Communications of the Association for Information Systems

Volume 50 Article 2

3-10-2022

Exploring Incentives and Challenges for Cybersecurity Intelligence Sharing (CIS) across Organizations: A Systematic Review

Farzan Kolini
The University of Auckland, f.kolini@auckland.ac.nz

Lech J. Janczewski
The University of Auckland, lech@auckland.ac.nz

Recommended Citation

Kolini, F., & Janczewski, L. J. (2022). Exploring Incentives and Challenges for Cybersecurity Intelligence Sharing (CIS) across Organizations: A Systematic Review. Communications of the Association for Information Systems, 50, pp-pp. https://doi.org/10.17705/1CAIS.05004

Communications of the Association for Information Systems

Research Article DOI: 10.17705/1CAIS.05004 ISSN: 1529-3181

Exploring Incentives and Challenges for Cybersecurity Intelligence Sharing (CIS) across Organizations: A Systematic Review

Farzan Kolini
Department of Information Systems and Operation Management (ISOM)
The University of Auckland
f.kolini@auckland.ac.nz

Lech Janczewski
Department of Information Systems and Operation Management (ISOM)
The University of Auckland
l.janczewski@auckland.ac.nz

Abstract:

Cybersecurity intelligence sharing (CIS) has gained significance as an organizational function to protect critical information assets, manage cybersecurity risks, and improve cybersecurity operations. However, few studies have synthesized accumulated scholarly knowledge on CIS practices across disciplines. Synthesizing the pertinent literature through a structured literature review, we investigated the incentives and challenges that influence organizations around adopting CIS practices. We used the overarching TOE framework to categorize these factors and propose a theoretical framework to establish common ground for future studies. We also developed a holistic and inclusive definition for cybersecurity intelligence that we present in the paper. We found 46 papers on CIS in different disciplines and analyzed them to answer our research questions. We identified 35 factors that we classified according to the TOE framework. With this paper, we facilitate further theory development by overviewing theories that researchers can use as a basis for CIS studies, suggesting future directions, providing a reference source, and developing a reference CIS framework for IS scholars.

Keywords: Cybersecurity, Intelligence Sharing, Threat Intelligence, TOE Framework, Information Sharing, Theoretical model, Systematic Review, Cross-discipline.

This manuscript underwent peer review. It was received 5/04/2020 and was with the authors for 12 months for three revisions. Thapa Devinder served as Associate Editor.

1 Introduction

The digital era has created unprecedented opportunities for enterprises to deliver services via the internet and online platforms. As of December, 2018, the Internet has over 4.1 billion users, 1.9 billion websites, and 67,000 gigabytes (GB) of traffic per second (Internet Live Stats, 2018). However, in recent times, the Internet has also become a minefield due to cyberattacks, personal and classified information breaches, cyber harassment, and cyber espionage on a large scale (Kolini & Janczewski, 2015). According to Alvarez et al. (2018), around 2.9 billion records from publicly disclosed information were breached or leaked in 2017. Alvarez et al. (2018) estimated ransomware attacks alone to cost organizations more than US$8 billion annually (Alvarez et al., 2018).

Due to the high number of security threats and vulnerabilities, organizations have found it increasingly impossible to protect their critical information assets and respond to cybersecurity vulnerabilities without leveraging collaboration from industry peers (NIST, 2014). Cyber attackers also exhibit more persistence, motivation, and collaboration than in the past. They also benefit from sharing novel tactics, techniques, and procedures (TTPs) to reduce the costs associated with conducting cyberattacks (Gal-Or & Ghose, 2005; Hausken, 2007). Hence, organizations need to participate in cybersecurity intelligence sharing (CIS) processes in order to receive timely and accurate cybersecurity intelligence and effectively respond to cybersecurity threats (Appan & Bacic, 2016; Greiman, 2015; Hernandez-Ardieta et al., 2013).

In short, CIS refers to sharing analyzed and contextualized cybersecurity intelligence so that organizations can make informed decisions about cybersecurity incidents, cyberattacks, cybersecurity operations, risks, and mitigating controls. Organizations primarily participate in CIS to develop a broader situational awareness towards protecting critical assets and responding quickly to large-scale cyberattacks. CIS also helps organizations prioritize their defense capabilities to shield their most vulnerable critical assets (Jasper, 2017).

Organizations can receive cybersecurity intelligence from different sources, such as partners, suppliers, governments, computer emergency response teams (CERTs), industry alliances, and commercial and open-source platforms. These sources generate cybersecurity intelligence in both human and machine-readable formats to facilitate automation and integration with other systems (Chismon & Ruks, 2015). Receiving reliable cybersecurity intelligence at the right time can empower decision makers to reduce risk, prepare timely incident responses, and enhance technological resiliency (Goodwin et al., 2015).

Organizations, governments, and policymakers have started to pay more attention to cybersecurity intelligence sharing (CIS) practices. However, these actors do not adequately practice nor understand how to actively generate cyber intelligence and share it with other parties (Goodwin et al., 2015). For instance, between 2015 and 2016, various cyberattacks against financial messaging systems such as SWIFT payment networks resulted in attackers stealing millions of dollars (Verizon, 2017). The financial institutions that this attack targeted either ignored or failed to share cybersecurity intelligence with their peers in other banks. Inadequate cybersecurity intelligence sharing allowed the attackers to replicate the same approach to compromise other banks using SWIFT systems. Thus, the unsuccessful collaboration across organizations in sharing cybersecurity intelligence led to hundreds of millions of dollars in losses and substantial reputational damage to financial service institutions (FSIs). However, studies show that one cannot easily define what constitutes cybersecurity intelligence (Dalziel, 2014) and identify the factors that determine whether organizations participate in CIS (Skopik et al., 2016). Researchers in the cyber domain have not holistically investigated this area to identify the incentives and challenges that influence organizations in relation to adopting cybersecurity intelligence operations or participating in CIS partnerships (Kolini & Janczewski, 2017; Tounsi & Rais, 2018). Indeed, research in this area remains scarce, and we require more (particularly empirical) studies that investigate CIS operations from different theoretical traditions.

Accordingly, in this paper, we explore the current state of CIS in the organizational context according to the existing literature and to identify incentives and challenges that respectively promote or undermine active participation in CIS. Although it may seem intuitive to reduce CIS to technical capabilities for supporting the “on-the-network fight”, one needs to thoroughly analyze non-technical elements and their synthesis with technical capabilities to better understand how CIS practices form and evolve. Therefore, in this study, we categorize influential factors from the technology, organization, and environment contexts (the TOE framework). We also contribute to the cybersecurity literature by deconstructing and defining cybersecurity intelligence (CI) to provide a richer context based on the notion’s characteristics and boundaries. Further, we propose a theoretical framework for CIS practices from the factors that we

identified in the literature review and perform a high-level analysis of well-known theories that future studies could use. Accordingly, the following research questions guide our research:

RQ1: What constitutes cybersecurity intelligence (CI)?

RQ2: What incentives and challenges influence organization's participation in CIS?

RQ3: What theories can one use to investigate organizations' participation in CIS?

This paper proceeds as follows: in Section 2, we present the theoretical framework that we used in this study. In Section 3, we present our research methodology. In Section 4, we review the literature on CIS, the cybersecurity intelligence concept, and research perspectives on theory, methods, and focus. In Section 5, based on the findings from studying the literature, we then classify the incentives and challenges for CIS practice according to the TOE framework. We also include potential theories that researchers could use. In Section 6, we discuss the study's implications for research and practice, outline opportunities for future studies and consider the study limitations as avenues for future research. Finally, in Section 7, we conclude the paper.

2 Theoretical Foundation: The Technology, Organization, Environment (TOE) Framework

Sharing sensitive and confidential cybersecurity intelligence constitutes a complex and challenging task for many organizations due to the technological, organizational, institutional, and social challenges it involves. Among the many CIS risks include privacy breaches, sensitive corporate information disclosures, reputational and brand damage, or financial losses (Kolini & Janczewski, 2017). We selected the TOE framework, an extension of the socio-technical framework, to provide a basis to understand how technological, organizational, and environmental factors influence participation in CIS practices across organizations. The TOE framework reflects the assumption that adopting new technologies concerns more than technical matters and that one should investigate should investigation such adoption in the broader organizational and social context in which they are embedded (Carter, 2015; Chen et al., 2004; Li et al., 2016). Moreover, the TOE framework has its roots in the innovation-adoption process at the firm level (Tornatzky et al., 1990). In this study, we view CIS as an organizational and technological innovation. Hence, to share cybersecurity intelligence, organizations may need to adopt new technologies (i.e., tools or platforms), organizational processes (i.e., participation in a CIS network), or new ways of thinking (i.e., governance of CIS network) (Akbulut-Bailey, 2011; Salleh & Janczewski, 2016). IS scholars have widely accepted and used the TOE framework in relation to electronic information sharing[1] (Furneaux & Wade, 2011; Gil-Garcia et al., 2010).

Researchers have also applied the TOE framework in the cybersecurity domain. For example, Skopik et al. (2016) applied five socio-technical dimensions to investigate intelligence sharing across organizations. In other studies, Salleh and Janczewski (2016) used the TOE framework to investigate the influence that security determinants had on whether organizations adopted big data, while Van Deursen et al. (2013) applied a socio-technical approach to categorize information security risks in the healthcare industry. Hence, we draw on the TOE framework as the basis for categorizing factors that may influence organizations around entering into CIS practices.

In the TOE framework, the technological context refers to infrastructure, tools, and technical elements that an organization needs to generate, consume, and share cybersecurity intelligence. Organizations should adopt fit-for-purpose cybersecurity intelligence-driven technologies that work with existing systems and internal processes to maximize their benefits from cybersecurity intelligence. The organizational context refers to an organization's internal and external characteristics, such as management support, strategies, culture, size, operational costs, and human resource quality (Chau & Tam, 1997; Kelly et al., 1999; Tornatzky et al., 1990; Zhu & Kraemer, 2005). Finally, the environmental context concerns the characteristics of the external environment in which organizations operate. Previous studies in the cybersecurity domain have shown organizations cannot ignore the influence that the institutional

[1] The term information sharing is a general concept that relates to sharing any type of information, which includes cybersecurity intelligence. In contrast, cybersecurity intelligence sharing more specifically focuses on sharing information about cyberattacks, incidents, or indicators of security compromises. We do not use these terms interchangeably in this review paper. We explore the differences between cybersecurity information and cybersecurity intelligence sharing in Section 4.1.

landscape and regulatory regimes have on cyber security practices (Choucri et al., 2014; Skopik et al., 2016).

In contrast to other popular theories, the TOE framework does not posit causal relationships between the influential factors that its dimensions identify (Mishra et al., 2007). Instead, it offers a broader range of factors that one can invoke to contextually classify phenomena under investigation (Orlikowski & Iacono, 2001).To better present this study's outcomes, we define two subcategories in the organizational context in the TOE framework: intra-organizational and inter-organizational. Yang and Maxwell (2011) followed the same approach in reviewing information sharing in a public organization. The intra-organizational category represents a firm's characteristics and readiness for adopting CIS practices to produce or consume cybersecurity intelligence for security operations. The inter-organizational category comprises external characteristics that may influence a firm's willingness to share or receive cybersecurity intelligence from other organizations. These inter-organizational characteristics may arise from interactions with other organizations. We perceive that a firm's intra-organizational and inter-organizational characteristics have equal importance in relation to entering or contributing to CIS operations. Figure 1 demonstrates the theoretical framework for this study and decomposes the TOE framework to show factors that influence CIS across organizations.

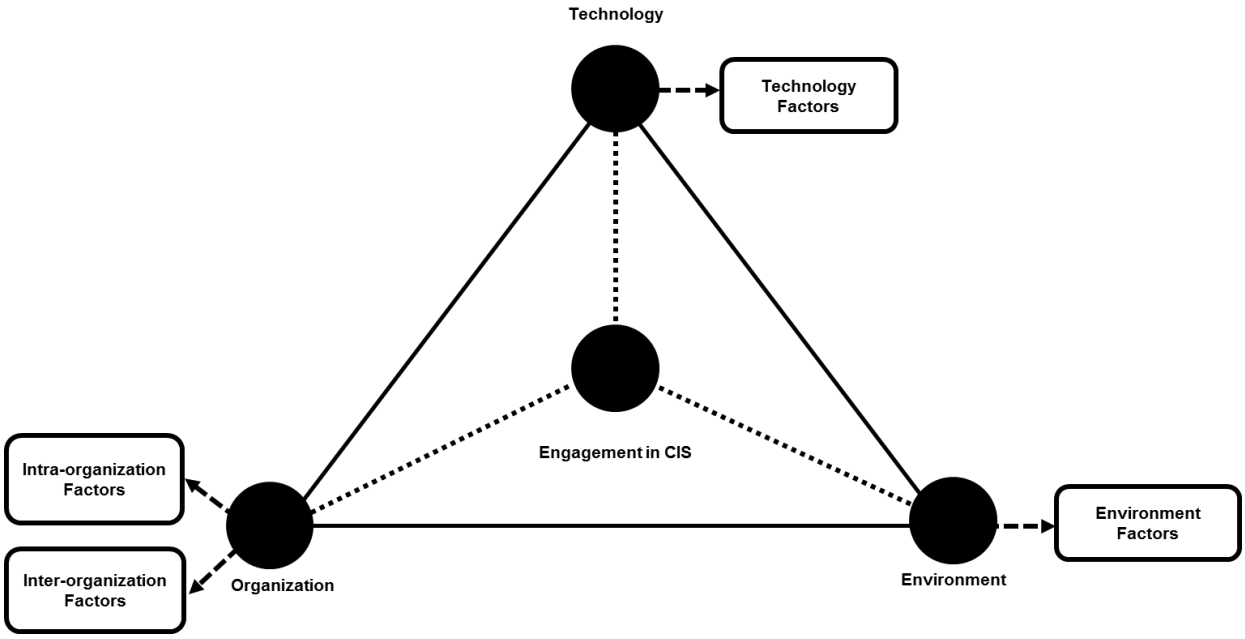

Figure 1. Proposed Framework for CIS

3 Research Methodology

In a literature review, one critically summarizes and assesses "the range of existing material dealing with knowledge and understanding in a given research domain" (Blaxter, 2010, p. 123). Literature reviews can take different forms, such as narrative reviews, scoping reviews, meta-analytical reviews, descriptive reviews, and critical reviews (Paré et al., 2015). We conducted a descriptive review to illustrate whether the existing literature supports pre-existing propositions and findings in order to identify any interpretable trends or patterns associated with a phenomenon (Grant & Booth, 2009; King & He, 2005, Paré et al., 2015).

