2017

Two Heads are Better than One: A Theoretical Model for Cybersecurity Intelligence Sharing (CIS) between Organisations

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

Two Heads are Better than One: A Theoretical Model for Cybersecurity Intelligence Sharing (CIS) between Organisations

Farzan Kolini
Department of Information Systems and Operation Management (ISOM)
The Business School
University of Auckland, New Zealand
F.kolini@aucklnad.ac.nz

Lech Janczewski
Department of Information Systems and Operation Management (ISOM)
The Business School
University of Auckland, New Zealand
L.janczewski@aukland.ac.nz

Abstract

The cyber threat landscape is constantly evolving with new vulnerabilities and zero-day threats. Cyber-attacks exploiting these vulnerabilities are increasing on a global scale, leading to significant loss to the world economy. A common need among organisations is to share early warnings and advice about different types of cyber threat intelligence. Cybersecurity Intelligence Sharing (CIS) has the potential to help organisations to gain an overarching view of attackers' intentions, behaviours, and tactics in order to define specific courses of actions in a timely manner, and ultimately to build a certain level of cyber situational awareness. Although CIS has been recently receiving more attention from organisations, the level of participation in CIS practices is not satisfactory. Besides, there is not enough information about the factors that are antecedent to CIS operations in an organisational context. Considering all these, this study proposes a theoretical model to investigate technical and non-technical determinant factors that influence organisations to adopt or participate in cyber intelligence sharing with their peers. Diffusion of Innovation (DOI) and Inter-organisational Relationships (IOR) theories are employed in a TOE framework to build an integrative model to better understand technological, organisational, interorganisational, and environmental factors in CIS.

Keywords Cybersecurity, Intelligence sharing, Threat information, TOE framework, Diffusion of innovation, Interorganisational relationships

1 Introduction

In recent years, there has been a growing interest in questions about how cybersecurity intelligence and information sharing (CIS) can help organizations including governmental agencies to mitigate the risk of cyber threats. A common need among organisations is to share discrete information about cyber attackers, victims, incidents, and vulnerabilities (Kolini & Janczewski 2015). An ultimate goal is to discover and disseminate solutions to these cyber threats and decrease the time between the discovery of zero-day exploits or vulnerabilities when a specific course of action against those threats is initiated (Burger et al. 2014). Although a number of new information sharing platforms have emerged on the internet, it now appears that many of these platforms offer only a general cyber threat information without providing in-depth knowledge, accurate information, attributes of attacks, or actionable solutions. Moreover, in many instances, cybersecurity threat intelligence cannot be found in the open web due to confidentiality of this information such as personally identifiable information (PII), and intellectual and reputational information. For instance, in 2015 and 2016 a series of cyber-attacks against SWIFT payment networks were reported, with the theft of millions of dollars (Verizon 2017). The financial institutions which has been the target of this attack failed to share the cyber incident information with their peers in other banks, resulting in attackers using the same approach to compromise other banks across the globe. This is one instance of unsuccessful cybersecurity information sharing (CIS) between organisations with hundreds of millions of dollar loss and substantial reputational damage to the banking community.

Existing cybersecurity research has not extensively explored the interdisciplinary aspects of CIS. To date, the CIS research has been mostly about the technical aspect of cybersecurity intelligence in organisations (Barnum 2002; Burger et al. 2014; Dandurand et al. 2013; Fernandez et al. 2012; Skopik et al. 2016; Brown et al. 2015). The field has yet to examine the other aspects of CIS including organisational, interorganisational, and environmental factors that influence an organisation to not participate in CIS practices. In this study, we attempt to extend our focus on the interdisciplinary study of cybersecurity. The interdisciplinary study draws on a variety of disciplines including information systems, computer science, organization and management science, and law. One of the challenges is grounded in the fact that interdisciplinary study of cybersecurity is complex by its nature and many researchers whose efforts can benefit the field are not yet aware of each other's contributions. Thus, the field suffers from alike of scientific rigour and coherence that is not yet present in the field. Consequently, the cybersecurity field is a collection of puzzling analogies, scattered results, and partial frameworks.

In this study, we shed more light into the dark side of CIS by exploring the implications of diffusion of innovation theory, interorganisational relationships theory, and a TOE framework to build a conceptual model of the antecedents in the CIS domain. The remainder of this paper is structured as follows. Section 2 presents the literature review and research questions. Section 3 addresses of theoretical background. After which we discuss the proposed hypotheses. Section 5 articulates the research method which is followed by the conclusion.

