | **0.958** | 0.593 | 0.587 | 0.574 |
| USE1 | 0.452 | 0.428 | 0.429 | 0.480 | **0.889** | 0.451 | 0.429 |
| USE2 | 0.512 | 0.423 | 0.487 | 0.567 | **0.923** | 0.490 | 0.519 |
| USE3 | 0.516 | 0.441 | 0.404 | 0.566 | **0.926** | 0.511 | 0.521 |
| USAT1 | 0.592 | 0.482 | 0.473 | 0.469 | 0.457 | **0.929** | 0.490 |
| USAT2 | 0.598 | 0.464 | 0.460 | 0.519 | 0.484 | **0.903** | 0.612 |
| USAT3 | 0.587 | 0.497 | 0.472 | 0.496 | 0.451 | **0.928** | 0.537 |
| USAT4 | 0.608 | 0.564 | 0.482 | 0.532 | 0.564 | **0.940** | 0.624 |
| NETB1 | 0.599 | 0.548 | 0.523 | 0.482 | 0.518 | 0.565 | **0.915** |
| NETB2 | 0.626 | 0.532 | 0.539 | 0.506 | 0.492 | 0.577 | **0.941** |
| NETB3 | 0.610 | 0.518 | 0.508 | 0.510 | 0.449 | 0.575 | **0.897** |
| NETB4 | 0.538 | 0.520 | 0.408 | 0.429 | 0.501 | 0.523 | **0.900** |
| NETB5 | 0.627 | 0.548 | 0.557 | 0.500 | 0.514 | 0.585 | **0.947** |

**Table 7.8:** Outer and cross-loadings of each indicator in the model.

a measure of the model's predictive accuracy. A model can be evaluated based on the $R^2$ values [214, 215]. $R^2$ takes values between 0 and 1 with higher values indicating higher predictive accuracy.

The use of the adjusted determination coefficient is suggested by [216] to avoid bias in the number of predictors included in the model. Four dependent variables were included in the research model. The adjusted $R^2$ for *perceived trust* was 0.361,

| | CONQ | SYSQ | SERQ | PT | USE | USAT | NETB |
|---|---|---|---|---|---|---|---|
| **CONQ** | **0.902** | | | | | | |
| **SYSQ** | 0.574 | **0.884** | | | | | |
| **SERQ** | 0.553 | 0.540 | **0.903** | | | | |
| **PT** | 0.545 | 0.481 | 0.498 | **0.943** | | | |
| **USE** | 0.540 | 0.472 | 0.482 | 0.591 | **0.913** | | |
| **USAT** | 0.645 | 0.544 | 0.510 | 0.546 | 0.531 | **0.925** | |
| **NETB** | 0.653 | 0.580 | 0.552 | 0.528 | 0.538 | 0.614 | **0.920** |

**Table 7.9:** Inter-construct correlations.

Note: numbers on the diagonal represent the square root of the average variance extracted

which means that *content quality*, *service quality*, and *system quality* explained 36% of the variability in *perceived trust*. The adjusted $R^2$ for *use*, *user satisfaction*, and *net benefits* were 0.369, 0.489, and 0.433 respectively. According to [217], values greater than 0.25 (25%) indicate moderate predictive power.

We also used the Standardised Root Mean Square Residual (SRMR) to test the model fit. SRMR is defined as the difference between the model's implied correlation matrix and the observed correlation, which allows us to assess the average magnitude of the discrepancies between observed and expected correlations as a measure of model. The test results showed that the model was a good fit for the data as shown by the SRMR value of 0.086 which was below the suggested threshold of 0.1 and indicated acceptable fit [218].

### Hypothesis testing

Path coefficients (regression coefficients) obtained from Partial Least Square (PLS) were used to test the research hypotheses. The path coefficient denotes the extent to which an independent variable affects its dependent variable. Regression coefficients were tested for statistical significance using 1000 bootstrapped resamples. The bootstrapped samples were used to calculate standard errors and the corresponding 95% confidence intervals. The consistent PLS (PLSc) algorithm was used to evaluate the research model. PLSc corrects the constructs' correlations to ensure the results are consistent with a factor-model [219].

| Hypothesis | | $\beta$ | $\bar{x}$ | $s$ | $t$ | $f^2$ | $p$ | Support |
|---|---|---|---|---|---|---|---|---|
| H1a | CONQ → USE | 0.227 | 0.228 | 0.095 | 2.398 | 0.041 | 0.017 | Yes |
| H1b | CONQ → USAT | 0.375 | 0.377 | 0.081 | 4.652 | 0.152 | <0.001 | Yes |
| H1c | CONQ → PT | 0.319 | 0.317 | 0.081 | 3.545 | 0.095 | <0.001 | Yes |
| H2a | SYSQ → USE | 0.123 | 0.126 | 0.090 | 1.289 | 0.014 | 0.198 | No |
| H2b | SYSQ → USAT | 0.172 | 0.170 | 0.082 | 2.092 | 0.035 | 0.037 | Yes |
| H2c | SYSQ → PT | 0.175 | 0.174 | 0.092 | 1.909 | 0.029 | 0.057 | No |
| H3a | SERQ → USE | 0.173 | 0.170 | 0.090 | 1.907 | 0.029 | 0.057 | No |
| H3b | SERQ → USAT | 0.107 | 0.108 | 0.077 | 1.394 | 0.014 | 0.164 | No |
| H3c | SERQ → PT | 0.227 | 0.229 | 0.088 | 2.580 | 0.051 | 0.010 | Yes |
| H4 | PT → USAT | 0.206 | 0.201 | 0.087 | 2.381 | 0.054 | 0.017 | Yes |
| H5 | USAT → USE | 0.230 | 0.226 | 0.109 | 2.114 | 0.045 | 0.035 | Yes |
| H6 | USE → NETB | 0.295 | 0.294 | 0.088 | 3.357 | 0.111 | 0.001 | Yes |
| H7 | USAT → NETB | 0.458 | 0.460 | 0.086 | 5.310 | 0.269 | <0.001 | Yes |

**Table 7.10:** Hypothesis testing results.

$\beta$: path coefficient
$\bar{x}$: sample mean
$s$: standard deviation
$f^2$: effect size
$t$: t statistics = $\beta/s$

We considered a hypothesis to be supported by the data if the corresponding path coefficient was significant at the $p < 0.05$ threshold (Table 7.10). Hypotheses testing results are as follows:

**H1.a Content quality has a positive influence on the use of the TIMP.**

There was a statistically significant positive association between CONQ and USE ($\beta = 0.227$, $p < 0.05$), which indicates that a 1 SD increase in *content quality* is associated with a 0.227 SD increase in platform *use*. Thus, the null hypothesis can be rejected in favour of the alternative hypothesis.

**H1.b Content quality has a positive influence on user satisfaction with a TIMP.**

There was a statistically significant positive association between CONQ and USAT ($\beta = 0.375$, $p < 0.001$), which indicates that a 1 SD increase in *content quality* is associated with a 0.375 SD increase in *user satisfaction*. Thus, the null hypothesis can be rejected in favour of the alternative hypothesis.

**H1.c Content quality has a positive influence on user trust in a TIMP.**

There was a statistically significant positive association between CONQ and PT ($\beta = 0.319$, $p < 0.001$), which indicates that a 1 SD increase in *content*

*quality* is associated with a 0.319 SD increase in the *perceived trust*. Thus, the null hypothesis can be rejected in favour of the alternative hypothesis.

**H2.a System quality has a positive influence on the use of a TIMP.**

No statistically significant association was observed between SYSQ and USE ($\beta = 0.123$, $p > 0.05$). Thus, the null hypothesis can be accepted.

**H2.b System quality has a positive influence on user satisfaction with a TIMP.**

There was a statistically significant positive association between SYSQ and USAT ($\beta = 0.172$, $p < 0.05$), which indicates that 1 SD increase in *system quality* is associated with a 0.172 SD increase in *user satisfaction*. Thus, the null hypothesis can be rejected in favour of the alternative hypothesis.

**H2.c System quality has a positive influence on the perceived trust.**

No statistically significant association was observed between SYSQ and PT ($\beta = 0.175, p > 0.05$). Thus, the null hypothesis can be accepted.

**H3.a Service quality has a positive influence on the use of a TIMP.**

No statistically significant association was observed between SERQ and USE ($\beta = 0.173$, $p > 0.05$). Thus, the null hypothesis can be accepted.

**H3.b Service quality has a positive influence on user satisfaction with a TIMP.**

No statistically significant association was observed between SERQ and USAT ($\beta = 0.107$, $p > 0.05$). Thus, the null hypothesis can be accepted.

**H3.c Service quality has a positive influence on the perceived trust.**

There was a statistically significant positive association between SERQ and PT ($\beta = 0.227$, $p < 0.05$), which indicates that a 1 SD increase in *service quality* is associated with a 0.227 SD increase in the *perceived trust*. Thus, the null hypothesis can be rejected in favour of the alternative hypothesis.

**H4 Perceived trust has a positive influence on user satisfaction with a TIMP.**

There was a statistically significant positive association between PT and USAT ($\beta = 0.206$, $p < 0.05$), which indicates that a 1 SD increase in *perceived*

*trust* is associated with a 0.206 SD increase in *user satisfaction*. Thus, the null hypothesis can be rejected in favour of the alternative hypothesis.

**H5 User satisfaction has a positive influence on the use of a TIMP.**

There was a statistically significant positive association between USAT and USE ($\beta = 0.23$, $p < 0.05$), which indicates that 1 SD increase in *user satisfaction* with the platform is associated with a 0.23 SD increase in the *use* of the platform. Thus, the null hypothesis can be rejected in favour of the alternative hypothesis.

**H6 TIMP use has a positive influence on the net benefits of the platform.**

There was a statistically significant positive association between USE and NETB ($\beta = 0.295$, $p < 0.05$), which indicates that 1 SD increase in the *use* of the platform is associated with a 0.295 SD increase in the *net benefits* of the platform. Thus, the null hypothesis can be rejected in favour of the alternative hypothesis.