We used the descriptive literature review approach for several reasons. First, while an increasing number of studies have investigated CIS in recent years, the CIS domain has attracted relatively little empirical research. Thus, by conducting a descriptive review, we could illuminate to what extent the existing literature applies theoretical lenses or supports propositions. Second, CIS studies draw on various disciplines such as information systems, computer science, information security, organization and management science, and law (Sommer & Brown, 2011). As a result, many researchers whose efforts benefit the CIS domain may not know about contributions in other disciplines. As such, a descriptive review provides a broader view across the various disciplines and can synthesize the trends and patterns

that have emerged from CIS studies in these different disciplines. Finally, a descriptive review provides a logical structure and robust approach for searching, filtering, interpreting, and classifying the existing literature (King & He, 2005; Paré et al., 2015).

Although we focus on exploring and synthesizing the CIS literature from the information systems and computer science perspective, we also consider other relevant disciplines to comprehensively overview CIS research. Hence, we conducted several detailed and systematic searches for related literature from different disciplines to create a master repository that contained all relevant papers. We treated each paper as a record in our master literature database and as the unit of analysis for this study. We comprehensively reviewed all selected papers to identify factors, patterns, and trends relevant to the existing concepts, propositions, and findings that make up CIS (Mathiassen et al., 2007; Webster & Watson, 2002). We selected relevant papers following the process that Webster and Watson (2002) discuss extensively. We also adopted the approaches that Templier and Paré (2015) and Mathiassen et al. (2007) describe and followed their recommendations in a three-step procedure (see Figure 2).

3.1 Step 1: Keywords Search and Analysis in Scholarly Databases

In order to fully cover existing CIS literature, in the first step, we conducted literature searches using three scholarly databases. Shea et al. (2007) suggest that researchers should use at least two complementary databases to ensure that they identify as much relevant research as possible. We chose three scholarly databases that previous studies have used or recommended: Web of Science, Scopus and ABI/Inform (ProQuest) (Templier & Paré, 2015; Webster & Watson, 2002). These citation databases provide access to abstracts of scientific peer-reviewed journal papers and conference proceedings from 1990 until present. Their comprehensive subject search engines allow scholars to identify relevant research across the social science, technical, and organizational disciplines. In this step, we tended to use relatively broad keywords to identify an extensive paper list. We used keywords from a list [2] in different combinations, such as “cybersecurity”, “intelligence sharing”, and “threat sharing”, to identify papers with a focus on cybersecurity intelligence. As a result, we identified 692 papers in English from both peer-reviewed journals and conference proceedings. The papers spanned eight years from 2010 to 2018.

Nevertheless, our initial analysis indicated that many of these papers lacked relevance due to the broader keywords that we used during the search phase. Next, we followed a screening and filtering approach to exclude duplicates and irrelevant papers by reviewing their title, keywords, abstract, and conclusion (Paré et al., 2015; Templier & Paré, 2015). In the screening process, we looked for papers that focused on cybersecurity domain and that considered information sharing. As a result, we retained only 133 papers for the next our analysis round.

Next, we analyzed each paper’s text in more detail to exclude papers that did not address CIS as their main topic or that did not consider efforts to implement or adopt CIS practices. In this process, we examined each paper extensively and asked ourselves whether we could use the paper to help answer our research questions (e.g., about incentives and challenges in adopting CIS practices) (Pawson et al., 2005; Webster & Watson, 2002). We also scrutinized the papers in relation to their research method, unit of analysis, and research questions to exclude unrelated papers that presented the same findings or results. For example, we excluded papers about sharing cyber information between individuals or communities since we focus on the organizational context. We documented, discussed, and agreed on reasons for inclusion and exclusion to ensure we selected reliable and valid papers in this stage. As a result, we identified 32 relevant papers from all the papers that we initially recorded in our master literature database.

3.2 Step 2: Complementary Search and Assessment

In the second step, we followed a systematic approach to identify additional papers that we did not identify in initially searching the three scholarly databases. Since researchers consider both cybersecurity and information systems (IS) cross-disciplinary fields, one can expect journals from other disciplines to have published work on CIS as well. Malone and Crowston (1994) suggest a study area will have reached maturity when scholars from different disciplines know about one another’s contributions. Hence, to identify relevant papers from other pertinent disciplines (e.g., computer science, management, and

[2] We used the following search terms and the search strategy: (“information sharing” OR “information-sharing” OR “information exchange” OR “intelligence sharing” OR “threat intelligence sharing” OR “threat sharing” OR “security information sharing”) AND (“cybersecurity” OR “cyber security” OR “cyber-security” OR “information security” OR “cyber” OR “security”).

organization science), we followed the same methodology that Chavarria et al. (2016) and Pink and Bascand (2008) describe. As such, we used the field of research (FOR) classification from the Australian and New Zealand Research Classification (ANZRC) to identify research disciplines that could have some relevance to our research domains (Chavarria et al., 2016; Pink & Bascand, 2008). Following Chavarria et al. (2016), we considered disciplines relating to information systems (including computer science and information security) and business and management (including organizational and public relations science) (Fielt et al., 2014; Zhang et al., 2009). Subsequently, we mapped these disciplines against the Australian Business Deans Council (ABDC) journal quality list (O'Neil, 2019) to identify journals relevant to the above-mentioned disciplines[3]. We then narrowed our focus to the top three tiers of journals (A*, A, and B) from the ABDC journal quality list and mapped them against the journal titles that scholarly databases indexed. As a result, we identified 53 top-tier journals (see Appendix A for the full list).

Next, we repeated the keyword searches and screened and analyzed the 53 newly identified journals in depth. However, in our keyword search and filtering analysis, we found that many of these journals either did not focus on the cybersecurity domain or lacked relevance to the CIS literature. As such, from our screening and full-text analysis, we found only two further papers relevant to this study.

In this step, we also considered peer-reviewed conference proceedings since papers in such proceedings can present new ideas, models, or theories (Webster & Watson, 2002). Here, we followed the same approach that previous studies (Bandara et al., 2015; Franke & Brynielsson, 2014) used to search for CIS-related conference papers in conference proceedings that the Association for Information System (AIS), Association for Computing Machinery (ACM), and Institute of Electrical and Electronics Engineers (IEEE) publish. Aware that the three scholarly databases index many such conference publications, we applied a screening process to exclude duplicate papers and identified only three new papers for inclusion in this study.

3.3 Step 3: Backward Reference Search

Finally, in in the third step, we performed a backward search: that is, we searched the reference list in (Jafarzadeh et al., 2015) in each paper we selected in the first two steps to collect further papers that we did not find in the previous steps. We also screened the practitioner-oriented publications that the references cited. Individuals, organizations, and government agencies seeking information and advice on how to address obstacles related to cybersecurity operations widely consult these practitioner outlets. In fact, practitioners have contributed significantly to the cybersecurity domain with novel frameworks, technical standards, and conceptual models to improve overall cybersecurity practices (Siponen, 2000; Willison & Siponen, 2007). Although many practitioner-oriented publications that we identified did not follow a robust scientific approach, excluding them from our analysis would have compromised how we understood the incentives and challenges that influence CIS practices across organizations. From our analysis in this step, we selected nine further papers relevant to CIS practices. In total, we identified 46 papers for inclusion in our review across all three steps.

3.4 Evaluation of Literature Review Procedures

We employed several strategies to minimize bias and errors in the review process, such as carefully documenting the review procedures and defining the study's boundaries. As we describe above, we discussed, documented, and agreed on a detailed procedure for searching the literature. We also explicitly articulated how we defined cybersecurity intelligence (see Section 4) to better delineate the study's boundaries. Second, to cover all relevant literature streams related to our keywords, we applied our searches across selected scholarly databases and top-tier journals from related disciplines and used backwards reference checks (Kitchenham & Charters, 2007). Third, to avoid publication bias (Templier & Paré, 2015), we included conference publications and performed reference checks to include non-academic practitioner-oriented outlets in the study's scope. Fourth, we discussed and agreed on the inclusion and exclusion criteria. We agreed that we should consider any paper that helped answer our research questions for analysis and investigation (Pawson et al., 2005).

[3] In Appendix A, we provide the internet hyperlink to the Australian Bureau of Statistics webpage, which provides further details about the Australian and New Zealand Standard Research Classification framework.

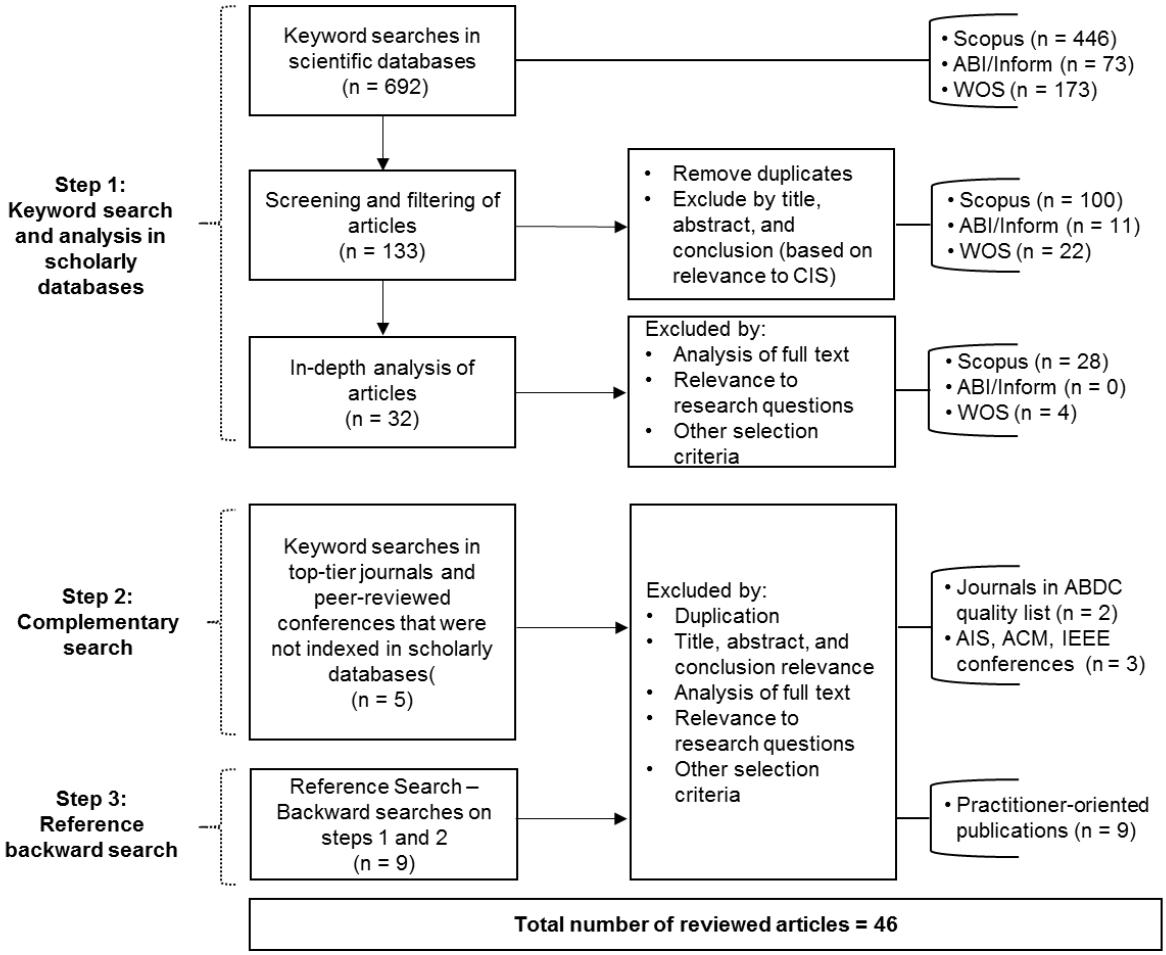

Figure 2. Literature Selection Overview

4 CIS in the Literature

In this section, we examine CIS in more detail based on the 46 selected papers. However, before we analyze the relevant extant literature, we first clarify how we understand the cybersecurity intelligence concept. By deconstructing the concept, we address our first research question and clarify the CIS building blocks that we targeted in our literature search strategy. Hence, in Section 4.1, we demonstrate the cybersecurity intelligence notion and discuss its facets by shedding more light on the activities and information types and sources that CIS operations require.