2 Research Gaps & Research Questions

In many recent studies, the notion of intelligence has often been used interchangeably with the concept of information or data. Although there are similarities between these terms, intelligence differs from information and data. In this study cybersecurity intelligence refers to verified, correlated, enriched, combined, and contextualized information that can be used for timely incident response or to advise decision makers. This definition is partially adapted from the traditional literature on intelligence where intelligence was presented as the collection and analysis of open, public or secret information related to attributes of other actors or their behaviours(Hilsman, 1952; Herman, 1966). The Carnegie Mellon Software Engineering Institute defines cyber intelligence as "the acquisition and analysis of information to identify, track and predict cyber capabilities, intention and activities that offer courses of action to enhance decision-making. Individuals and organisations can use cyber intelligence to reduce uncertainty and to draw conclusions about attributes of a cyber-attack or cyber actors, tactics, techniques and procedures (TTP), which are not directly observable (Kolini & Janczewski 2017; Brown et al. 2015). For instance, cyber intelligence can be generated by verifying, analysing, correlating contextualizing of information that is obtained from various technological security tools such as Firewall, Intrusion Detection and Prevention Systems (IDS/IPS), Anti-Viruses, Security Incident and Event Management (SIEM) Systems, Data Integrity and Access Management tools, and System Logs (Syslog Server).

The complexity of cybersecurity operations has made it ultimately impossible for any organization to protect the cyber assets appropriately without collaboration with other entities. Therefore, a sustained CIS can reinforce the understanding of the cyber threat landscape and assist the sharing parties with a timely attack detection, response, and risk mitigation capability. Although considerable strides have been made in this area, there is not too much inter-organisational experience in sharing of cybersecurity intelligence (ENISA 2013). The key challenge here is that CIS operations required overarching multidisciplinary studies to understand technical and non-technical determinants that influence participation in CIS practices. Therefore, this research aimed to investigate the following research questions:

1. How do technology, organisational, inter-organisational and environmental factors influence organisational participation in cybersecurity intelligence sharing between public and private sectors?
2. What might explain differences in engagement in CIS operations?
3. How to encourage organisations to participate in CIS?

3 Theoretical Background

3.1 Technology, Organisation, Environment (TOE) Framework

Building upon the TOE framework, which posits that IS-related decisions are influenced by three broad categories-Technology, Organisation, and Environment- which collectively impact innovation adoption and use in organisations (Depietro et al., 1990). In contrast to many other IS theories, the TOE framework does not offer a robust theoretical background to establish causal relationships. However, the TOE's simplicity and the breadth of attributes motivate IS researchers to decompose and combine these attributes with other IS theories (Mishra et al., 2007). Following this framework, we aim to investigate factors that holistically capture the relevant state-of-the-art in the domain of Cybersecurity Intelligence Sharing (CIS). This research project argues that public and private sector engagement in CIS operations will not only be influenced by technical determinants and organisational, inter-organisational, and environmental factors are needed to be considered equally important for investigation and analysis.

Technology in this context may refer to infrastructure, tools, and protocols that are selected on the technical layer and set into operation by adaptor firm. Hence, it is essential that selected technology fit into existing technologies and is compatible with organisational processes and operating model. Organisational context can be denoted by internal characteristics of a firm that might impact participation in CIS. A number of organisational characteristics such as management support, organisational strategies, culture, size , operational costs, quality of human resource have been scrutinised by IS scholars (Kelly et al. 1999; Tornatzky & Fleischer 1990; Chau & Tam 1997; Zhu & Kraemer 2005)) will also be considered for research project. The environmental context refers to the characteristic of the external environment in which public and private firms operate. Previous studies in the cyber domain have shown that the influence of international institutions such as CERTs or NATO, as well as the legal and regulatory requirements (Kolini & Janczewski 2017) cannot be ignored. Since this study primarily aims to understand what factors contribute to participation in CIS, our proposed model does not seek to investigate interactions between elements in our proposed theoretical model. We acknowledge that while such interaction is conceivable, our immediate purpose at this stage is to investigate important direct effects of combined TOE framework, diffusion of innovation theory (DOI), and inter-organisational relationships theory (IOR) on CIS.