**H7 User satisfaction has a positive influence on the net benefits of the TIMP.**

There was a statistically significant positive association between USAT and NETB ($\beta = 0.458$, $p < 0.001$), which indicates that a 1 SD increase in *user satisfaction* is associated with a 0.458 SD increase in *net benefits* of the platform. Thus, the null hypothesis can be rejected in favour of the alternative hypothesis.

**Effect size**

Effect size (ES) of independent variables on the corresponding dependent variables were calculated using $f^2$. Cohen's $f^2$ can be used to calculate the ES for multiple regression models when the independent variable of interest and the dependent variable are both continuous. Cohen's $f^2$ is presented in a form appropriate for global effect size: $f^2 = R^2/(1 - R^2)$. $f^2 \geq 0.02$, $f^2 \geq 0.15$, and $f^2 \geq 0.35$ represent small, medium, and large effect sizes, respectively. ES evaluation is presented in Table 7.10.

## 7.6 Discussion

As Table 7.10 shows, most of the model's hypotheses are supported by our study. The paths from *content quality* to *use* and *user satisfaction*, from *use* to *user satisfaction*, as well as from *use* and *user satisfaction* to *net benefits* appear to be consistent with the hypotheses made in the original D&M information systems success model [15]. Conversely, the paths from *system* and *service quality* to *use*, and from *service quality* to *user satisfaction* are not statistically significant.

Our results, however, provide evidence for most of the hypotheses involving the newly added success construct. The paths from *content* and *service quality* to *perceived trust*, as well as from *perceived trust* to *user satisfaction* are supported. Only the path between *system quality* and *perceived trust* is not significant.

The results indicate that *content quality* is the only construct that significantly influences *perceived trust*, *user satisfaction* and *use* at the same time. In other words, the quality of the platform's content seems to be one of the most important success factors. A high-quality content would increase the users' trust in the platform and their overall satisfaction. It would also drive them to utilise the platform in performing their tasks. Therefore, ensuring the provision of good content in a TIMP may directly strengthen trust, use and user satisfaction, and, eventually, the net benefits gained from deploying the platform.

As depicted in Figure 7.3, service quality does not significantly influence user satisfaction or use. This may be explained by assuming that, for the platform's users, vendor's support personnel play a minimal, if any, role in their everyday interaction with the platform. Instead, service quality significantly influence the user's perceived trust in the platform highlighting the role of the vendor's personnel in building and maintaining trust with the users. The relationship between service quality and user satisfaction has been investigated in several studies in the literature [220, 221]. However, these studies suggest mixed support for this relationship. Petter and colleagues suggest that the inconsistency in the findings is partly due to the utilisation of different methods in measuring service quality [56].

As for system quality, it also does not significantly influence use. One explanation could be that, for the users we surveyed, the actual use of a TIMP depends primarily on the content it provides and less so on the quality or features of the system. This explanation is consistent with earlier discussions with practitioners who stated that despite what is often promoted by vendors, the platform's technical features and capabilities are, in most cases, of limited use. Support for this relationship in the literature is mixed. The extent to which the technical aspect of an information system determines the use or discontinuance of use varies depending on the purpose of the system and the definition of system quality [56].

Nevertheless, system quality significantly influence user satisfaction, which is consistent with the findings of other studies in the information systems literature [56]. This observation in particular is not surprising as there is a strong support for the relationship between system quality and user satisfaction in the literature [56, 222].

It is important to note that although the utilisation of a TIMP is voluntary in most cases, for threat intelligence analysts, certain data or information can only be received or shared through the platform. The quasi-mandatory nature of using an information system as Urbach and colleagues suggest in [65] offers another possible explanation as to why system and service quality do not significantly influence the actual use of the platform.

In line with the corresponding hypotheses in the D&M model, our results suggest that both use and user satisfaction influence the net benefits gained by utilising a TIMP. The highly significant impact of user satisfaction on net benefits indicates that user satisfaction may serve as a reasonable surrogate for net benefits as suggested in previous studies [65, 194, 222]. However, the moderate $R^2$ of net benefits indicates that several other factors influence the final dependant construct in the model.

We also calculated the total effect of each of the model's exogenous variables, that is *content*, *system* and *service quality*, on *net benefits* in order to further investigate the success factors that have the highest impact on the model's effectiveness level [65]. The total effect of a latent variable on another is calculated by adding the latent variable's direct effect to all its indirect effects on the other [214]. The total effects

of *content*, *system* and *service quality*, on *net benefits* are 0.298, 0.146 and 0.131 respectively, indicating that *content quality* is the factor that influences the model's effectiveness level the most, followed by *system* and *service quality*.

In conclusion, our findings indicate that the success constructs of the D&M model fall short from fully capturing the characteristics of a threat intelligence management platform as a particular case of an information system. Although it provides a useful starting point for modelling the success of TIMPs, the applicability of the D&M success model is limited. On a practical level, the results provide practitioners with empirical evidence that helps in determining the organisation's priorities while trying to improve their threat intelligence platform. Accordingly, improving content quality should be the primary consideration since it potentially has the greatest impact on the users' day-to-day activities.

## 7.7 Summary

In this chapter we introduced and tested a multi-dimensional success model for threat intelligence management platforms. To the best of our knowledge, it is the first attempt to empirically validate a comprehensive success model for threat intelligence platforms.

The model was based on DeLone and McLean's information systems success model [15], and incorporated some of our findings from earlier chapters. We developed a number of hypotheses that reflected the associations between the models' success factors and tested them through a survey.

The measurement and structural evaluation of the model revealed that the quality of the content and the perceived trust in the platform are among the most important success factors and have to be considered as priorities for operating a successful TIMP.

These findings allow practitioners to better understand the factors that influence the improvement and success of their TIMP and how they interact with each other. The empirical validation of this comprehensive success model for TIMPs, advances

the theoretical and practical understanding in the area of threat intelligence sharing and provides solid grounds for further research in this field.

# 8 Conclusions

Efforts in the public and private sectors to foster information sharing initiatives have intensified in recent years resulting in the current complex constellation of sharing organisations, forums, platforms and tools, including threat intelligence management solutions. Nevertheless, despite the increased recognition of its importance, a number of questions pertaining to the nature of cyber security information sharing and its success remain unanswered.

In an attempt to answer some of these questions, this dissertation used mixed methods to draw on practitioners' experiences and collect empirical data necessary to ensure that our conclusions are relevant to theory and practice. The dissertation relied on the well-established premise that the success of a system or a process cannot be reasonably assessed without a thorough understanding of the goals it is designed to achieve.

Studying the practitioners' understanding of cyber security information sharing in Chapter 4 suggested that threat-centric data sharing has dominated cyber security information sharing efforts despite being perceived as the least useful activity. The survey also revealed that most respondents find it difficult to determine the effectiveness and quality of the data being shared. Nevertheless, they unanimously expressed interest in developing methods to address quality concerns and determine the overall success of information sharing activities.

The reasons behind the disparity between the perceived usefulness and the actual use of threat-centric information sharing were examined in Chapter 5 to gain some empirical insights. We started by attempting to explore the extent to which the benefits and barriers suggested by the cyber security information sharing literature were reflected in the attitudes of practitioners. Concerns regarding the quality and effectiveness of threat-centric information sharing echoed our findings in Chapter 4. Issues surrounding the quality of the information being shared including its timeliness, relevance and consistency represented the most agreed-on challenges among the participants.

Chapter 6 aimed to identify the practitioners' most important threat intelligence quality needs. A systematic review of relevant literature, followed by a modified Delphi study, resulted in identifying seven quality attributes. It also examined the literature definitions of threat data, information and intelligence, and suggested areas for improvement. We found that practitioners' quality priorities varied depending on the nature of the intelligence. We also observed that, despite increasing awareness of their potential value, organisations were yet to develop concrete metrics to measure any of the quality dimensions, and that they largely relied on consumer feedback and anecdotal evidence.

The success model introduced in Chapter 7 incorporated our earlier findings in developing and testing a comprehensive multi-dimensional model for determining the success of threat intelligence management platforms. The evaluation of the model revealed that the quality of the content and the perceived trust in the platform are among the most important success factors and have to be considered as priorities for operating a successful TIMP. Our findings also indicated that the success constructs of the D&M model provides a useful starting point for modelling the success of TIMPs. However, the model falls short from fully capturing the characteristics of a threat intelligence management platform as a particular case of an information system.

## 8.1 Benefits and impact

The categorisation of cyber security information sharing activities introduced in Chapter 4 could provide practitioners, researchers and policymakers with a useful tool to clearly distinguish and discuss each of the activities. Understanding what each of these activities is trying to achieve is also a critical first step for any evaluation effort. It could also help organisations make better investment decisions as it guides them to participating or implementing the form of information sharing that best meets their needs.

Researchers and practitioners can look at Chapter 5 for a summary of the real-world benefits and barriers facing threat-centric information sharing. For organisations planning to implement such forms of information sharing, the findings could help them understand what to expect. They also provide developers and organisers of current and future threat-centric information sharing activities with empirical evidence about the reasons behind the activities' shortcomings.

The quality requirements identified in Chapter 6 could contribute to mitigating some of the concerns surrounding the quality of information sharing by serving as a foundational framework for measuring, analysing and improving threat intelligence quality. Security vendors can look at the set of quality dimensions identified in this chapter to extend their knowledge of what quality attributes are most relevant to practitioners and redesign their products accordingly. Similarly, the dimensions can assist an organisation in comparing and selecting the most appropriate threat intelligence service for its needs.

Finally, the model introduced in Chapter 7 allows organisations to evaluate and predict the success of threat intelligence management platforms. Our findings assist practitioners with identifying the determinants of successful platforms and help them prioritise investments accordingly. The model also contributes to theory as it extends and further tests the D&M information systems success model in a different setting and for a new system context. It advances the theoretical development in the area of threat intelligence management solutions and serves as a basis for future research in this field.