In Section 4.2, we adopt a concept matrix approach to the literature as Webster and Watson (2002) suggest when designing a descriptive review. Concepts constitute a structured literature review's building blocks. One generates concepts by synthesizing, categorizing, and reviewing the themes that one identifies in research papers (Webster & Watson, 2002). We used a combination author-centric and concept-centric matrix to investigate each paper's focus, method, theoretical perspective, unit of analysis, and research objectives. Appendix B summarizes this analysis for the 46 papers we reviewed for this study. In Section 5, we address incentives and challenges that may influence whether organizations adopt CIS. We coded, classified, and checked all the papers until we reached full agreement. Next, we present the key findings from our analysis and pinpoint areas that may need more attention from cybersecurity researchers.

4.1 Deconstructing CIS

We needed to initially deconstruct the CIS concept before reviewing previous studies to advance how we understand CIS and develop a cumulative body of knowledge. We argue that the key problem with defining CIS concerns its reliance on cybersecurity intelligence (CI) that organizations can generate,

transmit, and use. Some studies used the term cybersecurity intelligence interchangeably with other terms, such as “cyber threat information”, “threat intelligence”, “security incident information”, and “cybersecurity information”. Despite some similarities, these terms differ from CI, and, surprisingly, researchers have not made enough effort to deconstruct the concept. Moreover, it appears that most existing CIS studies assume that a common definition for CI exists and, therefore, do not see explicitly defining it as necessary.

In addition, CI differs from collective intelligence, which involves multiple actors collaborating on various co-related tasks to successfully solve problems (Malone et al., 2010). In contrast to collective intelligence, organizations individually generate and enrich cybersecurity intelligence. Once managers approve this intelligence after considering its criticality and sensitivity, their organization can share it fully or partially with other organizations.

Among the first few attempts at defining CI, Robinson, and Disley (2012) described security information based on network and security-related information, such as risks, vulnerabilities, and incidents, and remediation activities. Ludwick et al. (2013), Jasper (2017), and Mutemwa et al. (2017) extended this definition by addressing cybersecurity intelligence as the process of acquiring and analyzing information to identify, track, and predict cyberattacks. CI provides knowledge of an attacker’s capabilities, motives, resources, and objectives to assist organizations in their decision-making processes and enhance their defense strategies.

On a more technical level, Brown et al. (2015) described cybersecurity threat intelligence as low-level compromise indicators (e.g., malware hash-value, malicious IP addresses) that require immediate action through an automated response. They maintain that organizations can collect threat intelligence from or generate it through analyzing existing cyber information to help human agents take more efficient action responses. In much the same vein, Dalziel (2014) and Tounsi and Rais (2018) illustrated threat intelligence as contextual data from logical and analytical processes, which a human agent often evaluates for accuracy and quality. In some cases, an organization can automate the whole process and, thus, shorten the time between detection and compromise to improve incident response.

Chismon and Ruks (2015) suggest that threat intelligence refers to the process of moving from an “unknown unknown” to a “known unknown” cybersecurity risk state by discovering potential threats and then shifting to a “known known” risk state where one has investigated, understands, and can mitigate the cyber threat[4]. Mtsweni et al. (2016) highlight some differences between cybersecurity information and threat intelligence. According to their analysis, cybersecurity intelligence refers to structured, relevant, reliable, and timely information that one can action to improve security posture. Based on this approach, we can classify threat intelligence as strategic, tactical, and operational (Luiijf & Klaver, 2015). Table 1 deconstructs the commonly used concepts in the cybersecurity intelligence domain.

Table 1. Summary of Cyber Intelligence Concepts

Terminology	Data source	Characteristics	Action type
Cybersecurity intelligence or threat intelligence	• Technology tools • Human source	• Correlated, combined, verified, and enriched cybersecurity information • Used for predicting and responding to cyberattacks • Requires decision making at human-level	• Manual (i.e., decision making) • Automated (i.e., incident response)
Cybersecurity information	• Technology tools	• Machine-readable information • Low-level indicator of compromise • Not verified for false-positive information	• Mostly automated
Cybersecurity data	• Technology tools	• Large volume of raw cybersecurity data • Not verified or contextualized • Transmitted automatically or manually	• Mostly automated

[4] Former U.S Secretary of Defense Donald Rumsfeld first introduced the “known” and “unknown” concepts at a briefing in February 2002 (Logan, 2009). As applied to cyber risks, a ‘Known Known’ is a state of cybersecurity in which cyber risks are well determined and mitigated, ‘Unknown Unknown’ is a state in which cyber risks and cyber threats are inherently unknown, and ‘Known Unknown’ is a state in which we know that we do not know much about potential cyber risks (Logan, 2009).

4.2 A Summary View of CIS in the Literature

After identifying relevant papers, we used a combination author-centric and concept-centric matrix to categorize the 46 studies (Appendix B) based on their focus, research method, applied theories, unit of analysis, and objectives (Wang et al., 2015). We also address the factors and concepts that influence CIS in Section 5. We analyzed these studies to establish how they contribute to the CIS domain. We found that 35 studies adopted conceptual models, applied analytical frameworks, or reviewed existing technologies and protocols. Therefore, they provided only anecdotal information on CIS since they did not offer empirical evidence nor build on theoretical foundation. They focused variously on network security (Choraś, 2013), data-sharing models and architecture (Kokkonen et al., 2016; Mtsweni et al., 2016; Serrano et al., 2014; Skopik & Li, 2013), analytical frameworks (Luiijf & Klaver, 2015; Skopik et al., 2016), strategy (Greiman, 2015; Veerasamy, 2017; Zhao & White, 2017), organizational trust (Vázquez et al., 2012), technology typologies (Barnum, 2012; Dandurand & Serrano, 2013; Fransen et al., 2015; Kampanakis, 2014; Lewis et al., 2014; Takahashi & Kadobayashi, 2015), and CIS platforms (Mutemwa et al., 2017; Sauerwein et al., 2017).

Of the three broad TOE categories, the technology aspect of CIS received the most attention in the papers we identified (34 studies). These studies contributed to the discipline by introducing the technical foundations or building blocks for generating or consuming cybersecurity intelligence in organizations. We found that the organizational aspects of CIS received much attention (27 studies). Interestingly, 16 of the 46 studies investigated the technology and organizational aspects together, which highlights the need for a more overarching approach to CIS operations. Regarding research methodology, we found only one paper that reported a multi-method approach (Robinson & Disley, 2012); specifically, the paper used interviews and the Delphi method.

5 Findings on the Incentives and Challenges that Influence CIS

We used the TOE framework (Hassandoust et al., 2016) to summarize the CIS studies that we selected to review incentives and challenges that impact participation in CIS across organizations. From our literature review analysis, we found 35 factors that influence CIS practices across organizations. We list the factors and describe them in Appendix C.

We organized these incentives and challenges into four categories of influential determinants based on our proposed TOE framework (refer to Figure 1): technological, intra-organizational, inter-organizational, and environmental. In Tables 2 to 5, we present the factors that we identified in the literature according to the TOE framework by frequency (i.e., the number of times we found a factor in the literature review).

We also assessed the impact that these factors have on CIS adoption. For instance, we assessed each factor in Tables 2 to 5 to determine its positive (incentive) or negative (challenge) influence on CIS adoption. Since our CIS literature sample did not contain many empirical studies (i.e., quantitative or qualitative studies that tested or developed hypotheses and propositions), we inferred the incentive and challenge factors based on interpreting the literature. However, because doing so could leave our findings open to criticism due to their subjectivity, we subsequently discussed our findings with an industry practitioner (a subject matter expert in this area and familiar with the study) to review the factors we identified. As a result, we merged, relabeled, or removed some factors.

5.1 Technological Context

Many current cybersecurity technologies rely on vulnerability patterns (i.e., attack signatures) to identify cyberattacks (Mitra & Ransbotham, 2015). Schneier (1998) posits that security defenders have an “inferior” position because they have to be prepared to respond to every possible cybersecurity threat. On the other hand, an attacker merely needs to identify an existing security flaw in a system or a new vulnerability (i.e., zero-day vulnerability) to be able to bypass existing security controls and perform unauthorized or malicious activities. Unfortunately, signature-based anomaly detection capabilities (i.e., firewalls, proxies, anti-malware, and IDS/IPS) fail to provide reliable detection or protection against new zero-day vulnerabilities that use multi-vector and multi-stage methods (Brown et al., 2015). Thus, security defenders generally face having to respond to novel security threats that motivated and persistent attackers pose (Tounsi & Rais, 2018). In order to detect cyberattacks early and more quickly respond to them, cybersecurity defenders need to actively participate in sharing cybersecurity intelligence to obtain situational awareness about the latest risks and threats in cyberspace. With threat intelligence feeds,

organizations can integrate security information and event management (SIEM), firewalls, mail filtering devices, or other security capabilities in response to the latest indicators of compromises (IOCs) (i.e., suspicious IP addresses, malicious payloads, and malware signature) to help them manage threats, vulnerabilities, and security incidents.

Without CIS practices, organizations put themselves in an inferior position by deploying their cybersecurity defense capabilities in isolation without leveraging others' cybersecurity intelligence. Attackers can then reuse the same exploit against multiple target organizations, which minimizes how much it costs for them to make such attacks while maximizing their attack success rate (Kolini & Janczewski, 2017).

Previous studies have extensively investigated the technology factors that influence whether organizations adopt intelligence-driven technologies. However, researchers have not further investigated most such factors empirically to unfold their positive, negative, or neutral impacts on whether organizations adopt CIS processes. From our efforts, we identified 10 technology-related factors that influence CIS implementations. We analyzed these factors in their contexts to shed more light on their causal relationships with the CIS-related technology adoption. Table 2 presents technology-related factors and their positive and negative relationships with CIS adoption.

Table 2. Technological Incentives and Challenges

Technological factors	Frequency	Incentives (positive relationship)	Challenges (negative relationship)
Information quality	17	3	14
Information confidentiality	12	1	11
Cybersecurity standards	13	2	11
CI complexity	11		11
Technology integration and interoperability	9		9
Infrastructure quality	5		5
Faster incident response	3	3	
Technology cost	1		1
Technology education	1		1
Cybersecurity posture	1	1	

We found some discordant findings in that information quality, information confidentiality, and cybersecurity standards emerged as both positive (incentive) and negative (challenge) factors. For instance, on the one hand, researchers have identified firms with different CIS standards as a key challenge for implementing CIS technologies (Brown et al., 2015; Dandurand & Serrano, 2013; Fransen et al., 2015; Lee & Rao, 2007). On the other hand, other studies suggest that the presence of a few good cybersecurity threat intelligence standards will incentivize organizations towards using a unified structure and technology for generating and consuming cybersecurity intelligence. Ultimately, organizations achieve such a unified threat intelligence structure via automated, integrated, and interoperable information systems (Barnum, 2012; ENISA, 2016; Qamar et al., 2017). Researchers and practitioners have developed various industry-based standards to address CIS across organizations, such as OpenIOC, STIX, and IODEF (Asgarli & Burger, 2016). To date, most ontologies and standards define cyber observables, indicators, incidents, attack methodologies, exploit targets, courses of action, threat actors, and attack campaigns (Barnum, 2012; Fransen et al., 2015). Appendix C shows the major frameworks, standards, protocols, and ontologies that form the CIS ecosystem across organizations. These protocols and standards commonly appear in open source and commercial cybersecurity threat intelligence platforms.

The confidentiality of technology information poses another key challenge for participation in CIS operations. For example, IP addresses, technology components (i.e., names, services, operating system, database), and detection mechanisms (e.g., Firewall, IDS/IPS, WAF) include the confidential information that organizations do not often share (Fisk et al., 2015; Jasper, 2017; Johnson et al., 2016; Kampanakis, 2014; Kokkonen et al., 2016; Sutton, 2015).

Research has also highlighted accessing high-quality and actionable cybersecurity intelligence that reduces uncertainty in cybersecurity operations as a key challenge in CIS practices (Brown et al., 2015;

Skopik & Li, 2013; Sutton, 2015; Vázquez et al., 2012). In turn, receiving reliable and superior cybersecurity intelligence from other organizations and government agencies with higher maturity in cybersecurity operations could incentivize less-resourced organizations to participate in CIS activities (Robinson & Disley, 2012).

Cybersecurity intelligence's technical and tactical aspects can help to protect critical assets by providing an organization with the capability to predict cybersecurity threats before a malicious perpetrator compromises a system's confidentiality, integrity, and/or availability. However, cybersecurity intelligence-driven operations' complexity poses another key challenge that can prevent organizations from achieving the expected outcomes from intelligence-led operations. Previous studies have identified several such challenges and made recommendations for addressing them. Such challenges mostly relate to intelligence sources' volume and variety, data-quality issues, intelligence-enrichment difficulties, and automation complexities (Brown et al., 2015; Dandurand & Serrano, 2013; Fransen et al., 2015; Haass et al., 2015; Johnson et al., 2016; Veerasamy, 2017). Tounsi and Rais (2018) pinpoint data-quality issues as largely related to the extent to which organizations can scale and integrate different threat intelligence data sources (i.e., open-source and public threat intelligence feeds). They suggested using a common standardized vocabulary for threat intelligence feeds to help organizations customize threat intelligence-sharing tools, stream aggregation, and the search capabilities required for daily intelligence-sharing tasks (Tounsi & Rais, 2018; Serrano et al., 2014).