3.2 Diffusion of Innovation (DOI) Theory

An organisational innovation can be defined as a technology, structure, process, practice, new vision or behaviour new to the organisation adopting it (Roger & Shoemaker 1983; Swanson 2004). Diffusion is the process by which an innovation spreads among different organisations (Wang 2010). Since the adoption of cooperative information sharing capabilities require new technologies, processes, and resources and incur economical cost, CIS operation is still scarce among organisations (Hausken 2007). Thus, this study is an initial attempt to investigate the factors that encourage organisation in the adoption of new technologies for CIS practices. Roger and Shoemaker (1983) identified five different attributes that influenced the adoption of technology innovation in organisations. These elements include relative advantage, compatibility, complexity, observability, tractability. Other studies found that noted that cost, Image, and voluntariness are other attributes which are not considered by Rogers's study (Tornatzky & Klein 1982; Moore & Benbasat 1991). Since DOI theory emphasized on the technological aspects as well the internal and external characteristics of an organisation (Rogers 1995),

it can be appropriately combined with the TOE framework to study technology or organisational factors that influence CIS operations. This approach is consistent with the extant literature (Kuan & Chau 2001; Zhu et al. 2006; Lin et al. 2008).

3.3 Inter-organisational Relationships (IOR) Theory

Another determinant that can influence the CIS operations is the formation of relationships and collaboration between various organisations. While intelligence sharing can enable organisations to benefit from coordinated and timely incident responses, there is no significant effort placed on such inter-organisational collaboration (Robinson 2012). We perceive that in order to better understand factors that contribute to an effective inter-organisational CIS collaborations, we may need to investigate attributes that are required to maintain sustainable relationships among organisations. Previous studies suggested that sharing of all types of knowledge or information, including cybersecurity information, required complex interactions between participating organisations because of key differences in their culture, value or origins (Yang & Maxwell 2011). Bouchard (1993) pointed out, an organisation's attitude towards engagement in collaborative operation is based on what their business partners are doing and not the characteristic of innovation or technology. In an effort to integrate underlying determinants of IOR's literature, Oliver (1990) proposed six types of contingencies that are central to the formation of relationships among organisations. These six contingencies included necessity, asymmetry, reciprocity, efficiency, stability and legitimacy.

Since CIS has offered certain operational effectiveness, benefits, and values for organisations (Johnson et al. 2016), IOR theory can be used as an appropriate lens to understand the contingencies that motivate organisations to enter into relationships for the purpose of CIS operations. Furthermore, understanding these factors can help governments to incentivise public-private partnerships in management and protection of cyber-critical infrastructures.

4 The Research Model and Hypotheses Development

In this section, we propose our research framework and hypotheses by synthesizing the TOE framework, diffusion of innovation (DOI) theory, and Inter-organisational relationships (IOR) to investigate the factors that influence organisational participation in CIS. We drew upon the TOE framework to posit that the non-technological factors in CIS practices including organisation, inter-organisation, and environment should be considered equally important as technological requirements. A typical goal of cyber intelligence technology is to establish a platform with multiple sources of intelligence, enriching and combining data, and finally delivery of aggregated intelligence into organisational workflows and into decision-making procedures.