The academic community can benefit from new research directions. In the next section we present our suggestions for how these contributions might be further developed in future work.

## 8.2 Future work

The empirical studies in Chapters 4 and 5 would benefit from replications in new countries and regions. After all, cyber security is a global challenge that requires a collaborative international effort. It would be useful to capture the practitioners' attitudes and understanding towards information sharing activities, incentives and barriers in regions beyond the United Kingdom and Europe. This could help identify specific cultural, economic or policy factors that positively or negatively influence the success of cyber security information sharing in those regions.

The high-level categorisation of cyber security information sharing activities introduced in Chapter 4 would benefit from further validation with larger sample size. It could also be used in developing a more granular taxonomy that clarifies and distinguishes each form of information sharing, and allows greater analytical precision.

There would also be value in repeating the study in Chapter 5 to determine whether the threat-centric information sharing landscape is maturing over time, and to continue to bridge the gap between theory and practice.

The generalisability of the findings of Chapter 6 is limited by the inherent limitations of the Delphi technique as it relies on a limited number of experts and could be the subject of a selection bias. Although we tried to minimise the impact by recruiting a large panel of 30 experts from around Europe, future research might replicate this study with a different panel or use our results as the basis for a different data collection approach designed to test for generalisability.

Finally, our model in Chapter 7 has a few limitations. Some of the hypothesised relationships are not supported. Although we provided possible explanations for these results, the available data does not allow for testing these explanations any further. The influence of system and service quality on user satisfaction and use of threat intelligence platforms seems especially worth investigating further. The

findings are further limited by the fact that we used a convenience sample of organisations for data collection. Future work could use a random and larger sample from a pool of organisations in order to provide a more accurate insight into the effects among the model's constructs, and increase the generalisability of the findings. It could also apply the proposed research instrument to a single organisation in order assess how the variables relate in the context of this particular organisation. We should also note that we captured and investigated the user perceptions of threat intelligence management platform based on different commercial platforms, each of which had been customised to the organisation's requirements. Future research could replicate the study across a group of organisations using the same platform.

## 8.3 Conclusion

To conclude, we return to the question *how can cyber security information sharing be made more successful?*. A comprehensive answer at this stage is beyond our scope and arguably unattainable in the foreseeable future given the multidimensional nature of the problem. Instead, we considered specific aspects in isolation. The first step towards achieving a successful information sharing is understanding what different activities are trying to accomplish and determining which one of them meets the organisation's requirements. We found that threat-centric data sharing is the most popular form of information sharing activities given the speed at which this type of information can be shared and the fact that it provides organisations with seemingly immediate benefits. Organisations however should not lose sight of equally beneficial forms of sharing including the exchange of triggers for action, knowledge and expertise.

We also found that practitioners have begun to place greater focus on generating value from threat-centric information sharing. Addressing quality concerns is therefore paramount to ensure that threat-centric information (or threat intelligence) sharing is serving the purpose it has been built for. The quality attributes we identified, including accuracy, actionability, provenance and timeliness, can serve as a foundation for bench-marking and developing effective metrics.

This is especially important when employing a threat intelligence management platform where we discovered that the quality of the content is the most important success factor. However, other variables, including system and service quality as well as perceived trust, also play a role in increasing the use of and user satisfaction with the platform and in ultimately increasing the overall benefits to the organisation.

Our multi-dimensional model can reduce uncertainty and offer a tool for organisations to evaluate and predict the success of their threat intelligence management platform. This, in turn, could offer an organisation a better understanding of their wider threat intelligence and information sharing needs and help inform their investment decisions accordingly.

# References


[1] A. Mohaisen, O. Al-Ibrahim, C. Kamhoua, K. Kwiat, and L. Njilla. "Rethinking Information Sharing for Threat Intelligence". In: *Proceedings of the 5th ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies*. HotWeb '17. San Jose, California: ACM, 2017, 6:1–6:7. URL: http://doi.acm.org/10.1145/3132465.3132468.

[2] 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. Denver, Colorado, USA: ACM, 2015, pp. 43–49. URL: http://doi.acm.org/10.1145/2808128.2808133.

[3] C. Gilbert. "Scalable security: Cyber threat information sharing in the internet age". MA thesis. Stanford University, 2014.

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

[5] 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.

[6] M. C. Libicki. *Sharing information about threats is not a cybersecurity panacea*. http://www.rand.org/pubs/testimonies/CT425.html. 2015.

[7] T. Ring. "Threat intelligence: why people don't share". In: *Computer Fraud & Security* 2014.3 (2014), pp. 5–9. URL: http://www.sciencedirect.com/science/article/pii/S1361372314704695.

[8] B. Buchanan. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford University Press, 2016.

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

[10] 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 13th International Conference on Wirtschaftsinformatik*. WI 2017. St. Gallen, Switzerland, 2017, pp. 837–851. URL: https://www.wi2017.ch/images/wi2017-0188.pdf.

[11] C. Sauerwein, C. Sillaber, and R. Breu. "Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes". In: *Proceedings of Multikonferenz Wirtschaftsinformatik 2018*. MKWI '18. Lüneburg, Germany, 2018, pp. 1333–1344.

[12] 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 2018*. MKWI '18. Lüneburg, Germany, 2018, pp. 1409–1420.

[13] 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". In: *Computers & Security* 60 (2016), pp. 154–176. URL: http://dx.doi.org/10.1016/j.cose.2016.04.003%20http://linkinghub.elsevier.com/retrieve/pii/S0167404816300347.

[14] W. H. DeLone and E. R. McLean. "Information Systems Success: The Quest for the Dependent Variable". In: *Information Systems Research* 3.1 (1992), pp. 60–95. URL: https://doi.org/10.1287/isre.3.1.60.

[15] W. H. DeLone and E. R. McLean. "The DeLone and McLean model of information systems success: A ten-year update". In: *Journal of Management Information Systems* 19.4 (2003), pp. 9–30.

[16] G. P. Z. Montesdioca and A. C. G. Maçada. "Quality Dimensions of the DeLone-McLean Model to Measure User Satisfaction: An Empirical Test on the Information Security Context". In: *Proceedings of the 2015 48th Hawaii International Conference on System Sciences*. IEEE, 2015, pp. 5010–5019.

[17] D. E. Zheng and J. A. Lewis. *Cyber Threat Information Sharing Recommendations for Congress and the Administration*. https://www.csis.org/analysis/cyber-threat-information-sharing. Washington, DC, 2015.

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

[19] A. Zibak and A. Simpson. "Can We Evaluate the Effectiveness of Cyber Security Information Sharing Efforts?" In: *Proceedings of the 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*. CyberSA 2018. Glasgow, UK: IEEE, 2018.

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

[21] 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.

[22] ENISA. *Standards and tools for exchange and processing of actionable information*. https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information. 2014.

[23] P. Kampanakis. "Security Automation and Threat Information-Sharing Options". In: *IEEE Security Privacy* 12.5 (2014), pp. 42–51.

[24] R. F. Dacey. *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*. https://www.gao.gov/new.items/d04699t.pdf. 2004.

[25] ENISA. *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. 2010.

[26] R. N. Thomas. *Securing Cyberspace Through Public-Private Partnerships*. https://www.csis.org/analysis/securing-cyberspace-through-public-private-partnerships. 2013.

[27] A. Aviram and A. Tor. "Overcoming Impediments to Information Sharing". In: *Harvard Law School John M. Olin Center for Law, Economics and Business Discussion Paper Series* 55 (Oct. 2010).

[28] L. A. Gordon, M. P. Loeb, and W. Lucyshyn. "Sharing information on computer systems security: An economic analysis". In: *Journal of Accounting and Public Policy* 22.6 (2003), pp. 461–485. URL: http://linkinghub.elsevier.com/retrieve/pii/S0278425403000632.

[29] S. E. Schechter and M. D. Smith. "How Much Security Is Enough to Stop a Thief?" In: *Proceedings of the Financial Cryptography Conference*. Springer, 2003, pp. 122–137.

[30] E. Gal-Or and A. Ghose. "The economic incentives for sharing security information". In: *Information Systems Research* 16.2 (2005), pp. 186–208.

[31] 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.

[32] M. Dunn-Cavelty and M. Suter. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection". In: *International Journal of Critical Infrastructure Protection* 2.4 (2009), pp. 179–187. URL: http://www.sciencedirect.com/science/article/pii/S1874548209000274.

[33] P. W. Singer and A. Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2013.

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

[35] A. Y. Akbulut and J. Motwani. "Integration and Information Sharing in E-Government". In: *Encyclopedia of Networked and Virtual Organizations*. IGI Global, 2008, pp. 729–734.

[36] US Department of Defense, Office of the Chief Information Officer. *Department of Defense Information Sharing Strategy*. https://dodcio.defense.gov/Portals/0/Documents/DIEA/InfoSharingStrategy.pdf. 2007.

[37] 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.

[38] ENISA. *Good Practice Guide: Network Security Information Exchanges*. https://www.enisa.europa.eu/publications/good-practice-guide. 2009.

[39] E. Luiijf and M. Klaver. "On the Sharing of Cyber Security Information". In: *Critical Infrastructure Protection IX*. Ed. by M. Rice and S. Shenoi. Springer International Publishing, 2015, pp. 29–46.

[40] W. Tounsi and H. Rais. "A survey on technical threat intelligence in the age of sophisticated cyber attacks". In: *Computers and Security* 72 (2018), pp. 212–233. URL: https://doi.org/10.1016/j.cose.2017.09.001.

[41] ISAO Standards Organization. *Introduction to Information Sharing*. Tech. rep. ISAO 300-1. 2016. URL: https://www.isao.org/products/isao-300-1-introduction-to-information-sharing/.

[42] D. Omand. "Is it time to move beyond the Intelligence Cycle? A UK practitioner perspective". In: *Understanding the Intelligence Cycle*. Routledge, 2013, pp. 148–162.