While cybersecurity intelligence operations ultimately focus on producing cybersecurity intelligence that organizations can embed into their workflows, previous studies show that integrating cybersecurity intelligence and ensuring that such intelligence operates with internal information systems pose key challenges for many organizations (Lee & Rao, 2007; Skopik et al., 2016). In much the same vein, Brown et al. (2015) posit that technology standards define normalized data models for detecting and responding to security events. However, these data models are not sufficiently generic to increase interoperability between CIS platforms. Establishing interoperability between cybersecurity intelligence platforms improves the quality of cybersecurity intelligence networks and provides more reliable cybersecurity intelligence in a faster time frame.

5.2 Organizational Context

The organizational context refers to internal organizational factors (intra-organizational factors) and external organizational factors (inter-organizational factors) that influence organizations with regard to entering into CIS projects. Intra-organizational incentive and challenge factors refer to a firm's characteristics that relate to strategy, structure, culture, processes, and resources (Salleh & Janczewski, 2016). As such, intra-organizational factors determine the likelihood that a firm will adopt repeatable processes and procedures to generate, consume, and/or share cybersecurity intelligence.

Inter-organizational incentive and challenge factors refer to determinants that arise from interaction with other organizations. With regard to inter-organizational CIS networks, these factors influence CIS effectiveness and fairness and network performance and quality (Gil-Garcia et al., 2010).

Previous studies show that organizations often operate in an interconnected environment where each organization's business excellence and performance depend highly on its cooperation and mutual relationships with other organizations (Gulati, 1998; Oliver, 1990). Inadequate inter-organizational relationships with business partners, suppliers, and competitors place efforts to form any network, including a CIS network, at risk (Oliver, 1990). Additionally, Bouchard (1993) argues that an organization's decision to participate in any collaborative activities will depend on the number of organizations that already participate or that plan to in them.

Hence, we see a need to investigate the organizational factors on which CIS networks depend to form and CIS operations depend to evolve. In this study, we consider intra-organizational and inter-organizational factors as subsets of organizational factors to better understand these factors. We acknowledge that inter-organizational and intra-organizational factors may sometimes overlap, which we discuss in our findings.

5.2.1 Intra-organizational Factors

From analyzing the literature, we found that organizational structure, people resources, operational costs, IT and security processes, intelligence-sharing models, information assurance, organizational performance, and culture constitute factors that may incentivize organizations to adopt cybersecurity intelligence-driven operations (Brown et al., 2015; Johnson et al., 2016). In particular, these factors (refer

to Table 3) may enable an organization to generate and use cybersecurity intelligence internally and/or share it with their partners in CIS networks. Cybersecurity intelligence creates organizational value by allowing senior and functional management to make informed decisions about cybersecurity operations, such as cyber threats, security incident responses, technology investment, and the prioritization of cybersecurity operations.

Several studies have addressed the negative impact that personal information breaches, intellectual property leaks, and damage to a firm's reputation have on whether organizations adopt intelligence-driven operations (Choraś, 2013; Fisk et al., 2015; Kantola & Jaitner, 2016; Lee & Rao, 2007; Serrano et al., 2014; Veerasamy, 2017). Primarily, leaked sensitive corporate information or personally identifiable information (PII), information that that cybersecurity intelligence may embed, can cause reputational risk issues for organizations. To address this risk, many organizations develop a privacy-preserving policy and data-classification framework to show what types of information they can share with other entities. For instance, applying the traffic light protocol (TLP) can help organizations share more cybersecurity threat intelligence across organizations (Fisk et al., 2015). However, in general, overly complex data-protection controls affect organizational attitudes towards CIS outside an organization's boundaries (Dandurand & Serrano, 2013; Fransen et al., 2015; Robinson & Disley, 2012). Further, another challenge in CIS operations involves the risks associated with an inability to control data that has been shared beyond the organizational network (Vázquez et al., 2012).

We also found cost to the organization as another factor with discordant results. On the one hand, papers identified concerns with profit realization and the costs associated with cybersecurity intelligence operations, organizational resources, and collaboration as determinants that can have a negative impact on the extent to which an organization adopts CIS practices (Fransen et al., 2015; Haass et al., 2015; Ring, 2014; Robinson & Disley, 2012). On the other hand, the cost-saving benefits achieved from receiving high-quality contextualized cybersecurity intelligence and timely incident responses can motivate organizations to actively participate in CIS practices (Vázquez et al., 2012). Table 3 presents intra-organizational factors and their positive and negative relationships with CIS adoption.

Table 3. Intra-organizational Incentives and Challenges

Intra-organizational factors	Frequency	Incentives (positive relationship)	Challenges (negative relationship)
Organizational cost	10	3	7
Information confidentiality (organizational)	9		9
Organizational performance	9	5	4
Organizational cybersecurity readiness	6	3	3
Information-sharing model	4	1	3
Organizational sharing culture	4	2	2
Organizational structure	3	2	1
Management support	2	2	2
Skilled resources	2		2
Formality of intelligence-driven operations	2	2	
Data governance	1		1

Without CIS practices, organizations work in isolation to mitigate cyberattacks. Meanwhile, attackers need only discover one security weakness to be able to subsequently replicate the attack on multiple vulnerable targets. To address this gap, organizations should promote an information-sharing culture to minimize the impact that cyberattacks have on their operations (Ring, 2014). Lee and Rao (2007) show that an organizational culture that fosters voluntary cooperation can emerge due to the mutual benefits achieved from receiving reliable cybersecurity intelligence. Hence, researchers have suggested voluntarily sharing cybersecurity intelligence as the most successful model for cybersecurity intelligence sharing in organizations (Goodwin et al., 2015).

5.2.2 Inter-organizational Factors

Cybersecurity intelligence benefits organizations by providing valuable information in a timely manner and helping them to coordinate cybersecurity operations and responses to incidents. However, many organizations resist sharing cybersecurity intelligence as they fear losing their operational excellence relative to other organizations (Robinson & Disley, 2012). However, without such sharing, cyber attackers maintain an advantage over organizational defenders (Skopik & Li, 2013). According to Yang and Maxwell (2011), sharing information requires complex interactions between participant organizations due to differences in their cultures, values, and origins. In our analysis, we identified nine inter-organizational incentive and challenge factors that influence how inter-organizational relationships form or progress in CIS (refer to Table 4). Among the identified factors, we found trust between organizations the most challenging for inter-organizational relationships and lack of trust to have a negative impact on whether organizations form CIS networks (Katsikeas et al., 2009; Robson et al., 2008). Further, we noted that the CIS literature lacks empirical research into organizational factors and underlying mechanics that account for how organizations should form and maintain trust-based relationships and strategic alliances to enhance their CIS. Table 4 presents inter-organizational factors and their positive and negative relationships with CIS adoption.

Table 4. Inter-organizational Incentives and Challenges

Inter-organizational factors	Frequency	Incentives (positive relationship)	Challenges (negative relationship)
Trust relationships	19		19
Reciprocity in CIS	7		7
Information assurance	7	1	6
Anonymity	4	2	2
Inter-organizational goal alignment	4		4
Inter-organizational culture	3	2	1
Data-sharing agreement	2	2	
Sharing community size	1	1	

A trust-based relationship constitutes a key determinant for establishing successful and efficient CIS across organizations. Vázquez et al. (2012) addressed two types of trust in CIS operations: trust in the CIS network and trust between CIS participants. They suggest that the trust level between CIS participants does not need to endure and, thus, differs from other inter-organizational relationships (i.e., supply chain). A temporary and transient trust between CIS participants during a cybersecurity event may allow them to share cybersecurity intelligence. However, if the trust between participants remains transitory, it may impede an effective and sustained CIS network from evolving over a longer time period (ENISA, 2016).

Other studies focused on antecedents that may have a causal effect on trust formation in CIS operations. In this context, elements such as data misuse, relationships with competitors, inter-organizational collaboration, and loyalty influence whether participants form sufficient trust for effective CIS practices (Fransen et al., 2015; Gal-Or & Ghose, 2005; Hernandez-Ardieta et al., 2013; Johnson et al., 2016; Murdoch & Leaver, 2015; Rak, 2002; Sutton, 2015; Tosh et al., 2015). Further, Mayer et al. (1995) suggest that poor trust has its roots in the term's definition since organizations may not mutually understand the concept in a way that would help them establish trust-based relationships.

From reviewing the literature, we found that organizations require sufficient confidence in terms of goal alignment and information assurance. In this setting, goal alignment refers to the strategic and tactical alignment between firms when combating cybersecurity threats. Previous studies have found that organizations find it challenging to align their cybersecurity goals since they often have have different priorities based on their capabilities (Helmbrecht et al., 2013; Murdoch & Leaver, 2015). Second, information assurance means that participants in the CIS network have built appropriate capabilities to protect and maintain the cybersecurity intelligence received from the other participants given cybersecurity intelligence's confidential nature.

Moreover, reciprocity in CIS constitutes an important incentive that relates to the improved reliability and transparency in CIS networks and results from limiting deviant participant behavior, such as "free-riding".

Free-riding features as an historical issue in the economics literature and refers to an entity's behaviors around maximizing their benefits while minimizing how much intelligence-driven operations cost (Appan & Bacic, 2016; Gal-Or & Ghose, 2005; Naghizadeh & Liu, 2016).

Several papers identified anonymity, culture, diversity, and data-sharing agreements as other determinants that may influence an organization's participation in CIS routines (de Fuentes et al., 2017; Johnson et al., 2016; Sutton, 2015; Vance et al., 2017).

5.3 Environmental Context

Studies no longer saw CIS challenges and incentives only in terms of organizational and technological factors. Indeed, many studies also discussed environmental factors. Environmental factors involve the setting in which a firm conducts its business and include industry, competitors, access to resources that others supply, and the regulatory environment (Tornatzky et al., 1990). From our review, we identified six factors that relate the environmental context (see Table 5). Papers identified factors such as market competition, laws and regulations, brand reputation, privacy, and government influence as determinants that influence CIS operations. From assessing these factors, we found that organizations find complying with laws and regulations as the most challenging activity in the environmental context. Challenges can stem from liability issues, differing legal and regulatory jurisdictions, attribution complexity, and fragmented organizational policies (ENISA, 2016; Greiman, 2015; Johnson et al., 2016; Kampanakis, 2014; Serrano et al., 2014).

Davenport et al. (1996) suggested that information represents a critical asset for improving business performance and retaining a competitive advantage. However, CIS practices are subject to information constraints created by the competitive environment and institutional pressures that negatively impact whether organizations form and continue with practices and routines (Rak, 2002; Skopik & Li, 2013). Greiman (2015) suggested that the "cybersecurity paradox" has emerged due to a tangled cybersecurity environment where corporate competition, privacy gaps, and unfit laws and regulatory structures commonly impact CIS practices. Davenport et al. (1992) coined the term "the politics of information" to describe how information owners resist sharing information freely through bureaucratic behaviors. As such, Appan and Bacic (2016) applied the relational view of the firm theory to investigate the competitive behaviors[5] of firms in trusted collaboration networks, such as the Information Sharing and Analysis Centre (IT-ISAC).

Some papers suggested that factors related to organizational reputation, such as adverse publicity or a drop in market value, have a negative impact on CIS practices (Goodwin et al., 2015; Rak, 2002; Tosh et al., 2015). Organizational reputation represents a valuable intangible asset for sustaining a competitive advantage (Rindova et al., 2005). Therefore, organizations generally tend to avoid any practices or operations that may have adverse impacts on their brand, reputation, and public image.

Other studies show that peer reputation and recognition from other CIS participants (e.g., "I want to be seen the [as the] first [to] have found, understood, and dealt with an exploit") constitutes a key incentive for some organizations to share cybersecurity intelligence with other parties (Murdoch & Leaver, 2015).

Finally, in the environmental context, organizations must obtain the benefits from CIS in a way that does not breach privacy or expose personal information (Goodwin et al., 2015). Improper personal information disclosures in cybersecurity intelligence occur due to privacy risks in organizations. The literature has addressed some such risks to privacy, such as inadequate data sanitization, confidential personally identifiable information (PII) leaks, non-compliance with laws and regulations, mishandled private information, and complex privacy models (de Fuentes et al., 2017; Goodwin et al., 2015; Haass et al., 2015; Johnson et al., 2016). In order to address privacy concerns, organizations should implement privacy-preserving controls and handling procedures to protect private information (Haass et al., 2015; Johnson et al., 2016). They should enforce these controls via intelligence-sharing platforms, standards, and privacy models such as STIX/TAXI, which transforms threat intelligence private data into a sanitized exchange format (de Fuentes et al., 2017; Kampanakis, 2014). Table 5 presents environmental factors and their positive and negative relationships with CIS adoption.

[5] The coopetition paradox refers to the situation where firms share sensitive and potentially competitive intelligence with their direct competitors (Appan & Basic, 2016).

Table 5. Environmental Incentives and Challenges

Environmental factors	Frequency	Incentives (positive relationship)	Challenges (negative relationship)
Laws and regulations	15	3	12
External pressure	9	3	6
Intensity of market competition	8		8
Privacy	7		7
Reputation	6	2	4
Communication channels	4	3	1

5.4 Revised CIS Framework

Via synthesizing the reviewed literature and influential technology, organizational, and environmental factors, we developed a revised research framework that we illustrate in Figure 3. Our revised research framework demonstrates how factors that we identified from the TOE framework contribute to explaining the factors that influence organizations to adopt CIS technologies and processes. Future research can advance this framework by considering the direct and indirect effect that factors that operate across the TOE dimensions have on CIS adoption.