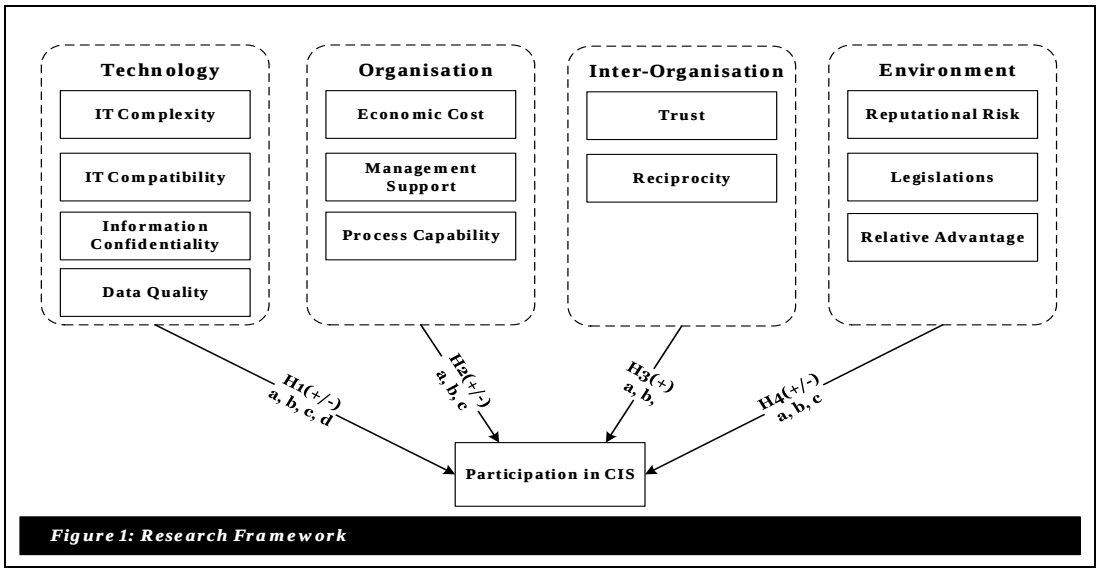

Figure 1: Research Framework

4.1 Technological Factors

4.1.1 IT Compatibility and IT Complexity

We drew upon DOI theory to specify that complexity of cyber intelligence operations and compatibility with organisational IT systems are among factors that influence CIS operations. While complexity refers

to the degree to which participation in CIS with other organisations is perceived to be a complex operation, IT compatibility focuses on perceived compatibility of existing IT systems, protocols and standards with CIS requirements. To cope with the growing amount of data that needs to be handled in a complex cyber intelligence operation, human resources are not sufficient anymore. Therefore, IT systems that enable automation of a cyber intelligence operation are fundamental for CIS practices. Several technical standards including MITRE's STIX, CybOX, and TAXII (Barnum 2012), ITU's CYBEX (Rutkowski et al. 2010), or NATO's CDXI (Dandurand & Serrano 2013) are currently used by agencies and organisations. However, compatibility of infrastructure, software, and communication protocols of these standards with the organisation current technology is crucial in participation in CIS (Skopik et al. 2016). Thus, it is hypothesized that:

> H1a: Perceived complexity of CIS operation will have a negative effect on organisational participation in CIS.
>
> H1b: Perceived IT compatibility will have a positive effect on organisation participation in CIS.

4.1.2 Confidentiality and Data Quality

Information confidentiality refers to organisation's sensitive information or personally identifiable information (PII) that disclosure of which can result in financial loss, reputational damage, or legal action (Johnson et al. 2016).Sharing of cybersecurity intelligence such as security logs, scan results or IP addresses may expose personal information or defensive capabilities of an organisation. Organisations should implement data classification and handling standards to actively anonymize or remove any information identifying the source of information shared with other organisations. Murdoch (2015) posited that anonymity and data handling could encourage participation in cybersecurity collaboration. Gil-Garcia (2005) and Landsbergen (2001) suggested that information privacy and confidentiality are significant issues for inter-governmental collaborations.

The quality of information is another key requirement for CIS operations. For instance, increased productivity, accuracy and timeliness of collected intelligence, reduced duplicate data collection, and increased relevancy of information are among those benefits that can be achieved by participating in CIS operations (Gil-Garcia et al. 2007; Brown et al. 2015; Robinson 2012). Considering all these, we present the following hypotheses:

> H1c: Perceived confidentiality and anonymity of information will have a positive effect on organisational participation in CIS.
>
> H1d: Quality of cyber intelligence information will have a positive effect on organisational participation.

4.2 Organisational Factors

4.2.1 Economic Costs

Economic cost refers to perceived potential costs of participating in CIS operations. The cost of CIS is primarily related to infrastructure, communication, operations and human resources costs. Although some studies suggested that CIS can offer some economic advantage (Gal-Or and Ghose 2005; Robinson 2012), other major studies advocated that there are significant constraints in respect to the feasibility of cost contribution, especially when the benefit of such operation is not well-defined (Gil-Garcia et al. 2007; Fan et al. 2014; Lips et al. 2011). Hence,

> H2a: Economic costs of CIS will have a negative effect on organisational participation in CIS operations.

4.2.2 Management Support

Top Management support denoted the commitment of senior management and key stakeholders by providing vision, guidance, and resource to initiate and sustain participation in CIS (Akbulut et al. 2009). Top management involvement can encourage organisations for the adoption of IT systems and platforms that are required for CIS initiatives (Grover 1993). Hence, we can propose:

> H2b: Senior management support and commitment will have of positive effect on organisational participation in CIS.