[43] The Communications Security, Reliability and Interoperability Council. *Conduits for Information Sharing*. https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_InterimReport_122116.PDF. 2016.

[44] T. Sander and J. Hailpern. "UX Aspects of Threat Information Sharing Platforms: An Examination & Lessons Learned Using Personas". In: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*. WISCS '15. Denver, Colorado, USA: ACM, 2015, pp. 51–59. URL: http://doi.acm.org/10.1145/2808128.2808136.

[45] D. F. Vazquez, O. P. Acosta, C. Spirito, S. Brown, and E. Reid. "Conceptual framework for cyber defense information sharing within trust relationships". In: *Proceedings of the 4th International Conference on Cyber Conflict*. CYCON 2012. Tallinn, Estonia: IEEE, 2012. URL: https://ieeexplore.ieee.org/document/6243990.

[46] 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 and Collaborative Security*. WISCS '14. Scottsdale, AZ, USA: ACM, 2014, pp. 61–69. URL: http://dl.acm.org/citation.cfm?doid=2663876.2663882.

[47] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah. "Cyber threat intelligence sharing: Survey and research directions". In: *Computers & Security* (2019).

[48] Ponemon Institute. *Third Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way*. https://www.infoblox.com/wp-content/uploads/infoblox-white-paper-ponemon-infoblox-2018-final-report.pdf. 2018.

[49] ENISA. *Exploring the opportunities and limitations of current Threat Intelligence Platforms*. https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms. 2017.

[50] ISAO Standards Organization. *Automating Cyber Threat Intelligence Sharing*. Tech. rep. ISAO 300-2. 2019. URL: https://www.isao.org/storage/2019/04/ISAO-300-2-Automated-Cyber-Threat-intelligence-Sharing.pdf.

[51] L. Dandurand and O. Serrano. "Towards improved cyber security information sharing ". In: *Proceedings of the 5th International Conference on Cyber Conflict*. CyCon 2013. Tallinn, Estonia: IEEE, 2013. URL: http://ieeexplore.ieee.org/xpls/abs%7B%5C_%7Dall.jsp?arnumber=6568369.

[52] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody. "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, 2016, pp. 49–56. URL: http://doi.acm.org/10.1145/2994539.2994542%20http://dl.acm.org/citation.cfm?doid=2994539.2994542.

[53] C. Edwards, S. Migues, R. J. Nebel, and D. Owen. *System and Method of Data Collection, Processing, Analysis, and Annotation for Monitoring Cyber-threats and the Notification Thereof to Subscribers*. https://patentimages.storage.googleapis.com/94/f9/db/f9ef412c858dc1/US20020038430A1.pdf. U.S. Patent Application No. 09/950,820. 2002.

[54] 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.

[55] S. Appala, N. Cam-Winget, D. McGrew, and J. Verma. "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. Denver, Colorado, USA: ACM, 2015, pp. 61–70. URL: http://dl.acm.org/citation.cfm?doid=2808128.2808131.

[56] S. Petter, W. H. DeLone, and E. R. McLean. "Measuring information systems success: Models, dimensions, measures, and interrelationships". In: *European Journal of Information Systems* 17.3 (2008), pp. 236–263.

[57] L. F. Pitt, R. T. Watson, and C. B. Kavan. "Service Quality: A Measure of Information Systems Effectiveness". In: *MIS Quarterly* 19.2 (1995), pp. 173–187. URL: http://www.jstor.org/stable/249687.

[58] P. B. Seddon. "A Respecification and Extension of the DeLone and McLean Model of IS Success". In: *Information Systems Research* 8.3 (1997), pp. 240–253. URL: https://doi.org/10.1287/isre.8.3.240.

[59] P. B. Seddon, S. Staples, R. Patnayakuni, and M. Bowtell. "Dimensions of Information Systems Success". In: *Communications of the Association for Information Systems* 2.20 (1999). URL: https://aisel.aisnet.org/cais/vol2/iss1/20.

[60] S. Chatterjee, S. Chakraborty, S. Sarker, S. Sarker, and F. Y. Lau. "Examining the success factors for mobile work in healthcare: A deductive study". In: *Decision Support Systems* 46.3 (2009), pp. 620–633. URL: http://dx.doi.org/10.1016/j.dss.2008.11.003.

[61] J. Wu and Y. Wang. "Measuring KMS success: A respecification of the DeLone and McLean's model". In: *Information and Management* 43.6 (2006), pp. 728–739. URL: http://www.sciencedirect.com/science/article/pii/S0378720606000498.

[62] U. Kulkarni, S. Ravindran, and R. Freeze. "A Knowledge Management Success Model: Theoretical Development and Empirical Validation". In: *Journal of Management Information Systems* 23 (Jan. 2007), pp. 309–347.

[63] W. H. DeLone and E. R. McLean. "Measuring e-Commerce Success: Applying the DeLone and McLean Information Systems Success Model". In: *International Journal of Electronic Commerce* 9 (Sept. 2004), pp. 31–47.

[64] Y. Wang and Y. Liao. "Assessing eGovernment systems success: A validation of the DeLone and McLean model of information systems success". In: *Government Information Quarterly* 25.4 (2008), pp. 717–733. URL: http://www.sciencedirect.com/science/article/pii/S0740624X07000615.

[65] N. Urbach, S. Smolnik, and G. Riempp. "An empirical investigation of employee portal success". In: *Journal of Strategic Information Systems* 19.3 (2010), pp. 184–206. URL: http://dx.doi.org/10.1016/j.jsis.2010.06.002.

[66] J. M. Juran and A. B. Godfrey. *Juran's quality handbook*. 5th ed. McGraw Hill, 1998.

[67] P. B. Crosby. *Quality is free : the art of making quality certain*. McGraw-Hill, 1979.

[68] C. Batini and M. Scannapieco. *Data and Information Quality: Dimensions, Principles and Techniques*. Data-Centric Systems and Applications. Springer International Publishing, 2016. URL: https://books.google.co.uk/books?id=kJ%5C_WCwAAQBAJ.

[69] G. K. Tayi and D. P. Ballou. "Examining Data Quality". In: *Communications of the ACM* 41.2 (1998), pp. 54–57. URL: http://doi.acm.org/10.1145/269012.269021.

[70] D. M. Strong, Y. W. Lee, and R. Y. Wang. "Data Quality in Context". In: *Communications of the ACM* 40.5 (1997), pp. 103–110. URL: http://doi.acm.org/10.1145/253769.253804.

[71] R. Y. Wang and D. M. Strong. "Beyond Accuracy: What Data Quality Means to Data Consumers". In: *Journal of Management Information Systems* 12.4 (1996), pp. 5–33. URL: https://doi.org/10.1080/07421222.1996.11518099.

[72] S. Sadiq. *Handbook of Data Quality: Research and Practice*. Springer Berlin Heidelberg, 2013. URL: https://books.google.co.uk/books?id=da-9BAAAQBAJ.

[73] T. C. Redman. *Data Quality for the Information Age*. Artech House Telecommunications Library. Artech House, 1996. URL: https://books.google.co.uk/books?id=UExPAAAAMAAJ.

[74] Y. Wand and R. Y. Wang. "Anchoring Data Quality Dimensions in Ontological Foundations". In: *Communications of the ACM* 39.11 (1996), pp. 86–95. URL: http://doi.acm.org/10.1145/240455.240479.

[75] J. R. Joseph and J. Corkill. "Information evaluation: How one group of intelligence analysts go about the task". In: *Proceedings of the 4th Australian Security and Intelligence Conference*. Perth, Australia, 2011.

[76] M. Sandow-Quirk. "A Failure of Intelligence". In: *Prometheus* 20.2 (2002), pp. 131–142.

[77] D. McDowell. *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users*. Scarecrow Press, 2009.

[78] D. T. Moore, L. Krizan, and E. J. Moore. "Evaluating intelligence: a competency-based model". In: *International Journal of Intelligence and CounterIntelligence* 18.2 (2005), pp. 204–220.

[79] R. J. Heuer. *Psychology of Intelligence Analysis*. Center for the Study of Intelligence, US Central Intelligence Agency (CIA), 1999.

[80] K. Wheaton and D. Chido. "Evaluating intelligence". In: *Competitive Intelligence Magazine* 10.5 (2007), pp. 32–36.

[81] J. J. Peterson. "Appropriate factors to consider when assessing analytic confidence in intelligence analysis". MA thesis. Mercyhurst College Institute for Intelligence Studies (MCIIS), 2008.

[82] H. Zhu and R. Y. Wang. "Information quality framework for verifiable intelligence products". In: *Data Engineering*. Springer, 2009, pp. 315–333.

[83] J. Davis. *Sherman Kent and the profession of intelligence analysis*. https://www.cia.gov/library/kent-center-occasional-papers/vol1no5.htm. Accessed: 2019-11-25. 2002.

[84] J. M. Hanson. "The Admiralty Code: A cognitive tool for self-directed learning". In: *International Journal of Learning, Teaching and Educational Research* 14.1 (2015).

[85] D. Irwin and D. Mandel. "Improving Information Evaluation for Intelligence Production". In: *Intelligence & National Security* 34.4 (2019), pp. 503–525.

[86] G. Spinelli and B. Sharma. "A Paper-Centred Information System: Effectiveness and Quality Implications in UK Police Intelligence Units". In: *Journal of Convergence Information Technology* 2.3 (2007), pp. 11–21.

[87] W. S. Brei. *Getting intelligence right: The power of logical procedure*. Joint Military Intelligence College, 1996.

[88] Ž. Gajić, Z. Jeremić, and M. Stefanović. "Desirable attributes of an effective intelligence analyst". In: *Vojno delo* 69.4 (2017), pp. 86–95.

[89] J. D. Corkill, T. K. Cunow, E. H. Ashton, and A. East. "Attributes of an analyst: What we can learn from the intelligence analysts job description". In: *Proceedings of the 8th Australian Security and Intelligence Conference*. Perth, Australia, 2015.