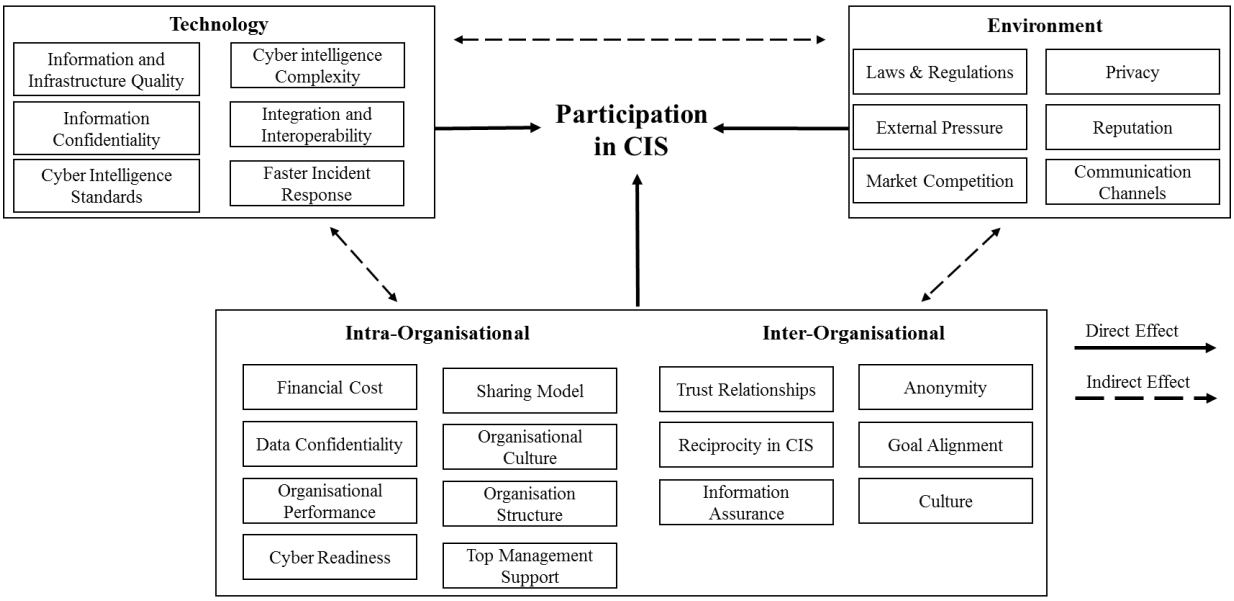

Figure 3. Revised Framework for CIS Engagement

5.5 Theoretical Approaches

Many researchers assume that research papers should follow a systematic approach to apply theory and a scientific research method (Lee, 2004). However, only 11 studies (among the 46 we reviewed) applied theoretical foundations to investigate CIS (Lee & Rao, 2007; Gal-Or & Ghose, 2005; Appan & Bacic (2016); Liu et al., 2014; Hernandez-Ardieta et al., 2013; Naghizadeh & Liu, 2016; Vance et al., 2017; Tosh et al., 2015; Robinson & Disley, 2012; Webb et al., 2016; Lewis et al., 2014). In general, these 11 studies derived the theories they applied, such as exchange theory, the relational view of the firm, the theory of reasoned action (TRA), and situational awareness theory (SAT), from social science and economic paradigms (Gal-Or & Ghose, 2005; Lee & Rao, 2007; Vance et al., 2017; Webb et al., 2016). For example, Appan and Bacic (2016) applied the relational view of the firm at the organizational level to investigate the "coopetition paradox", which refers to the situation where firms share sensitive and potentially competitive intelligence with their direct competitors. The studies based in economics applied game theory to explore the economic incentives that foster or the challenges that hinder organizations from sharing cybersecurity intelligence (Gal-Or & Ghose, 2005; Naghizadeh & Liu, 2016; Tosh et al., 2015). These studies investigated the influence that organizational factors such as competitive advantage,

operational costs, financial performance, and security investment have on firms' CIS practices. Only Vance et al. (2017) scrutinized inter-organizational trust, which firms require to form or develop relationships with one another (Robson et al., 2008). Hence, research has not empirically proven to what extent enhanced trust between firms can address challenges in adopting CIS operations, such as cybersecurity risk management, venture performance, incident sharing, brand damage, and deviant inter-firm behaviors.

Pursuant to this context, Lee (2001) argued that research in the IS discipline should not only investigate the socio-technical system but also the phenomena that emerge from the interaction between these two dimensions. Thus, it remains for future research to advance theory building in the discipline through formal theorizing in combination with the development of substantive and mid-range theories (Gregor, 2006; Markus & Robey, 1988) that explain the interaction between different IS phenomena dimensions; in this case, CIS across organizations. This process should then lead to researchers to develop theoretical models for analyzing, explaining, and predicting how CIS routines begin and advance across organizations.

In relation to our third research question, we present Table 6 as a guide for IS scholars who seek to investigate CIS. For example, diffusion of innovation (DOI) (Rogers & Shoemaker, 1983), inter-organizational relationships (IOR) (Oliver, 1990), social exchange theory (SET) (Gefen & Ridings, 2002), critical mass theory (CMT) (Bouchard, 1993), a general theory of network governance (GTNG) (Jones et al., 1997), and resource dependence theory (RDT) (Jayatilaka, Schwarz, & Hirschheim, 2003) represent just some a priori theories that have strong roots in the IS discipline. However, researchers have yet to explore them empirically in the CIS domain. In Table 6, we map the focus point for each theory against the TOE framework and identify example areas that future studies could investigate.

Table 6. Recommended Theories for Future Studies

TOE dimension	Example areas for future study	Point of focus	Theory						
			DOI	IOR	SET	CMT	GTN	RDT	TAM
Technology	• Adoption of CIS technology • Adoption of intelligence-driven processes	Complexity	✓						✓
		Compatibility	✓						✓
		Transactional cost							
		Usability							✓
		Efficiency		✓					✓
		Relative advantage	✓						✓
Organization	• Formation of CIS network • Participation in CIS network • Performance of CIS network	Trust		✓	✓				
		Reciprocity		✓					
		Network size				✓			
		Network benefit		✓		✓			
		Interconnectedness						✓	
		Network benefit		✓		✓			
		Performance				✓		✓	
Environment	• Governance of CIS network	Laws and regulations			✓		✓		
		Culture					✓		
		External pressure			✓		✓		
		Reputation	✓				✓		

Table 6 shows potential overlaps between the focus points across the recommended theories. For instance, researchers could use both IOR and SET to address the trust element or apply DOI and TAM to investigate whether organizations will adopt CIS technology and intelligence-driven processes. Existing competing theories may raise questions about favoring one theory over another. Although we cannot formulate an absolute answer to this question since a "best theory" does not exist, we can draw on Truex et al. (2006) and the four recommendations for using theory in IS domain work that they developed after investigating adapting theories in IS research. They recommend considering the fit between the theory

and phenomenon of interest, the theory's historical context, the method one chooses, and how the theorizing contributes to cumulative theory. As such, we recommend that researchers who seek to investigate CIS consider their research question carefully and understand the ontological and epistemological underpinnings of the theories they select (Gregor, 2006). This process includes defining and applying constructs to identify fundamental differences between theories, establishing an appropriate research methodology for CIS, and following the cumulative tradition by adding to the CIS theorizing process where possible.

6 Research Discussion, Contribution, and Future Studies

In this study, we performed a systematic descriptive literature review of CIS research. We used the TOE framework to systematically categorize incentives and challenges that we found in the literature. Prior studies have used this framework to investigate cyber security initiatives (Salleh & Janczewski, 2016; Skopik et al., 2016). From our literature search methodology, we found 46 relevant studies. Also, from our in-depth literature analysis, we found 35 different incentives and challenges, which we categorized according to the TOE framework. Findings from the literature review show technological and organizational factors represent common challenges for CIS adoption in organizations. We also noted that many studies in CIS have focused on solving problems form a narrow technology deployment lens such as technology implementation or information systems integration (Dandurand & Serrano, 2013; Kampanakis, 2014; Veerasamy, 2017). We found that only 11 studies used theoretical assumptions and provided empirical evidence—an insufficient number for the CIS domain. Also, we find some discordant findings in the technology and organization domains that require further investigation in future research. With this study, we make six contributes to CIS research.

First, we note that some factors have received more attention based on the incentive and challenge factors we identified in our literature review. These factors included information quality, information confidentiality, intelligence-sharing standards, technology complexity (technology factors); organizational cost, organizational performance, information confidentiality, organizational readiness (intra-organizational factors); trust relationships, reciprocity, information assurance (inter-organizational factors); and law and regulations, competition in the market, and external pressure (environmental factors).

Second, in most papers we reviewed, the incentive and challenge factors identified as influencing engagement in CIS practices had no basis in empirical analysis and hypothesis testing. Hence, we lack empirical proof as to the extent to which these factors influence CIS. While some studies reported receiving guidance from theoretical foundations (namely, TRA, TAM, and economic cost theory) (Gal-Or & Ghose, 2005; Lee & Rao, 2007; Liu et al., 2014; Vance et al., 2017), due to their generic nature, these theories cannot measure the interaction between CIS operations' technological, organizational, and environmental dimensions.

Third, we found some factors that occurred across multiple categories in the TOE framework. Specifically, information confidentiality, data privacy, transactional cost, and culture appeared in multiple TOE framework categories. Thus, scholars need to pay more attention to these incentives and challenges to ensure that they have adequately investigated them from various perspectives. For instance, from a technical viewpoint, Organizations consider protecting sensitive technology information by sanitizing and anonymizing it a key challenge for technology and security functions (Fisk et al., 2015; Jasper, 2017; Johnson et al., 2016; Kampanakis, 2014).

From an organizational viewpoint, protecting personal information and managing data-classification and privacy risks represent the main concerns for the business function. Privacy concerns that arise from leaked personally identifiable information (PII) and privacy and regulatory breaches emerged as the main concern in the environmental context (Murdoch & Leaver, 2015; Serrano et al., 2014; Sutton, 2015; Veerasamy, 2017). Thus, our findings support our decision to choose the TOE framework as the basis for our literature review and highlight the need to explore CIS operations using multidisciplinary paradigms to ensure that we identify and consider all the CIS practice determinants for improvement. Additionally, CIS practice involves not only technology but also organizational processes and procedures. As such, organizations need to promote a CIS culture across their business and technology functions to ensure that all employees understand cybersecurity intelligence sharing's value and that they communicate it to all relevant stakeholders.

Fourth, from reviewing the literature, we identified discordant findings for some factors; namely, information quality, incident response, cybersecurity standards (technology factors); organizational performance, readiness, culture, and structure (organizational factors); anonymity (inter-organizational factor); and laws and regulations, government influence, and organizational reputation (environment factors). Scholars need to further examine these factors by applying different research methods, paradigms, and theoretical foundations. According to Soh and Markus (1995), studies with conflicting results invite researchers to better understand the phenomenon in question. Hence, CIS resembles other domains such as management and organizational science, which demand multiple research paradigms (Benbasat & Weber, 1996; Mingers, 2001). Kaplan and Duchon (1988) suggest that mixed-methods studies represent an appropriate choice in these cases. Mixed methods increase scientific rigor since researchers can assess results' validity via triangulating different data sources.

Fifth, we also found that the studies we reviewed did not focus on individual factors and human characteristics that might impact engagement in CIS practices. Therefore, future research needs to consider CIS-related factors at the individual level, such as individual behavior, intrinsic and extrinsic motivation, experience, and top management and C-level influence on decision making. We also found culture and data-sharing model agreement to be important factors in both the intra-organizational and inter-organizational dimensions, which shows that researchers should empirically investigate the interaction between intra-organizational and inter-organizational factors to understand how intra-organizational factors may impact inter-organizational relationships and vice versa.

Sixth, from analyzing the theories we recommended that future studies adopt, it seems that researchers may not be able to rely on a single theory to sufficiently explain the causal relationships between influential factors in CIS. Researchers could find adopting multiple theories challenge since they would need to combine them in order to analyze, explain, predict and/or provide guidance on the sequence of events that occur in CIS (Gregor, 2006). This situation could represent an opportunity for IS scholars to expand existing theories to craft our "own" tailored theory (Weber, 2003) to study CIS across organizations.

Practitioners looking to embark on CIS initiatives could also apply our findings. The incentives and challenges that we discuss shed more light into the complexities that CIS projects involve and can help practitioners define fit-for-purpose CIS initiatives. Armed with this knowledge, technology and security leaders can influence key stakeholders in their organizations and develop support for CIS operations. In this study, we also offer a holistic and inclusive definition for cybersecurity intelligence and a typology for CIS standards that any organization can use as a reference resource.

6.1 Research Limitations

As with any study, ours has several limitations. First, we limited our keyword search to include the terms that we list in Section 3. We acknowledge that using other additional keywords may have returned additional papers for assessment. Nevertheless, we focused strictly on "cybersecurity" and "threat" intelligence sharing in this paper. Second, we examined relevant journals that the three scholarly databases we chose indexed and additional journals that we identified from the ABDC journal quality list. Hence, we did not consider papers that these databases did not index for investigation or analysis. We also may have missed relevant conference papers that our selected scholarly databases did not index.