4.2.3 Process Capability

Organisation process capability refers to the availability of operating procedures and knowledge within an organisation that could facilitate participation in CIS. Many organisations developed and owned their

distinct operating models, procedures, and work flows, which can impede engagement in CIS operation (Yang and Maxwell 2011). Since the adoption of a cyber-intelligence-based operations is relatively new in organisations, diverse maturity levels are expected from organisations. In a mature organisation the cyber intelligence is the process by which intelligence strategy, process, and objectives are embedded into the organisational structure (Brown et al. 2015). This type of organisation may participate in CIS to manage the flow of valuable cyber intelligence and feed them into their organisational process to help decision maker and practitioner. As a result, we can argue that:

H2c: Organisational process capability will have a positive effect on participation in CIS.

4.3 Inter-Organisational Factors

4.3.1 Inter-organisational Trust

The literature suggests that inter-organisational trust is an enabler for information sharing across organisations. Hart and Saunders (1997) articulated that trust provided an agency with an optimistic anticipation of the benevolent behaviour of another entity in inter-organisational relationships. In cybersecurity, Vazquez and Brown (2012) identified two key components of trust in CIS operation: trust in the CIS network, and trust in other participants as their relationships strengthen However, Inter-organisational trust can be attenuated in the case of information misuse, loss of autonomy, and lack of secure communications (Faerman et al. 2001). Based on the extant literature we propose that:

H3a: Inter-Organisational trust will have a positive effect on organisation participation in CIS .

H3b: Trust in CIS network will have a positive effect on organisation participation in CIS with other organisations.

4.3.2 Reciprocity

The IOR theory pinpointed that interagency reciprocity is one of the elements that can build inter-agency relationships. In Literature reciprocity denotes as cooperation, collaboration, and cooperation among organisations rather than organisational domination, control, and power. Besides, reciprocity can be achieved for the purpose of the pursuing common or mutually beneficial goals or interests (Oliver 1990). In order to achieve the desired effect of early warning and improved detection of cybersecurity threat reciprocity is an important factor to enforce information sharing among organisations(Rak 2002; Constant et al. 1994).

An important enabler of reciprocity is the commitment of organisations to bilateral and multilateral cyber information sharing operations. At this stage engagement in CIS operation is completely voluntary and, therefore, a contractual obligation is not present to define and enforce the minimum CIS commitment requirement. For instance, in many instances public and governmental organisations do not stand by their CIS's commitment due to confidentiality concern. Therefore, we posit:

H3c: Perceived reciprocity of information will have a positive effect on organisation participation in CIS.

4.4 Environmental Factors

4.4.1 Reputational Risk

Reputational risk often arises as a result of loss resulting from damage to an organisation's reputation. There are several risks associated with CIS primarily due to disseminating valuable cybersecurity intelligence to another organisation. Once this information has been shared by an organisation, there would be no full control over the propagation of this information with other parties, which may result in damage to the reputation of an organisation (Akbulut 2009). Furthermore, since this information is highly sensitive, it might result in privacy issues and consequently severe reputation risks. Considering all these points, we perceive that:

H4a: Reputational risk will have a negative impact on organisational participation in CIS.

4.4.2 Legal and Policy Framework

Previous studies suggested that legal and policy frameworks either have a positive influence on the sharing of information or create barriers for inter-organisation information sharing (Gil-Garcia & Pedro 200; Yang and Maxwell 2011). The concern that disclosure of cyber-breach may lead to legal action against an organisation participating in CIS is a significant barrier for CIS operations (Robinson & Disley 2012). Legal liability is another challenge that may impede collaboration in CIS. At present, It is

not clear whether it would be an increased legal liability for an organisation that has received Cyber intelligence but has not applied it (Haass et al. 2015). Thus, we propose that

> H4b: Legal and policy framework uncertainties will have a negative effect on organisational participation in CIS.

4.4.3 Image

Drawing on the DOI theory the image refers to the degree to which use of an innovation, in this case participation in CIS, is perceived to enhance an organisation's image in a social system (Moore & Benbasat 1991). Roger (2010 subsumed the image as an aspect of relative advantage. However other researchers (Tornatzky and Klein 1982) found the effect of the image is different from relative advantage, therefore, it can be investigated as separate attributes. Since there are still significant concerns around laws and legislation that could preserve citizens' privacy and confidentiality, organisations who engaged in sharing of cybersecurity information will be received more affection from public and society.(Clarkson et al. 2007). Therefore we presume that:

> H4c: Concern over public image of organisation will have negative effect on organisation participation in CIS with other organisations.