[90] J. Scholtz, E. Morse, and T. Hewett. "In depth observational studies of professional intelligence analysts". In: *Proceedings of the Human Performance, Situation Awareness and Automation Technology Conference*. Daytona Beach, Florida , USA, 2004.

[91] B. L. W. Wong. "How Analysts Think (?): Early Observations". In: *Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference*. The Hague, Netherlands: IEEE, 2014, pp. 296–299.

[92] S. Marrin. "Evaluating the Quality of Intelligence Analysis: By What (Mis) Measure?" In: *Intelligence and National Security* 27.6 (2012), pp. 896–912.

[93] Ponemon Institute. *The Value of Threat Intelligence: Annual Study of North American & United Kingdom Companies*. `https://www.anomali.com/resources/whitepapers/2019-ponemon-report-the-value-of-threat-intelligence-from-anomali`. 2019.

[94] SANS Institute. *The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey*. `https://www.sans.org/reading-room/whitepapers/analyst/evolution-cyber-threat-intelligence-cti-2019-cti-survey-38790`. 2019.

[95] M. Talha, A. Abou El Kalam, and N. Elmarzouqi. "Big Data: Trade-off between Data Quality and Data Security". In: *Procedia Computer Science* 151 (2019). The 10th International Conference on Ambient Systems, Networks and Technologies (ANT 2019) / The 2nd International Conference on Emerging Data and Industry 4.0 (EDI40 2019), pp. 916–922.

[96] T. W. Phua and R. K. L. Ko. "Data Provenance for Big Data Security and Accountability". In: *Encyclopedia of Big Data Technologies*. Ed. by S. Sakr and A. Zomaya. Springer, 2018, pp. 1–6.

[97] L. Cai and Y. Zhu. "The challenges of data quality and data quality assessment in the big data era". In: *Data science journal* 14 (2015).

[98] W. She, W. Zhu, I. Yen, F. Bastani, and B. Thuraisingham. "Role-Based Integrated Access Control and Data Provenance for SOA Based Net-Centric Systems". In: *IEEE Transactions on Services Computing* 9.6 (2016), pp. 940–953.

[99] E. Bertino, A. Jabal, S. Calo, D. Verma, and C. Williams. "The Challenge of Access Control Policies Quality". In: *Journal of Data and Information Quality* 10.2 (2018).

[100] J. Wu, Z. Zhu, and S. Guo. "A Quality Model for Evaluating Encryption-as-a-Service". In: *Security, Privacy, and Anonymity in Computation, Communication, and Storage*. Ed. by G. Wang, M. Atiquzzaman, Z. Yan, and K. R. Choo. Cham: Springer International Publishing, 2017, pp. 557–569.

[101] G. Grispos, W. B. Glisson, and T. Storer. "How Good is Your Data? Investigating the Quality of Data Generated During Security Incident Response Investigations". In: *CoRR* abs/1901.03723 (2019). arXiv: `1901.03723`. URL: `http://arxiv.org/abs/1901.03723`.

[102] C. Sillaber and R. Breu. "Using Stakeholder Knowledge for Data Quality Assessment in IS Security Risk Management Processes". In: *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. SIGMIS-CPR '15. Newport Beach, California, USA: ACM, 2015, pp. 153–159.

[103] C. Sillaber, A. Mussmann, and R. Breu. "Experience: Data and Information Quality Challenges in Governance, Risk, and Compliance Management". In: *Journal of Data and Information Quality* 11.2 (2019), pp. 1–14.

[104] 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. Vienna, Austria: ACM, 2016, pp. 65–70. URL: http://doi.acm.org/10.1145/2994539.2994546.

[105] A. Mohaisen, O. Al-Ibrahim, C. Kamhoua, K. Kwiat, and L. Njilla. "Assessing Quality of Contribution in Information Sharing for Threat Intelligence". In: *Proceedings of the 2017 IEEE Symposium on Privacy-Aware Computing*. PAC. IEEE, 2017, pp. 182–183.

[106] J. Park, H. Alasmary, O. Al-Ibrahim, C. Kamhoua, K. Kwiat, L. Njilla, and A. Mohaisen. "QOI: Assessing Participation in Threat Information Sharing". In: *Proceedings of the 2018 International Conference on Acoustics, Speech and Signal Processing*. ICASSP. IEEE, 2018, pp. 6951–6955.

[107] S. Chandel, M. Yan, S. Chen, H. Jiang, and T. Ni. "Threat Intelligence Sharing Community: A Countermeasure Against Advanced Persistent Threat". In: *Proceedings of the 2019 Conference on Multimedia Information Processing and Retrieval*. MIPR. IEEE, 2019, pp. 353–359.

[108] R. Meier, C. Scherrer, D. Gugelmann, V. Lenders, and L. Vanbever. "FeedRank: A tamper- resistant method for the ranking of cyber threat intelligence feeds". In: *Proceedings of the 2018 10th International Conference on Cyber Conflict*. CyCon 2018. IEEE, 2018, pp. 321–344.

[109] L. Li, X. Li, and Y. Gao. "MTIV: A Trustworthiness Determination Approach for Threat Intelligence". In: *Security, Privacy, and Anonymity in Computation, Communication, and Storage*. Ed. by G. Wang, M. Atiquzzaman, Z. Yan, and K. R. Choo. SpaCCS 2017. Springer, 2017, pp. 5–14.

[110] T. Schaberreiter, V. Kupfersberger, K. Rantos, A. Spyros, A. Papanikolaou, C. Ilioudis, and G. Quirchmayr. "A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources". In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. ARES '19. ACM, 2019, 83:1–83:10. URL: http://doi.acm.org/10.1145/3339252.3342112.

[111] L. Qiang, J. Zhengwei, Y. Zeming, L. Baoxu, W. Xin, and Z. Yunan. "A Quality Evaluation Method of Cyber Threat Intelligence in User Perspective". In: *Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering*. IEEE, 2018, pp. 269–276.

[112] Z. Rashid, U. Noor, and J. Altmann. "Network Externalities in Cybersecurity Information Sharing Ecosystems". In: *Economics of Grids, Clouds, Systems, and Services*. Ed. by M. Coppola, E. Carlini, D. D'Agostino, J. Altmann, and J. Á. Bañares. GECON 2018. Springer, 2019, pp. 116–125.

[113] L. Liu and L. Chi. "Evolutional Data Quality: A Theory-Specific View." In: *Proceedings of the Seventh International Conference on Information Quality*. ICIQ-02. 2002, pp. 292–304.

[114] V. Venkatesh, S. Brown, and H. Bala. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems". In: *MIS Quarterly: Management Information Systems* 37 (Mar. 2013), pp. 21–54.

[115] R. B. Johnson and A. J. Onwuegbuzie. "Mixed Methods Research: A Research Paradigm Whose Time Has Come". In: *Educational Researcher* 33.7 (2004), pp. 14–26. eprint: https://doi.org/10.3102/0013189X033007014. URL: https://doi.org/10.3102/0013189X033007014.

[116] C. Teddlie and A. Tashakkori. *Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences*. Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences. SAGE Publications, 2009. URL: https://books.google.co.uk/books?id=c3uojOS7pK0C.

[117] J. W. Creswell and V. L. P. Clark. *Designing and Conducting Mixed Methods Research*. SAGE Publications, 2017.

[118] V. Garousi, M. Felderer, and M. V. Mäntylä. "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. Limerick, Ireland: ACM, 2016, 26:1–26:6. URL: http://doi.acm.org/10.1145/2915970.2916008.

[119] The Communications Security, Reliability and Interoperability Council. *Cybersecurity Information Sharing Working Group Barriers Report*. https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Info_Sharing_Report_062016.pdf. 2016.

[120] A. Fink. *Conducting research literature reviews: From the internet to paper*. Sage publications, 2019.

[121] B. Kitchenham and S. Charters. *Guidelines for performing systematic literature reviews in software engineering*. Tech. rep. Technical report, Ver. 2.3 EBSE Technical Report. EBSE, 2007.

[122] C. Wohlin. "Guidelines for snowballing in systematic literature studies and a replication in software engineering". In: *Proceedings of the 18th international conference on evaluation and assessment in software engineering*. 2014, pp. 1–10.

[123] C. Mu, M. Yu, Y. Li, and W. Zang. "Risk balance defense approach against intrusions for network server". In: *International Journal of Information Security* 13.3 (2014), pp. 255–269. URL: https://doi.org/10.1007/s10207-013-0214-9.

[124] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and Coen-Porisini. A. "Security policy enforcement for networked smart objects". In: *Computer Networks* 108 (2016), pp. 133–147. URL: http://www.sciencedirect.com/science/article/pii/S1389128616302663.

[125] T. D. Wagner, E. Palomar, K. Mahbub, and A. E. Abdallah. "Relevance Filtering for Shared Cyber Threat Intelligence (Short Paper)". In: *Information Security Practice and Experience*. Ed. by J. K. Liu and P. Samarati. Springer, 2017, pp. 576–586.

[126] P. Shamala, R. Ahmad, A. Zolait, and M. Sedek. "Integrating information quality dimensions into information security risk management (ISRM)". In: *Journal of Information Security and Applications* 36 (2017), pp. 1–10. URL: http://www.sciencedirect.com/science/article/pii/S2214212617300972.

[127] V. G. Li, M. Dunn, P. Pearce, D. McCoy, G. M. Voelker, and S. Savage. "Reading the Tea leaves: A Comparative Analysis of Threat Intelligence". In: *Proceedings of the 28th USENIX Security Symposium*. USENIX Security 19. USENIX Association, 2019, pp. 851–867. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/li.

[128] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah. "Cyber threat intelligence sharing: Survey and research directions". In: *Computers & Security* 87 (2019), p. 101589. URL: http://www.sciencedirect.com/science/article/pii/S016740481830467X.

[129] H. A. Linstone and M. Turoff. *The Delphi Method: Techniques and Applications*. Advanced Book Program. Addison-Wesley Publishing Company, Advanced Book Program, 1975.