Third, we used reference searches or backward searching to broadly identify and review industry-based practitioner publications. Therefore, we did not apply a systematic method to identify and review non-academic journal and conference publications. Fourth, since this study builds on other scholars' work, our review may reflect the weaknesses in previous studies.

Fifth, following Webster and Watson (2002), we approached the literature in order to extend the current body of knowledge about CIS practices across organizations. Since CIS represents a relatively recent phenomenon, we focused on identifying organizational challenges and incentives that motivate or hinder engagement in CIS practices. As such, our approach offers a specific but limited view of actual CIS practices across organizations both nationally and globally.

Finally, we did not empirically corroborate how well the TOE framework categorizes factors that influence CIS practices. Instead, we developed the factors we identified based on analyzing and interpreting previous publications. Thus, we recommend that researchers further develop and validate CIS engagement models to support their practical use.

7 Conclusions

CIS remains in its infancy, and shortcomings related to CIS practices have attracted great interest from academics and practitioners. We encourage interdisciplinary scholars to conduct empirical studies to address these shortcomings. In this study, we reviewed the CIS literature and identified 35 incentive and challenge factors from previous studies that influence CIS. We classified these factors based on the TOE framework and, specifically, its technological, intra-organizational and inter-organizational, and environmental dimensions. This study offers both theoretical and practical perspectives. Theoretically, by incorporating concepts from the CIS literature, we provide a foundation for future research into determinants that may impact engagement in CIS routines. From a practical perspective, we also considers some industry best practices and integrate them with findings from academic papers to view cybersecurity intelligence operations in organizations in a holistic manner. This study should help organizations understand the benefits they can expect from receiving reliable and appropriate cybersecurity intelligence due to investing in CIS practices and routines.

References

Akbulut, A. Y. (2003). *An investigation of the factors that influence electronic information sharing between state and local agencies* (doctoral dissertation). Louisiana State University and Agricultural and Mechanical College.

Akbulut-Bailey, A. Y. (2011). Information sharing between local and state governments. *Journal of Computer Information Systems, 51*(4), 53-63.

Alvarez, M., Bradley, N., Bryan, D., Craig, S., Kassem, L., Kravitz, J., & Usher, M. (2018). IBM X-Force threat intelligence index 2018. *IBM*. Retrieved from https://www.justinholman.com/wp-content/uploads/2019/03/Threat-Intelligence-2018-IBM-X-Force.pdf

Appan, R., & Bacic, D. (2016). Impact of information technology (IT) security information sharing among competing IT firms on firm's financial performance: An empirical investigation. *Communications of the Association for Information Systems, 39*, 214-241.

Asgarli, E., & Burger, E. (2016). Semantic ontologies for cyber threat sharing standards. In *Proceedings of the IEEE Symposium on Technologies for Homeland Security.*

Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., & Beekhuyzen, J. (2015). Achieving rigor in literature reviews: Insights from qualitative data analysis and tool-support. *Communications of the Association for Information Systems, 37*, 154-204.

Barnum, S. (2012). *Standardizing cyber threat intelligence information with the structured threat information expression (STIX™).* MITRE Corporation. Retrieved from https://www.mitre.org/sites/default/files/publications/stix.pdf

Benbasat, I., & Weber, R. (1996). Research commentary: Rethinking "diversity" in information systems research. *Information Systems Research, 7*(4), 389-399.

Blaxter, L. (2010). *How to research*. McGraw-Hill Education.

Bouchard, L. (1993). Decision criteria in the adoption of EDI. In *Proceedings of the 14th International Confernce on Information Systems*.

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security.*

Carter, J. G. (2015). Inter-organizational relationships and law enforcement information sharing post 11 September 2001. *Journal of Crime and Justice, 38*(4), 522-542.

Casciaro, T., & Piskorski, M. J. (2005). Power imbalance, mutual dependence, and constraint absorption: A closer look at resource dependence theory. *Administrative Science Quarterly, 50*(2), 167-199.

Chau, P. Y., & Tam, K. Y. (1997). Factors affecting the adoption of open systems: An exploratory study. *MIS Quarterly, 21*(1), 1-24.

Chavarria, J. A., Andoh-Baidoo, F. K., Midha, V., & Hughes, J. (2016). Software piracy research: A cross-disciplinary systematic review. *Communications of the Association for Information Systems, 38*, 624-669.

Chen, H., Wang, F.-Y., & Zeng, D. (2004). Intelligence and security informatics for homeland security: information, communication, and transportation. *IEEE Transactions on Intelligent Transportation Systems, 5*(4), 329-341.

Chismon, D., & Ruks, M. (2015). *Threat intelligence: Collecting, analysing, evaluating*. MWR InfoSecurity.

Choraś, M. (2013). Comprehensive approach to information sharing for increased network security and survivability. *Cybernetics and Systems*, *44*(6-7), 550-568.

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, *20*(2), 96-121.

Dalziel, H. (2014). *How to define and build an effective cyber threat intelligence capability*. Elsevier.

Dandurand, L., & Serrano, O. S. (2013). Towards improved cyber security information sharing. In *Proceedings of 5th International Conference on Cyber Conflict.*

Davenport, T. H. (1996). Some principles of knowledge management. *Strategy & Business, 1*(2), 34-40.

de Fuentes, J. M., González-Manzano, L., Tapiador, J., & Peris-Lopez, P. (2017). PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing. *Computers & Security, 69*, 127-141.

ENISA. (2016). *Report on cyber security information sharing in the energy sector.* Retrieved from https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector/at_download/fullReport

Fielt, E., Bandara, W., Miskon, S., & Gable, G. (2014). Exploring shared services from an IS perspective: a literature review and research agenda. *Communications of the Association for Information Systems, 34*, 1001-1040.

Fisk, G., Ardi, C., Pickett, N., Heidemann, J., Fisk, M., & Papadopoulos, C. (2015). Privacy principles for sharing cyber security data. In *Proceedings of IEEE Symposium on Security and Privacy Workshops.*

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness—a systematic review of the literature. *Computers & Security, 46*, 18-31.

Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *e & i Elektrotechnik und Informationstechnik, 132*(2), 106-112.

Furneaux, B., & Wade, M. R. (2011). An exploration of organizational level information systems discontinuance intentions. *MIS Quarterly, 35*(3), 573-598.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research, 16*(2), 186-208.

Gefen, D., & Ridings, C. (2002). Implementation team responsiveness and user evaluation of customer relationship management: A quasi-experimental design study of social exchange theory. *Journal of Management Information Systems, 19*(1), 47-69.

Gil-Garcia, R., Pardo, T. A., & Burke, G. B. (2010). Conceptualizing information integration in government. *In H. J. Schnoll (Ed.), E-Government: Information, Technology, and Transformation.* Routledge.

Goodwin, C., Nicholas, J. P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., Neutze, J. (2015). A framework for cybersecurity information sharing and risk reduction. *Microsoft*. Retrieved from https://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal, 26*(2), 91-108.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly, 30*(3), 611-642.

Greiman, V. (2015). Public/private partnerships in cyberspace: Building a sustainable collaboration. *Journal of Information Warfare, 14*(3), 30-42.

Gulati, R. (1998). Alliances and networks. *Strategic Management Journal, 19*(4), 293-317.

Haass, J. C., Ahn, G.-J., & Grimmelmann, F. (2015). ACTRA: A case study for threat information sharing. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*.

Hallen, L., Johanson, J., & Seyed-Mohamed, N. (1991). Interfirm adaptation in business relationships. *Journal of Marketing, 55*(2), 29-37.

Hassandoust, F., Techatassanasoontorn, A. A., & Tan, F. B. (2016). Factors influencing the infusion of information systems: A literature review. *Pacific Asia Journal of the Association for Information Systems, 8*(1), 1-32.

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy, 26*(6), 639-688.

Helmbrecht, U., Purser, S., Cooper, G., Ikonomou, D., Marinos, L., Ouzounis, E., Capogrossi, S. (2013). *Cybersecurity cooperation—defending the digital frontline*. *ENISA*. Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-cooperation-defending-the-digital-frontline

Hernandez-Ardieta, J., Tapiador, J., & Suarez-Tangil, G. (2013). Information sharing models for cooperative cyber defence. In *Proceedings of 5th International Conference on Cyber Conflict.*

Internet Live Stats. (2018). *In 1 second, each and every second there are….* Retrieved from http://www.internetlivestats.com/one-second/#traffic-band

Jafarzadeh, H., Aurum, A., D'Ambra, J., & Ghapanchi, A. (2015). A systematic review on search engine advertising. *Pacific Asia Journal of the Association for Information Systems, 7*(3), 1-32.

Jasper, S. E. (2017). US cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence, 30*(1), 53-65.

Jayatilaka, B., Schwarz, A., & Hirschheim, R. (2003). Determinants of ASP choice: An integrated perspective. *European Journal of Information Systems, 12*(3), 210-224.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to cyber threat information sharing* (SP 800-150). *NIST*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-150/final

Jones, C., Hesterly, W. S., & Borgatti, S. P. (1997). A general theory of network governance: Exchange conditions and social mechanisms. *Academy of Management Review, 22*(4), 911-945.

Kampanakis, P. (2014). Security automation and threat information-sharing options. *IEEE Security & Privacy, 12*(5), 42-51.

Kantola, H., & Jaitner, M. L. (2016). Cyber defence information sharing in a federated network. In *Proceedings of 8th International Conference on Cyber Conflict.*

Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: a case study. *MIS Quarterly, 12*(4), 571-586.

Katsikeas, C. S., Skarmeas, D., & Bello, D. C. (2009). Developing successful trust-based international exchange relationships. *Journal of International Business Studies, 40*(1), 132-155.

Kelly, S., Gibson, N., Holland, C. P., & Light, B. (1999). Focus issue on legacy information systems and busines process engineering: A business perspective of legacy information systems. *Communications of the Assocation for Information Systems, 2*, 1-40.

King, W. R., & He, J. (2005). Understanding the role and methods of meta-analysis in IS research. *Communications of the Association for Information Systems, 16*, 665-686.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (technical report version 2.3). Retrieved from https://www.elsevier.com/__data/promis_misc/525444systematicrev iewsguide.pdf

Kokkonen, T., Hautamäki, J., Siltanen, J., & Hämäläinen, T. (2016). Model for sharing the information of cyber security situation awareness between organizations. In *Proceedings of 23rd International Conference on Telecommunications.*

Kolini, F., & Janczewski, L. (2015). Cyber defense capability model: A foundation taxonomy. In *Proceedings of 5th International Conference on Information Resource Management.*

Kolini, F., & Janczewski, L. (2017). Two heads are better than one: A theoretical model for cybersecurity intelligence sharing (CIS) between organisations. In *Proceedings of 17th Australaisian Conferences on Information Systems.*

Lee, A. (2001). MIS Quarterly's editorial policies and practices. *MIS Quarterly, 25*(1), iii-vii.

Lee, A. S. (2004). Thinking about social theory and philosophy for information systems. In L. Willcocks & J. Mingers (Eds.), *Social theory and philosophy for information systems* (pp. 1-26). John Wiley & Sons.

Lee, J., & Rao, H. R. (2007). Understanding socio-technical environments for acceptance of inter-agency anti/counter-terrorism information sharing systems. In *Proceedings of 40th Annual Hawaii Internation Conference on System Sciences.*

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). Cybersecurity information sharing: A framework for sustainable information security management in UK SME supply chains. In *Proceedings of 22nd European Conference in Information Systems.*

Li, J., Zic, J., Oakes, N., Liu, D., & Wang, C. (2016). Design and evaluation of an integrated collaboration platform for secure information sharing. In *Proceedings of the International Conference on Cooperative Design, Visualization and Engineering*.

Liu, C. Z., Zafar, H., & Au, Y. A. (2014). Rethinking FS-ISAC: An IT security information sharing network model for the financial services sector. *Communications of the Association for Information Systems, 34*, 15-36.

Logan, D. C. (2009). Known knowns, known unknowns, unknown unknowns and the propagation of scientific enquiry. *Journal of experimental botany*, *60*(3), 712-714.

Ludwick, M., McAllister, J., Mellinger, A., Sereno, K., & Townsend, T. (2013). *SEI emerging technology center: Cyber intelligence tradecraft*. Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=40201

Luiijf, E., & Klaver, M. (2015). On the sharing of cyber security information. In *Proceedings of 10th International Conference on Critical Infrastructure Protection*.

Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. *ACM Computing Surveys, 26*(1), 87-119.

Malone, T. W., Laubacher, R., & Dellarocas, C. (2010). The collective intelligence genome. *MIT Sloan Management Review, 51*(3), 21.

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: causal structure in theory and research. *Management Science, 34*(5), 583-598.

Mathiassen, L., Saarinen, T., Tuunanen, T., & Rossi, M. (2007). A contingency model for requirements development. *Journal of the Association for Information Systems, 8*(11), 569-597.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734.

Mingers, J. (2001). Combining IS research methods: Towards a pluralist methodology. *Information Systems Research, 12*(3), 240-259.

Mishra, A. N., Konana, P., & Barua, A. (2007). Antecedents and consequences of internet use in procurement: An empirical investigation of US manufacturing firms. *Information Systems Research, 18*(1), 103-120.

Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. *Information Systems Research, 26*(3), 565-584.

Mtsweni, J., Shozi, N. A., Matenche, K., Mutemwa, M., Mkhonto, N., & Jansen van Vuuren, J. (2016). Development of a semantic-enabled cybersecurity threat intelligence sharing model. In *Proceedings of the 11th International Conference on Cyber Warfare & Security.*

Murdoch, S., & Leaver, N. (2015). Anonymity vs. trust in cyber-security collaboration. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*.

Mutemwa, M., Mtsweni, J., & Mkhonto, N. (2017). Developing a cyber threat intelligence sharing platform for South African organisations. In *Proceedings of the Conference on Information Communication Technology and Society.*

Naghizadeh, P., & Liu, M. (2016). Inter-temporal incentives in security information sharing agreements. In *Proceedings of the Information Theory and Applications Workshop.*

NIST. (2014). *Framework for improving critical infrastructure cybersecurity*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

O'Neil, A. (2019). Australian Business Deans Council 2019 journal quality list review final report. *Australian Business Deans Council.* Retrieved from https://abdc.edu.au/wp-content/uploads/2020/03/abdc-2019-journal-quality-list-review-report-6-december-2019_2.pdf

Oliver, C. (1990). Determinants of interorganizational relationships: Integration and future directions. *Academy of Management Review, 15*(2), 241-265.

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking the "IT" in IT research—a call to theorizing the IT artifact. *Information Systems Research, 12*(2), 121-134.

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management, 52*(2), 183-199.

Pawson, R., Greenhalgh, T., Harvey, G., & Walshe, K. (2005). Realist review—a new method of systematic review designed for complex policy interventions. *Journal of Health Services Research & Policy, 10*(1), 21-34.

Pink, B., & Bascand, G. (2008). Australian and New Zealand standard research classification. Australian Bureau of Statistics. Retrieved from https://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/1297.02008?OpenDocument

Qamar, S., Anwar, Z., Rahman, M. A., Al-Shaer, E., & Chu, B.-T. (2017). Data-driven analytics for cyber-threat intelligence and information sharing. *Computers & Security, 67*, 35-58.

Rak, A. (2002). Information sharing in the cyber age: A key to critical infrastructure protection. *Information Security Technical Report, 7*(2), 50-56.

Rindova, V. P., Williamson, I. O., Petkova, A. P., & Sever, J. M. (2005). Being good or being known: An empirical examination of the dimensions, antecedents, and consequences of organizational reputation. *Academy of Management Journal, 48*(6), 1033-1049.

Ring, T. (2014). Threat intelligence: Why people don't share. *Computer Fraud & Security, 2014*(3), 5-9.

Robinson, N., & Disley, E. (2012). Incentives and challenges for information sharing in the context of network and information security. *ENISA*. Retrieved from https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing

Robson, M. J., Katsikeas, C. S., & Bello, D. C. (2008). Drivers and performance outcomes of trust in international strategic alliances: The role of organizational complexity. *Organization Science, 19*(4), 647-665.

Rogers, E. M., & Shoemaker, F. (1983). *Diffusion of innovation: A cross-cultural approach.* Free Press.

Salleh, K. A., & Janczewski, L. (2016). Technological, organizational and environmental security and privacy issues of big data: A literature review. *Procedia Computer Science, 100*, 19-28.

Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. In *Proceedings of 13th International Conference of Wirtschaftsinformatik*.

Schneier, B. (1998). *Security pitfalls in cryptography.* Retrieved from https://www.schneier.com/essays/archives/1998/01/security_pitfalls_in.html

Serrano, O., Dandurand, L., & Brown, S. (2014). On the design of a cyber security data sharing system. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*.

Shea, B. J., Grimshaw, J. M., Wells, G. A., Boers, M., Andersson, N., Hamel, C., & Bouter, L. M. (2007). Development of AMSTAR: A measurement tool to assess the methodological quality of systematic reviews. *BMC Medical Research Methodology, 7*.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information *Management & Computer Security, 8*(1), 31-41.

Skopik, F., & Li, Q. (2013). Trustworthy incident information sharing in social cyber defense alliances. In *Proceedings of 2013 IEEE Symposium on Computers and Communications.*

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security, 60*, 154-176.

Soh, C., & Markus, M. L. (1995). How IT creates business value: A process theory synthesis. In *Proceedings of 15th International Conference of Information Systems.*

Sommer, P., & Brown, I. (2011). Reducing systemic cybersecurity risk. *OECD*. Retrieved from https://www.oecd.org/gov/risk/46889922.pdf

Sutton, D. (2015). Trusted information sharing for cyber situational awareness. *Elektrotechnik und Informationstechnik, 132*(2), 113-116.

Takahashi, T., & Kadobayashi, Y. (2015). Reference ontology for cybersecurity operational information. *The Computer Journal*, *58*(10), 2297-2312.

Templier, M., & Paré, G. (2015). A framework for guiding and evaluating literature reviews. *Communications of the Association for Information Systems, 37*, 112-137.

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. (1990). *The processes of technological innovation. Issues in organization and management series.* Lexington Books.

Tosh, D. K., Molloy, M., Sengupta, S., Kamhoua, C. A., & Kwiat, K. A. (2015). Cyber-investment and cyber-information exchange decision modeling. In *Proceedings of 17th IEEE International Conference on High Performance Computing and Communications.*

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security, 72*, 212-233.

Truex, D., Holmström, J., & Keil, M. (2006). Theorizing in information systems research: A reflexive analysis of the adaptation of theory in information systems research. *Journal of the Association for Information Systems*, *7*(12), 797-821.

Van Deursen, N., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within health care. *Computers & Security, 37*, 31-45.

Vance, A., Lowry, P. B., & Wilson, D. W. (2017). Using trust and anonymity to expand the use of anonymizing systems that improve security across organizations. *Security Journal, 30*(3), 979-999.

Vázquez, D. F., Acosta, O. P., Spirito, C., Brown, S., & Reid, E. (2012). Conceptual framework for cyber defense information sharing within trust relationships. In *Proceedings of the 4th International Conference on Cyber Conflict.*

Veerasamy, N. (2017). Cyber threat intelligence exchange: A growing requirement. In *Proceedings of 16th European Conference on Cyber Warfare and Security*.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186-204.

Verizon. (2017). *Verizon data breach investigation report.* Retrieved from https://www.phishingbox.com/downloads/verizon-data-breach-investigations-report-dbir-2017.pdf

Wang, X., Brooks, S., & Sarker, S. (2015). A review of green IS research and directions for future studies. *Communications of the Association for Information Systems, 34,* 395-429.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2016). Foundations for an intelligence-driven information security risk-management system. *Journal of Information Technology Theory and Application, 17*(3), 25-51.

Weber, R. (2003). Theoretically speaking. *MIS Quarterly*, 27(3), iii-xii.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii-xxiii.

Willison, R., & Siponen, M. (2007). A critical assessment of IS security research between 1990-2004. In *Proceedings of 15th European Conference.*

Yang, T., & Maxwell, T. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly, 28*(2), 164-175.

Zhang, P., Li, N., Scialdone, M., & Carey, J. (2009). The intellectual advancement of human-computer interaction research: A critical assessment of the MIS literature (1990-2008). *AIS Transactions on Human-Computer Interaction, 1*(3), 55-107.

Zhao, W., & White, G. (2017). An evolution roadmap for community cyber security information sharing maturity model. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Zhu, K., & Kraemer, K. L. (2005). Post-adoption variations in usage and value of e-business by organizations: Cross-country evidence from the retail industry. *Information Systems Research, 16*(1), 61-84.

Appendix A: List of Journals from Research Disciplines not Indexed in the Scientific Databases Scopus, Web of Science, and ABI/Inform

Table A1. List of Journals by Research Discipline

Journal title*	Research disciplines (ANZRC)	Rating (2019)
Electronic Journal of IS Evaluation	Information systems	B
INFOR		B
Information Technology Management		B
Information, Communication & Society		A
INFORMS Journal on Applied Analytics		B
Journal of Community Informatics		B
Journal of Information Technology Theory and Application		A
Journal of Knowledge Management Practice		B
Pacific Asia Journal of the Association for Information Systems		B
The Information Management Journal		B
The Information Society		A
Academy of Management Discoveries	Business and management	A
Asia-Pacific Journal of Human Resources		B
Benchmarking: an international journal		B
Built Environment Project and Asset Management		B
Business Ethics: A European Review		B
Business Research Quarterly		B
Canadian Journal of Administrative Sciences		B
Canadian Public Policy		B
Journal of Global Business and Political Economy		B
E-Service Journal		B
Ethics: an international journal of social, political, and legal philosophy		A
European Journal of Sociology		A
Group Dynamics: Theory, Research and Practice		B
Human Resource Management (US)		A*
Industrial and Organizational Psychology: Perspectives on Science & Practice		B
Innovation: The European Journal of Social Sciences Research		B
International Journal of Logistics: Research and Applications		B
International Journal of Quality & Reliability Management		B
Journal of Global Mobility		B
Journal of Health, Organization and Management		B
Just Labour		B
Labour: Studies in Working Class History		B
Labour: Review of Labour Economics and Industrial Relations		B
Media Culture and Society		B
MIT Sloan Management Review		A
New Technology, Work & Employment		B
New Zealand Journal of Employment Relations		B
Pacific Affairs		B
Prometheus		B
Quality & Quantity		B
Relations Industrielles/Industrial Relations		B
Research Technology Management: International Journal of Research Management		A
Rutgers Business Review		B
Science, Technology, & Human Values		A
Strategy Science		A
The Milbank Quarterly		B
The Sociological Review		A
The TQM Journal		B
Voluntas: International Journal of Voluntary and Non-Profit Organizations		B
Written Communication		B

Table A1. List of Journals by Research Discipline

Journal title*	Research disciplines (ANZRC)	Rating (2019)
* For the Australian and New Zealand Standard Research Classification (ANZSRC), see http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1297.0Main%20Features32008?opendocument&tabname=Summary&prodno=1297.0&issue=2008&num=&view= For the 2018 Australian Business Deans Council (ABDC) journal quality list, see https://abdc.edu.au/wp-content/uploads/2019/01/abdc_journal_list_16052019-csv.xls		

Appendix B: An Author-centric View of Reviewed Papers

Table B1. Review of Cybersecurity Intelligence Sharing (CIS) Studies

#	Author(s)	Focus	Method	Theory	Unit of Analysis	Research objectives
1	Haass et al. (2015)	TOE framework	Case study	N/A	Organization	Review a case study for successful information sharing between the public and private sectors.
2	Murdoch & Leaver (2015)	Organisation and Inter-organizational trust	Case study	N/A	Organization	Investigate a case study of a cybersecurity intelligence sharing partnership across industry and the government in the United Kingdom.
3	Choraś (2013)	Technology	Conceptual framework	N/A	N/A	Present a technical framework for cybersecurity sharing with a focus on network security.
4	Brown et al. (2015)	Technology	N/A	N/A	Organization	Address technical challenges for threat intelligence sharing platforms.
5	Kokkonen et al. (2016)	Technology	Conceptual model	N/A	Organization	Propose a model for sharing cybersecurity.
6	Luiijf & Klaver (2015)	Strategy, tactical and organizational	Analytical Framework	N/A	Individual	Propose a three-level analytic framework for CIS.
7	Fisk et al. (2015)	Technology	N/A	N/A	Organization	Investigate technical principles for a secure CIS across organizations.
8	Greiman (2015)	Environment (legislation)	Conceptual framework (interview)	N/A	Organization	Explore the issues for security partnerships between government and private sector.
9	Takahashi & Kadobayashi (2015)	Technology	Conceptual Taxonomy	N/A	N/A	Address a reference ontology for cybersecurity collaboration between organisations.
10	Lee & Rao (2007)	Technology, Organization, and Environment	Quantitative method (survey)	Exchange theory, transaction cost, and IT acceptance theory	Information systems	Investigate the socio-technical factors that influence acceptance of anti/counter-terrorism information sharing systems across federal agencies in the US.
11	Kampanakis (2014)	Technology	Models/Standards for CIS	N/A	N/A	Summarize various threat intelligence sharing models
12	Dandurand & Serrano (2013)	Technology	Conceptual framework	N/A	N/A	Provide a knowledge management tool “CDXI” to facilitate CIS
13	Fransen et al. (2015)	Technology	Conceptual framework	N/A	Organization	Investigate how national cybersecurity centers (NCSC) can leverage CIS infrastructure.
14	Skopik et al. (2016)	Technology, organization, and environment	Conceptual Model	N/A	Organization	Suggest dimensions for CIS across organizations.
15	Jasper (2017)	Technology	Conceptual framework	N//A	Organization	Discuss existing CIS frameworks across agencies in the United States.
16	Gal-Or & Ghose (2005)	Economic	Mathematical model	Game theory	Organization	Develop a model to understand the benefits firms received from participating in information sharing operations.
17	Appan & Bacic (2016)	Economic	Quantitative method (survey)	Relational view of the firm	Organization	Investigate whether CIS influences a firm’s financial performance.
18	Sutton (2014)	Governance	Conceptual model	N/A	Organization	Investigate trust factors for information exchange.
19	Liu et al. (2014)	Economic	Mathematical model	Game theory	Organization	Develop a model to examine information sharing network policies and their impacts.