[130] M. Lewis-Beck, A. E. Bryman, and T. F. Liao. *The SAGE Encyclopedia of Social Science Research Methods*. SAGE Publications, 2003.

[131] H. A. von der Gracht. "Consensus measurement in Delphi studies: Review and implications for future quality assurance". In: *Technological Forecasting and Social Change* 79.8 (2012), pp. 1525–1536. URL: http://www.sciencedirect.com/science/article/pii/S0040162512001023.

[132] A. L. Delbecq, A. H. Van de Ven, and D. H. Gustafson. *Group techniques for program planning: a guide to nominal group and Delphi processes*. Management applications series. Scott, Foresman, 1975.

[133] J. R. Avella. "Delphi panels: Research design, procedures, advantages, and challenges". In: *International Journal of Doctoral Studies* 11.1 (2016), pp. 305–321.

[134] D. Fink-Hafner, T. Dagen, M. Doušak, M. Novak, and M. Hafner-Fink. "Delphi Method: Strengths and Weaknesses". In: *Metodoloski zvezki* 16 (2019), pp. 1–19.

[135] C. Hsu and B. A. Sandford. "The Delphi technique: making sense of consensus". In: *Practical Assessment, Research, and Evaluation* 12.10 (2007).

[136] H. M. Donohoe and R. D. Needham. "Moving best practice forward: Delphi characteristics, advantages, potential problems, and solutions". In: *International Journal of Tourism Research* 11.5 (2009), pp. 415–437.

[137] N. Dalkey and O. Helmer. "An Experimental Application of the DELPHI Method to the Use of Experts". In: *Management Science* 9.3 (1963), pp. 458–467.

[138] J. L. Campbell, C. Quincy, J. Osserman, and O. K. Pedersen. "Coding in-depth semistructured interviews: Problems of unitization and intercoder reliability and agreement". In: *Sociological Methods & Research* 42.3 (2013), pp. 294–320.

[139] H. Donohoe, M. Stellefson, and B. Tennant. "Advantages and limitations of the e-Delphi technique". In: *American Journal of Health Education* 43.1 (2012), pp. 38–46.

[140] N. Urbach, S. Smolnik, and G. Riempp. "The State of Research on Information Systems Success". In: *Business & Information Systems Engineering: The International Journal of WIRTSCHAFTSINFORMATIK* 1.4 (2009), pp. 315–325. URL: https://ideas.repec.org/a/spr/binfse/v1y2009i4p315-325.html.

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

[142] A. Zibak and A. Simpson. "Towards Better Understanding of Cyber Security Information Sharing". In: *Proceedings of the 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*. CyberSA 2019. Oxford, UK: IEEE, 2019.

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

[144] C. Zins. "Conceptual approaches for defining data, information, and knowledge". In: *Journal of the American Society for Information Science and Technology* 58.4 (2007), pp. 479–493.

[145] D. W. De Long and L. Fahey. "Diagnosing cultural barriers to knowledge management". In: *Academy of Management Perspectives* 14.4 (2000), pp. 113–127.

[146] 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*. Washington, DC, USA, 2007.

[147] 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.

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

[149] D. M. Mertens and A. T. Wilson. *Program Evaluation Theory and Practice*. Guilford Publications, 2018.

[150] A. Zibak and A. Simpson. "Cyber Threat Information Sharing: Perceived Benefits and Barriers". In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. ARES '19. Canterbury, United Kingdom: ACM, 2019, 85:1–85:9. URL: http://doi.acm.org/10.1145/3339252.3340528.

[151] V. Mavroeidis and S. Bromander. "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. Athens, Greece: IEEE, 2017, pp. 91–98.

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

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

[154] T. Kokkonen, J. Hautamaki, J. Siltanen, and T. Hamalainen. "Model for sharing the information of cyber security situation awareness between organizations". In: *Proceedings of 23rd International Conference on Telecommunications (ICT)*. Thessaloniki, Greece: IEEE, 2016, pp. 1–5. URL: http://ieeexplore.ieee.org/document/7500406/.

[155] B. Woods, S. J. Perl, and B. Lindauer. "Data Mining for Efficient Collaborative Information Discovery". In: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*. WISCS '15. ACM, 2015, pp. 3–12. URL: http://dl.acm.org/citation.cfm?doid=2808128.2808130.

[156] S. E. Jasper. "U.S. Cyber Threat Intelligence Sharing Frameworks". In: *International Journal of Intelligence and CounterIntelligence* 30.1 (2017), pp. 53–65. URL: https://doi.org/10.1080/08850607.2016.1230701.

[157] S. Murdoch and N. Leaver. "Anonymity vs. Trust in Cyber-Security Collaboration". In: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*. WISCS '15. ACM, 2015, pp. 27–29. URL: http://dl.acm.org/citation.cfm?doid=2808128.2808134.

[158] D. Shackleford. *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_Survey_CTI-2017_LookingGlass.pdf. 2017.

[159] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou. "The impact of information sharing on cybersecurity underinvestment: A real options perspective". In: *Journal of Accounting and Public Policy* 34.5 (2015), pp. 509–519. URL: http://dx.doi.org/10.1016/j.jaccpubpol.2015.05.001.

[160] R. Garrido-Pelaz, L. González-Manzano, and S. Pastrana. "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, 2016, pp. 15–24.

[161] K. E. Eichensehr. "Public-Private Cybersecurity". In: *Texas Law Review* 95.3 (2017), pp. 467–538.

[162] ENISA. *Information Sharing and Analysis Center (ISACs) - Cooperative models*. https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models. 2018.

[163] E. H. Spafford. *Cyber Security: Assessing Our Vulnerabilities and Developing an Effective Defense*. Ed. by C. S. Gal and M. E. Kantor P. B.and Lesk. Springer Berlin Heidelberg, 2009, pp. 20–33.

[164] D. Mann, S. S. Shapiro, and D. Bodeau. "Bilateral Analysis of Information Sharing Efforts: Determining the Expected Effectiveness of Information Sharing Efforts". In: *Proceedings of the 2014 ACM Workshop on Information Sharing and Collaborative Security*. WISCS '14. Scottsdale, Arizona, USA: ACM, 2014, pp. 41–50. URL: https://doi.org/10.1145/2663876.2663880.

[165] T. D. Wagner, E. Palomar, K. Mahbub, and A. E. Abdallah. "A Novel Trust Taxonomy for Shared Cyber Threat Intelligence". In: *Security and Communication Networks* 2018 (2018). URL: https://doi.org/10.1155/2018/9634507.

[166] M. Lee and J. Lee. "The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet". In: *Information Systems Frontiers* 14.2 (2012), pp. 375–393. URL: https://doi.org/10.1007/s10796-010-9253-1.

[167] K. H. Wilson. "Sharing Securely within Government: Best Practices for Facilitating Interagency Data Science". In: *Proceedings of Data Science for Social Good*. DSSG '17. Chicago, Illinois, USA, 2017. URL: https://dssg.uchicago.edu/wp-content/uploads/2017/09/kwilly.pdf.

[168] E. Ruel, W. E. Wagner III, and B. J. Gillespie. *The Practice of Survey Research: Theory and Applications*. 2016. URL: https://methods.sagepub.com/book/the-practice-of-survey-research.

[169] G. W. Corder and D. I. Foreman. *Nonparametric Statistics: A Step-by-Step Approach*. Wiley, 2014.

[170] G. Upton and I. Cook. *A Dictionary of Statistics 3ed.* Oxford Paperback Reference. OUP Oxford, 2014. URL: https://books.google.co.uk/books?id=4WygAwAAQBAJ.

[171] M. L. McHugh. *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*. SAGE Publications, Inc., 2018.

[172] Kris Oosthoek and Christian Doerr. "Cyber Threat Intelligence: A Product Without a Process?" In: *International Journal of Intelligence and CounterIntelligence* 34.2 (2021), pp. 300–315. URL: https://doi.org/10.1080/08850607.2020.1780062.

[173] T. De Zan. *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/. 2019.

[174] V. A. Chinn, L. T. Furches, and B. A. Woodward. *Information-Sharing with the Private Sector*. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_32-38_Chinn-Furches-Woodward.pdf. 2014.

[175] R. Y. Wang. "A Product Perspective on Total Data Quality Management". In: *Communications of the ACM* 41.2 (Feb. 1998), pp. 58–65. URL: https://doi.org/10.1145/269012.269022.

[176] A. Zibak, C. Sauerwein, and A. Simpson. *Towards a Cyber Threat Intelligence Quality Model*. Under consideration by Digital Threats: Research and Practice. 2020.

[177] PROTECTIVE. *Threat Intelligence Sharing: State of the Art and Requirements*. https://protective-h2020.eu/wp-content/uploads/2017/07/PROTECTIVE-D5.1-E-0517-Threat-Intelligence-Sharing.pdf. Accessed: 2020-04-07. 2016.

[178] Joint Chiefs of Staff, United States Department of Defense. *Joint Intelligence, Joint Publication 2-0*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf. Accessed: 2020-06-10. 2013.

[179] D. J. Bianco. *The Pyramid of Pain*. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html. Accessed: 2020-06-12. 2013.

[180] CREST. *What is Cyber Threat Intelligence and how is it used?* https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf. Accessed: 2020-06-12. 2019.

[181] R. McMillan. *Definition: Threat Intelligence*. https://www.gartner.com/en/documents/2487216. Accessed: 2020-04-07. 2013.

[182] International Organization for Standardization. *ISO/IEC 25012:2008: Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model*. Dec. 2008.

[183] E. M. Hutchins, M. J. Cloppert, and R. M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains". In: *Leading Issues in Information Warfare & Security Research* 1.1 (2011), pp. 80–106.

[184] ThreatConnect. *Threat Intelligence Platforms Everything you've ever wanted to know but didn't know to ask*. https://threatconnect.com/wp-content/uploads/ThreatConnect-TIP-EBook.pdf. 2019.

[185] V. Gover, S. Ryul Jeong, and A. H. Segars. "Information systems effectiveness: The construct space and patters of application". In: *Information and Management* 31.4 (1996), pp. 177–191. URL: http://www.sciencedirect.com/science/article/pii/S0378720696010798.

[186] E. W. N. Bernroider. "IT governance for enterprise resource planning supported by the DeLone–McLean model of information systems success". In: *Information & Management* 45.5 (2008), pp. 257–269. URL: http://www.sciencedirect.com/science/article/pii/S0378720608000323.

[187] A. Molla and P. S. Licker. "E-Commerce Systems Success : an Attempt To Extend and Respecify the Delone and Maclean Model of IS Success". In: *Journal of Electronic Commerce Research* 2.4 (2001), pp. 131–141.

[188] P. B. Seddon and S. K. Yip. "An empirical evaluation of user information satisfaction (UIS) measures for use with general ledger accounting software". In: *Journal of Information Systems* 6.1 (1992), pp. 75–92.

[189] W. Choi, M. J. Rho, J. Park, K. J. Kim, Y. D. Kwon, and I. Y. Choi. "Information system success model for customer relationship management system in health promotion centers". In: *Healthcare Informatics Research* 19.2 (2013), pp. 110–120.

[190] A. Parasuraman, V. A. Zeithaml, and L. L. Berry. "Servqual: A multiple-item scale for measuring consumer perceptions of service quality". In: *Journal of Retailing* 64.1 (1988), pp. 12–40.

[191] C. W. Chen. "Impact of quality antecedents on taxpayer satisfaction with online tax-filing systems - An empirical study". In: *Information and Management* 47 (2010), pp. 308–315. URL: http://dx.doi.org/10.1016/j.im.2010.06.005.

[192] J. J. Jiang, G. Klein, and C. L. Carr. "Measuring Information System Service Quality: SERVQUAL from the Other Side". In: *MIS Quarterly* 26.2 (2002), p. 145. URL: https://www.jstor.org/stable/10.2307/4132324?origin=crossref.

[193] W. J. Doll and G. Torkzadeh. "Developing a multidimensional measure of system-use in an organizational context". In: *Information and Management* 33.4 (1998), pp. 171–185. URL: http://www.sciencedirect.com/science/article/pii/S0378720698000287.

[194] B. Ives, M. H. Olson, and J. J. Baroudi. "The measurement of user information satisfaction". In: *Communications of the ACM* 26.10 (1983), pp. 785–793.

[195] P. B. Seddon and Min-Yen Kiew. "A Partial Test and Development of Delone and Mclean's Model of IS Success". In: *Australasian Journal of Information Systems* 4.1 (1996), pp. 90–109. URL: http://journal.acs.org.au/index.php/ajis/article/view/379.

[196] K. Hornbaek. "Current practice in measuring usability: Challenges to usability studies and research". In: *International Journal of Human-Computer Studies* 64.2 (2006), pp. 79–102. URL: http://www.sciencedirect.com/science/article/pii/S1071581905001138.

[197] A. Rai, S. S. Lang, and R. B. Welker. "Assessing the validity of IS success models: An empirical test and theoretical analysis". In: *Information Systems Research* 13.1 (2002), pp. 50–69.

[198] W. W Chin. "The partial least squares approach for structural equation modeling." In: *Modern methods for business research*. Methodology for business and management. Lawrence Erlbaum Associates Publishers, 1998, pp. 295–336.

[199] J. F. Hair, M. Sarstedt, L. Hopkins, and V. G. Kuppelwieser. "Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research". In: *European Business Review* 26.2 (2014), pp. 106–121. URL: https://doi.org/10.1108/EBR-10-2013-0128.

[200] C. Fornell and F. L. Bookstein. "Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory". In: *Journal of Marketing Research* 19.4 (1982), pp. 440–452. URL: http://www.jstor.org/stable/3151718.

[201] C. M. Ringle, S. Wende, and J. Becker. *SmartPLS 3*. http://www.smartpls.com. 2015.

[202] W. Trochim and J. P. Donnelly. *The Research Methods Knowledge Base*. Cengage Learning, 2006. URL: https://books.google.co.uk/books?id=097mAAAACAAJ.

[203] D. Straub, M. Boudreau, and D. Gefen. "Validation Guidelines for IS Positivist Research". In: *Communications of the Association for Information Systems* 3 (Jan. 2004), pp. 380–427.

[204] B. R. Lewis, G. F. Templeton, and T. A. Byrd. "A methodology for construct development in MIS research". In: *European Journal of Information Systems* 14.4 (2005), pp. 388–400. URL: https://doi.org/10.1057/palgrave.ejis.3000552.

[205] D. W. Gerbing and J. C. Anderson. "An Updated Paradigm for Scale Development Incorporating Unidimensionality and Its Assessment". In: *Journal of Marketing Research* 25.2 (1988), pp. 186–192. URL: http://www.jstor.org/stable/3172650.

[206] H. F. Kaiser. "The Application of Electronic Computers to Factor Analysis". In: *Educational and Psychological Measurement* 20.1 (1960), pp. 141–151. URL: https://doi.org/10.1177/001316446002000116.

[207] R Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing. Vienna, Austria, 2013. URL: http://www.R-project.org/.

[208] D. Gefen and D. Straub. "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example". In: *Communications of the Association for Information Systems* 16 (Jan. 2005), pp. 91–109.

[209] C. M. Cassel, P. Hackl, and A. H. Westlund. "On measurement of intangible assets: A study of robustness of partial least squares". In: *Total Quality Management* 11.7 (2000), pp. 897–907.

[210] J. F. Hair, G. T. M. Hult, C. Ringle, and M. Sarstedt. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. SAGE Publications, 2016. URL: https://books.google.co.uk/books?id=JDWmCwAAQBAJ.

[211] L. J. Cronbach. "Coefficient alpha and the internal structure of tests". In: *Psychometrika* 16.3 (1951), pp. 297–334.

[212] K. Wong. "Partial least square structural equation modeling (PLS-SEM) techniques using SmartPLS". In: *Marketing Bulletin* 24 (2013), pp. 1–32.

[213] C. Fornell and D. F. Larcker. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error". In: *Journal of Marketing Research* 18.1 (1981), pp. 39–50. URL: http://www.jstor.org/stable/3151312.

[214] J. Henseler, C. M. Ringle, and R. R. Sinkovics. "The use of partial least squares path modeling in international marketing". In: *New Challenges to International Marketing*. Ed. by R. R. Sinkovics and P. N. Ghauri. Vol. 20. Advances in International Marketing. Emerald Group Publishing Limited, 2009, pp. 277–319. URL: https://doi.org/10.1108/S1474-7979(2009)0000020014.

[215] J. F. Hair, M. Sarstedt, T. M. Pieper, and C. M. Ringle. "The Use of Partial Least Squares Structural Equation Modeling in Strategic Management Research: A Review of Past Practices and Recommendations for Future Applications". In: *Long Range Planning* 45.5 (2012), pp. 320–340. URL: http://www.sciencedirect.com/science/article/pii/S0024630112000568.

[216] J. Cohen, P. Cohen, S. West, and L. Aiken. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*. Routledge, 2003.

[217] I. Ghozali. *Structural equation modeling: metode alternatif dengan partial least square (PLS)*. Badan Penerbit Universitas Diponegoro, 2008. URL: https://books.google.com.eg/books?id=x1ZAngAACAAJ.

[218] L. Hu and P. Bentler. "Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification". In: *Psychological Methods* 3 (1998), pp. 424–453.

[219] T. Dijkstra and J. Henseler. "Consistent Partial Least Squares Path Modeling". In: *MIS Quarterly* 39 (June 2015), pp. 297–316.

[220] J. M. Choe. “The Relationships among Performance of Accounting Information Systems, Influence Factors, and Evolution Level of Information Systems”. In: *Journal of Management Information Systems* 12.4 (1996), pp. 215–239.

[221] L. A. Halawi, R. V. McCarthy, and J. E. Aronson. “An Empirical Investigation of Knowledge Management Systems’ Success”. In: *Journal of Computer Information Systems* 48.2 (2008), pp. 121–135.

[222] J. Iivari. “An Empirical Test of the DeLone-McLean Model of Information System Success”. In: *ACM SIGMIS Database* 36 (June 2005), pp. 8–27.

# Appendices

# A
# Questionnaire 1

**Q1. Which of these best describe your organisation's primary activity?**

☐ Manufacturing ☐ Utilities
☐ Construction ☐ Retail/wholesale
☐ Food/hospitality ☐ Transportation/storage
☐ Finance/insurance ☐ Information/communication
☐ Real estate ☐ Professional/scientific/technical
☐ Administration ☐ Public Sector/defence
☐ Education ☐ Health/social care
☐ Entertainment ☐ Other service activities

**Q2. Which of these best represents the number of employees working in your organisation?**

☐ <50 ☐ 50–249
☐ 250-1000 ☐ > 1000

**Q3. How many years of professional experience do you have in cyber security?**

☐ <2 years ☐ 2–5 years ☐ > 5 years

**Q4. For how long has your organisation been sending and/or receiving cyber security information?**

☐ <1 year ☐ 1–2 years
☐ 2–5 years ☐ >5 years

**Q5. What is your understanding of the term *cyber security information sharing*?**

**Q6. Please describe your organisation's information sharing efforts.**

**Q7. How would you characterise the maturity level of your organisation's information sharing efforts?**

☐ Fully mature ☐ Maturing ☐ Immature

**Q8. Does your organisation have methods in place to assess the effectiveness of its cyber security information sharing efforts?**

☐ Yes, we have established formal methods
☐ Yes, we have established informal methods

☐ No, but we are in the process of establishing methods
☐ No, but we plan to establish methods within the next 12 months
☐ No, but we are interested in establishing methods
☐ No, and we do not have plans or interest in establishing methods