20	Ring (2014)	Technology, Organization, and Environment	Non-academic interview	N/A	N/A	Investigate why the organization does not share cyber threat information.
21	Hernandez-Ardieta et al. (2013)	Technology	Mathematical model	Graph theory	Organization	Propose a model for information security sharing.
22	Serrano et al. (2014)	Technology	Conceptual model	N/A	Organization	Propose a technical solution to develop CIS platforms.
23	Naghizadeh & Liu (2016)	Economic	Mathematical model	Game theory	Organization	Present a game-centric model of information sharing agreements across firms.
24	Kantola & Jatiner (2016)	Technology	N/A	N/A	Organization	Address the benefits of incident sharing and present an overview of responsive cyber defense.
25	Skopik & Li (2013)	Organization and Environment	Conceptual model	N/A	Organization	Introduce the concept of the social cybersecurity defense alliance to increase the efficiency of cybersecurity incident sharing.
26	Mtsweni et al. (2016)	Technology	Conceptual framework	N/A	Organization	Propose a semantic-enabled sharing model for exchanging timely and relevant cybersecurity intelligence with trusted collaborators.
27	Veerasamy (2017)	Technology and Organization	Conceptual framework	N/A	Organization	Present a framework that includes the source of data, tools, and skills required to encompass influential challenges in the CIS area.
28	de Fuentes et al. (2017)	Technology	Conceptual model	N/A	Organization	Introduce a scheme for CIS networks. The proposed schema leverages the STIX standard.
29	Vance et al. (2017)	Technology and Organization	Simulation experiment	Theory of reasoned action (TRA)	Individual	Investigate the factors that influence the adoption of anonymizing systems for CIS.
30	Mutemwa et al. (2017)	Technology	Conceptual model and platform	N/A	Organization	Address a conceptual CIS model and platforms to aggregate, analyze, and share actionable cybersecurity threat intelligence.
31	Tosh et al. (2015)	Technology and Finance	Mathematical model	Game Theory	Organization	Investigate incentives and cost associated with CIS.
32	Rak (2002)	Technology, Organization, and Environment	N/A	N/A	Organization	Address the successes and impediments for CIS program in critical U.S. infrastructures.
33	Vázquez el al. (2012)	Technology, Organization, and Environment	Conceptual framework	N/A	Organization	Investigate incentives and challenges for CIS.
34	Johnson et al. (2016)	Technology and Organization	N/A	N/A	Organization	NIST: provide guidelines for developing and participating in cybersecurity intelligence sharing relationships.
35	Robinson & Disley (2010)	Technology, Organization, and Environment	Qualitative method (Interview and Delphi)	N/A	Organization	ENISA: investigate barriers and incentives for information exchange (IE) and information sharing analysis centers (ISACs).
36	Goodwin et al. (2015)	N/A	N/A	N/A	Organization	Microsoft best practice for CIS.

37	ENISA (2016)	Technology, Organization, and Environment	N/A	N/A	Organization	ENISA: address initiatives on sharing of cyber incidents in the energy sector.
38	Barnum (2012)	Technology	Standard	N/A	N/A	MITRE: introduce STIX as a collaborative community-driven effort standard for representing structured threat information and sharing across participants.
39	Tounsi & Rais (2018)	Technology	Survey on technical threat intelligence	N/A	N/A	Classify different existing technologies for CIS.
40	Lewis et al. (2014)	Technology and Organization	Quantitative (scenario-based survey)	N/A	Organization	Propose a taxonomy for CIS for identifying risk exposure across small and medium-sized enterprises (SMEs).
41	Zhao & White (2017)	Technology and Organization	Conceptual framework	N/A	Organization	Present a collaborative information sharing framework to improve community cybersecurity practices and develop an information-sharing maturity model for community organizations.
42	Sauerwein et al. (2017)	Technology	Quantitative method	N/A	Intelligence sharing platform	Conduct a systematic review of the software landscape of 22 CIS platforms and identify their gaps.
43	Chismon & Rukes (2015)	UK CERT	Conceptual framework	N/A	Organization	Present a framework for threat intelligence in organizations.
44	Ludwick et al. (2013)	Technology and Organization	Conceptual Framework and survey	N/A	Organization	Study the state of practice in cybersecurity intelligence to advance the capabilities of organizations and provide practical solutions to common challenges.
45	Borum et al. (2014)	Organization	Research literature	N/A	Organization	Highlight the role of cybersecurity intelligence to support risk-informed decision making for improving policies, architecture, and investment in the cyber domain.
46	Webb et al. (2016)	Organization	Design science and Focus Group validation	Situation Awareness Theory		Develop an intelligence-driven security risk management system.

Appendix C: Cybersecurity Intelligence Sharing Standards

Table C1. Standards, Frameworks, and Protocol for CIS

Abbrev.	Name	Description	Type	Adoption	Standard Organization
STIX	Structured threat information expression	A structured language for representing structured cybersecurity threat information	Language and Schema	Extensive	MITRE
TAXII	Trusted automated exchange of indicator information	A standard for transporting cybersecurity intelligence	Standard-Protocol	Extensive	MITRE
CYBOX	Cyber observable expression	Threat events and machine property representation	Language-Dictionary	Extensive	MITRE
CAPEC	Common attack pattern enumeration and classification	Attack pattern description	Language-Dictionary	Moderate	ITU
MAEC	Malware attribute enumeration and characterization	Malware attack representation	Language-Dictionary	Moderate	ITU
IODEF	Incident object description exchange format	A standard for sharing cyber incident information	Language and Schema	Extensive	IETF
RID	Real-time inter-network defense	A standard for transportation of cyber incident	Standard-Protocol	Moderate	IETF
OVAL	Open vulnerability and assessment language	System information and state representation and assessment reporting	Language-Dictionary	Extensive	ITU
XCCDF	Extensible configuration checklist description format	Security checklist and benchmark representation	Language and Schema	Moderate	NIST
CPE	Common platform enumeration	Hardware and Software asset description and identification	Language-Dictionary	Moderate	NIST
CVE	Common vulnerabilities and exposures	Public security vulnerability and exposure dictionary	Language-Dictionary	Extensive	ITU
CVSS	Common vulnerability scoring system	Security vulnerability scoring system	Language-Dictionary	Extensive	ITU
CCE	Common configuration enumeration	Security configuration issue dictionary	Language-Dictionary	Limited	NIST
CWE	Common Weakness enumeration	Common software weakness dictionary	Language-Dictionary	Moderate	ITU
CWSS	Common weakness scoring system	Software weakness scoring system	Language-Dictionary	Moderate	MITRE
SCAP	Security content automation protocol	A framework consisting of various specifications for sharing CIS	Standard	Extensive	NIST
CVRF	Common vulnerability reporting framework	A framework for the classification of vulnerability	Standard-Language	Moderate	ICASI
OpenIOC	Open indicators of compromise	A language for describing indicators of compromise	Standard-Language	Extensive	Mandiant
YARA	YARA	A standard for incident	Standard-	N/A	Virustotal

		reporting and analysis	Language		
VERIS	Vocabulary for event recording and incident sharing	A standard for malware property and packet representation	Standard-Language	Limited	Verizon
CDXI	Cyber security data exchange and collaboration infrastructure	A knowledge management tool for CIS	Knowledge management framework	Limited	NATO
CYBEX	Cyber security information exchange framework	A standard for exchanging cybersecurity intelligence	Standard-Framework	Limited	ITU
CIF	Collective intelligence framework	A framework for combining malicious threat information from various sources.	Standard-Framework	N/A	N/A

Appendix D: Definition of Identified Factors and Application of Theories

Table D1. Defining Identified Factors based on the TOE Framework

Identified factors	Definition(s)/explanation(s)
Information quality	Refers to accuracy (confidence information), timeliness, traceability, and relevancy of collected cybersecurity intelligence (Brown et al., 2015).
Information confidentiality (technology)	Refers to technology-related sensitive and confidential/classified information (e.g., internal IP addresses, server names and descriptions, or services) whose disclosure can result in financial or reputational loss (Johnson et al., 2016; Kampanakis, 2014; Lee & Rao 2007).
Cybersecurity standards	Refers to standardization efforts to address the challenges in representing cybersecurity information using standardized language (Brown, et al., 2015; Fransen et al., 2015) and facilitate cybersecurity information exchange across an organization (Dandurand et al., 2013).
CI operation complexity	Refers to the degree to which organizations perceive participation in CIS operations as a relatively difficult process (Dandurand et al., 2013).
Technology integration and interoperability	Refers to the extent to which an organization's cyber technologies can readily connect and exchange cyber intelligence with other internal and external systems without any restriction (Jasper, 2017; Johnson et al., 2016).
Infrastructure quality	Refers to the quality and maturity of existing cyber-infrastructure in an organization that can facilitate the CIS technology adoption (Vance et al., 2015).
Incident response	Refers to an organization's ability to respond to a cybersecurity threat due to adopting and/or participating in CIS practices with other organizations (Haass et al., 2015).
Technology cost	Refers to the technology-adoption costs that arise in planning, implementing, and maintaining cybersecurity intelligence-driven practices in an organization (Skopik et al., 2014).
Education	Individual-level cybersecurity intelligence awareness, training, and education required to deliver and manage cybersecurity intelligence-led operations that CIS practices require (Kolini & Janczewski, 2015). Organizations should provide the necessary training funding for ongoing operational support for data collection, enrichment, analysis, and dissemination to other organizations (Johnson et al., 2016).
Organizational cost	Refers to an organization's decision to participate in CIS practices according to a business case that incorporates all organizational benefits and costs associated with CIS operations.
Information confidentiality	Refers to confidential and sensitive information such as intellectual property (IP), personal information, and client information (Fisk et al. 2015; Kokkonen et al. 2016) whose loss may result in financial loss or reputational damage.
Organizational performance	The extent to which deploying cyber intelligence-led operations impacts organizational performance when cybersecurity risks and events occur (Dandurand & Serrano, 2013; Furneaux & Wade, 2011).
Organizational cyber readiness	An organization's ability to maximize its potential to use cybersecurity intelligence while minimizing how much it costs to run its cybersecurity intelligence operation.
Data-sharing model	Refers to available or existing data-sharing models for exchanging cyber intelligence CIS. For example, organizations can develop their data-sharing models based on a common and acceptable standard (i.e. STIX and TAXII) for CIS practices (Kokkonen et al., 2016).
Organizational culture	The extent to which an organization can instill a culture that fosters sharing cybersecurity intelligence regardless of whether it buys intelligence, gets it for free, or rents it through a managed service (Ring, 2014).
Organizational structure	Refers to the structure of an organization that facilitates CIS (Qin & Fan, 2016).
Skilled technical resources	Refers to the technical expertise and experience required to deploy and maintain CIS operations in an organization (ENISA, 2016).
Top management support	Refers to the commitment and support from top management and executive board members towards providing an environment that encourages participation in CIS with other organizations (Akbulut, 2003).

Table D1. Defining Identified Factors based on the TOE Framework

Data governance	Refers to practices that govern and control data and information use and to problems with validating data quality (Dandurand & Serrano, 2013).

Table D2. Application of Theories for CIS Studies

Theory name	Applications of theories in CIS studies
Diffusion of innovation (DOI) (Rogers & Shoemaker 1983)	Explains an organization's willingness to accept and adopt new ideas, processes, or innovative technologies. In the CIS context, the theory explains how and why organizations decide to adopt and implement CIS technologies and processes.
Critical mass theory (CMT) (Bouchard, 1993)	Explains that an organization's decision regarding the adoption of CIS operations depends on perceptions of other organizations' actions (i.e., "bandwagon effect").
Social exchange theory (SET) (Hallen et al., 1991)	Explains how relationships between organizations form in CIS through a non-economic aspect (e.g., power, trust, and interdependency) lens.
Inter-organizational relationships (IOR) (Oliver, 1990)	Investigates the contingencies of inter-organizational relationship formation in the CIS context. The theory examines the interaction of six contingencies to predict IOR formation.
A general theory of network governance (GTN) (Jones et al., 1997)	Explains under which conditions the network's governance is likely emerged and addressed social mechanisms that allow network governance to coordinate and safeguard customized exchange in the market.
Resource dependence theory (RDT) (Casciaro & Piskorski, 2005)	Explains interfirm relationships when the potential for mutual resource dependency in CIS exists.
Technology acceptance model (TAM) (Venkatesh & Davis, 2000)	Explains that the perceived usefulness and ease of use of cybersecurity intelligence technologies and procedures may influence an organization's intention to adopt such technologies.

About the Authors

Farzan Kolini is a PhD student in the Department of Information Systems at the University of Auckland, New Zealand. His research interests include cybersecurity intelligence sharing, threat intelligence, phishing and email security, and national cybersecurity strategies. His work has been published in journals and conferences such as *Journal of Computer Information Systems*, the Pacific Asia Conference on Information Systems, and the Australian Conference on Information Systems. He has worked in cybersecurity for more than ten years with different organizations such as Deloitte.

Lech Janczewski (MEng, MASc, DEng) has over 50 years' experience in information technology. He is Associate Professor at the University of Auckland, Department of Information Systems and Operations Management. His area of research includes management of IS resources with the special emphasis on data security. He wrote above 400 publications presented in scientific journals, conference proceedings and books. He is the chairperson of the New Zealand Information Security Forum, Fellow of the Institute of IT Professionals NZ (former NZ Computer Society), and Secretary of the IFIP's Technical Committee 11 on Security and Privacy Protection in Information Processing Systems.