**Q9. How useful do you find the following forms of information sharing?**

| | Not useful | Slightly useful | Neutral | Somewhat useful | Very useful |
|---|---|---|---|---|---|
| Threat-centric data | ☐ | ☐ | ☐ | ☐ | ☐ |
| Triggers for action | ☐ | ☐ | ☐ | ☐ | ☐ |
| Knowledge | ☐ | ☐ | ☐ | ☐ | ☐ |
| Expertise | ☐ | ☐ | ☐ | ☐ | ☐ |

**Q10. How willing is your organisation to share each of the following?**

| | Not willing | Slightly willing | Neutral | Somewhat willing | Very willing |
|---|---|---|---|---|---|
| Threat-centric data | ☐ | ☐ | ☐ | ☐ | ☐ |
| Triggers for action | ☐ | ☐ | ☐ | ☐ | ☐ |
| Knowledge | ☐ | ☐ | ☐ | ☐ | ☐ |
| Expertise | ☐ | ☐ | ☐ | ☐ | ☐ |

**Q11. How often does your organisation share each of the following?**

| | Never | Rarely | Sometimes | Often | Always |
|---|---|---|---|---|---|
| Threat-centric data | ☐ | ☐ | ☐ | ☐ | ☐ |
| Triggers for action | ☐ | ☐ | ☐ | ☐ | ☐ |
| Knowledge | ☐ | ☐ | ☐ | ☐ | ☐ |
| Expertise | ☐ | ☐ | ☐ | ☐ | ☐ |

**Q12. How difficult is it to determine the *quality* of each of the following?**

| | Very difficult | Slightly difficult | Neutral | Somewhat easy | Very easy |
|---|---|---|---|---|---|
| Threat-centric data | ☐ | ☐ | ☐ | ☐ | ☐ |
| Triggers for action | ☐ | ☐ | ☐ | ☐ | ☐ |
| Knowledge | ☐ | ☐ | ☐ | ☐ | ☐ |
| Expertise | ☐ | ☐ | ☐ | ☐ | ☐ |

**Q13. How difficult is it to determine the *effectiveness* of each of the following?**

| | Very difficult | Slightly difficult | Neutral | Somewhat easy | Very easy |
|---|---|---|---|---|---|
| Threat-centric data | ☐ | ☐ | ☐ | ☐ | ☐ |
| Triggers for action | ☐ | ☐ | ☐ | ☐ | ☐ |
| Knowledge | ☐ | ☐ | ☐ | ☐ | ☐ |
| Expertise | ☐ | ☐ | ☐ | ☐ | ☐ |

# B
# Questionnaire 2

**Q1. Which of these best describe your organisation's primary activity?**
☐ Manufacturing ☐ Utilities
☐ Construction ☐ Retail/wholesale
☐ Food/hospitality ☐ Transportation/storage
☐ Finance/insurance ☐ Information/communication
☐ Real estate ☐ Professional/scientific/technical
☐ Administration ☐ Public Sector/defence
☐ Education ☐ Health/social care
☐ Entertainment ☐ Other service activities

**Q2. Which of these best represents the number of employees working in your organisation?**
☐ <50 ☐ 50–249
☐ 250–1000 ☐ > 1000

**Q3. What is your current position at the organisation?**

**Q4. How many years of professional experience do you have in cyber security?**
☐ <2 years ☐ 2–5 years ☐ > 5 years

**Q5. How many years of professional experience do you have in threat intelligence?**
☐ <2 years ☐ 2–5 years ☐ > 5 years

**Q6. Are you currently involved in threat intelligence sharing?**
☐ Yes ☐ No

**Q7. How strongly do you agree or disagree with the following statements?**
**1 (strongly disagree) to 7 (strongly agree).**
**S01** Threat actors are deterred by TIS among organisations
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S02** TIS supports incident response efforts
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S03** TIS contributes to breach detection and recovery
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S04** TIS reduces duplicate information handling

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S05** TIS strengthens and expands professional networks
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S06** TIS validates and complements other sources of intelligence
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S07** TIS improves overall security posture and situational awareness
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S08** TIS enhances defensive agility and resilience
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S09** TIS helps in combating cyber security skills shortages
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S10** TIS reduces overall cyber security costs
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S11** TIS lowers cyber insurance premiums
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S12** TIS reduces uncertainty surrounding security investment decisions
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S13** TIS strengthens relationship with government agencies
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S14** TIS offers organisations liability protection
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

**Q8. How strongly do you agree or disagree with the following statements? 1 (strongly disagree) to 7 (strongly agree).**
**S15** Standardisation issues continue to hinder TIS
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S16** Inconsistent definitions and terminology undermine efficient TIS
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S17** It is difficult to determine the overall quality of TIS
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S18** It is difficult to ensure the timeliness of TIS
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S19** Achieving interoperability and automation of TIS is difficult
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S20** TIS results in redundant and irrelevant data
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S21** There is a shortage of skilled analysts to handle TIS
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S22** It is difficult to trust the other participants in TIS efforts
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S23** Free riding will impede TIS efforts
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S24** Setting up TIS infrastructure is expensive and resource draining
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S25** TIS erodes clients' confidence
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S26** Government over-classification undermine effective TIS
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S27** Privacy and antitrust legal concerns impede TIS
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
**S28** Inconsistent legal frameworks undermines cross-border TIS
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

# C
# Questionnaire 3

**Q1. Which of the following describes your organisation's cyber threat intelligence activities?**
☐ We only produce cyber threat intelligence
☐ We only consume cyber threat intelligence
☐ We produce and consume cyber threat intelligence

**Q2. The quality of cyber threat data (e.g. indicators of compromise) must be evaluated against the following dimensions:**
Accuracy (i.e. exact and correct)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Actionability (i.e. allows decision making)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Interoperability (i.e. formats compatible with internal systems)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Provenance (i.e. ability to track sources and processes)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Relevance (i.e. tailored to the organisation's requirements)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Source reliability (i.e. trusted and legitimate source)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Timeliness (i.e. available without delay)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree

**Q3. The quality of cyber threat intelligence (e.g. analytical reports, threat assessments) must be evaluated against the following dimensions:**
Accuracy (i.e. exact and correct)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Actionability (i.e. allows decision making)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Interoperability (i.e. formats compatible with internal systems)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Provenance (i.e. ability to track sources and processes)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Relevance (i.e. tailored to the organisation's requirements)

☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Source reliability (i.e. trusted and legitimate source)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree
Timeliness (i.e. available without delay)
☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree

**Q4. Which of the following dimensions are the most important to you as you evaluate the quality of cyber threat data (e.g. indicators of compromise)? (1 is the most important and 7 is the least important)**

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Accuracy | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Actionability | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Interoperability | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Provenance | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Relevance | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Source reliability | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Timeliness | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

**Q5. Which of the following dimensions are the most important to you as you evaluate the quality of cyber threat intelligence (e.g. analytical reports, threat assessments)? (1 is the most important and 7 is the least important)**

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Accuracy | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Actionability | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Interoperability | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Provenance | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Relevance | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Source reliability | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Timeliness | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

# D

# Questionnaire 4

**Q1. Which of these best describe your organisation's primary activity?**

☐ Manufacturing ☐ Utilities
☐ Construction ☐ Retail/wholesale
☐ Food/hospitality ☐ Transportation/storage
☐ Finance/insurance ☐ Information/communication
☐ Real estate ☐ Professional/scientific/technical
☐ Administration ☐ Public Sector/defence
☐ Education ☐ Health/social care
☐ Entertainment ☐ Other service activities

**Q2. Which of these best represents the number of employees working in your organisation?**

☐ <50 ☐ 50–249
☐ 250–1000 ☐ > 1000

**Q3. What is your current position at the organisation?**

**Q4. How many years of professional experience do you have in threat intelligence?**

☐ <2 years ☐ 2–5 years ☐ > 5 years

**Q5. Please assess the *content quality* of your organisation's threat intelligence management platform. 1 (strongly disagree) to 7 (strongly agree).**

The platform's content is accurate
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform's content is actionable
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform's content is relevant
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform's content is reliable
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform's content is timely
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The process through which the platform's content was produced is traceable
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

**Q6. Please assess the *system quality* of your organisation's threat intelligence management platform. 1 (strongly disagree) to 7 (strongly agree).**
The platform is easy to use and navigate
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform is reliable
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform offers appropriate functionality
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform is interoperable with other systems or tools
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

**Q7. Please assess the *service quality* of the vendor responsible for the support of your organisation's threat intelligence management platform. 1 (strongly disagree) to 7 (strongly agree).**
The vendor is willing to help whenever I need support with the platform
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The vendor provides personal attention when I experience problems with the platform
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The vendor provides services related to the platform at the promised time
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The vendor has sufficient knowledge to answer my questions regarding the platform
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

**Q8. Please assess the your *trust* in the organisation's threat intelligence management platform. 1 (strongly disagree) to 7 (strongly agree).**
The platform is compliant with applicable data protection and privacy regulations
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform is secure and safe to use
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
Overall, I trust the platform
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

**Q9. To what extent you agree or disagree with the following statements regarding the *use* of your organisation's threat intelligence management platform? 1 (strongly disagree) to 7 (strongly agree).**
I use the platform to receive and collect threat data or intelligence
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
I use the platform to enrich and analyse the collected threat data or intelligence
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
I use the platform to disseminate threat data or intelligence to relevant tools or stakeholders
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

**Q10. Please assess your *satisfaction* with your organisation's threat intelligence management platform. 1 (strongly disagree) to 7 (strongly agree).**
The platform adequately supports my area of work and responsibility
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform is efficient
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform is effective
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
I am satisfied with the platform as a whole
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

**Q11. To what extent you agree or disagree with the following statements regarding the *benefits* of your organisation's threat intelligence management platform? 1 (strongly disagree) to 7 (strongly agree).**

The platform contributes to breach detection and recovery
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform supports incident response efforts
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform enhances defensive agility and resilience
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform complements other sources of intelligence
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
The platform improves overall security posture and situational awareness
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7