5 Research Design

This study employs a quantitative study designed to test the theoretical model of CIS through the evaluation of TOE factors that may influence organisational participation. We will design a data collection instrument, where the constructs will be operationalised using measures form validated instrument. The selected instruments are modified to fit with this research design. The target recipients of the survey are organisational employees who are responsible for cybersecurity practices across the organisation. We also plan to conduct a pilot study to evaluate and refine the measurement instrument. Since data collection and statistical analysis will be conducted at the organisational level, the unit of analysis will be an organisation. In order to validate this study instrument, we will examine construct reliability, convergent validity, and discriminant validity for all designed constructs. Moreover, we will measure the common method bias by using Herman's single-factor test (Podsakoff et al. 2003). We will apply a structural equation modelling (SEM) for measuring the statistical significance and regression analysis.

6 Conclusion

Most other studies investigate the technological constraints that influence sharing of cybersecurity, therefore, this study aimed to adopt a broader TOE framework to investigate non-technical factors including organisational, inter-organisational and environmental factors that potentially influence CIS operations. Drawing on DOI and IOR theories we have designed our theoretical framework which will be examined through quantitative study. To our best knowledge, this study is one of the first attempts to explore cybersecurity intelligence sharing at the organisational level. Moreover, we seek to identify factors that impede organisational participation in sustained cybersecurity intelligence sharing practices. Among other contributions, this study aims to add to the body of literature on multidisciplinary cybersecurity research. One potential limitation of this study is that we did not consider the individual expectation of CIS operations in our proposed model. We assume that organisational factors would have a strong influence in shaping employees attitude towards CIS operation (Yang & Maxwell 2010). Hence, we intentionally exclude them from this study.

7 References

Akbulut, A. Y., Kelle, P., Pawlowski, S. D., Schneider, H., & Looney, C. A. (2009). To share or not to share? Examining the factors influencing local agency electronic information sharing. *International Journal of Business Information Systems, 4*(2), 143-172.

Barnum, S. (2012). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). *MITRE Corporation*, 11.

Bergman, M., King, J. L., & Lyytinen, K. (2002). Large-scale requirements analysis revisited: the need for understanding the political ecology of requirements engineering. *Requirements Engineering*, *7*(3), 152-171.

Bouchard, L. (1993). *Decision criteria in the adoption of EDI*: Direction de la recherche, Faculté des sciences de l'administration, Université Laval.

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

Burger, E. W., Goodman, M. D., Kampanakis, P., & Zhu, K. A. (2014). *Taxonomy model for cyber threat intelligence information exchange technologies.* Paper presented at the Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security.

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

Clarkson, G., Jacobsen, T. E., & Batcheller, A. L. (2007). Information asymmetry and information sharing. *Government Information Quarterly, 24*(4), 827-839.

Constant, D., Kiesler, S., & Sproull, L. (1994). What's mine is ours, or is it? A study of attitudes about information sharing. *Information Systems Research, 5*(4), 400-421.

Dandurand, L., & Serrano, O. S. (2013). *Towards improved cyber security information sharing.* Paper presented at the Cyber Conflict (CyCon), 2013 5th International Conference on.

Depietro, R., Wiarda, E., & Fleischer, M. (1990). The context for change: Organization, technology and environment. *The processes of technological innovation, 199*(0), 151-175.

ENISA, D. SHARE, Protect-Solutions for Improving Threat Data Exchange among CERTs, 2013.

Faerman, S. R., McCaffrey, D. P., & Slyke, D. M. V. (2001). Understanding interorganizational cooperation: Public-private collaboration in regulating financial market innovation. *Organization science, 12*(3), 372-388.

Fan, J., Zhang, P., & Yen, D. C. (2014). G2G information sharing among government agencies. *Information & Management, 51*(1), 120-128.

Fernandez Vazquez, D., Pastor Acosta, O., Brown, S., Reid, E., & Spirito, C. (2012). *Conceptual framework for cyber defense information sharing within trust relationships.* Paper presented at the Cyber Conflict (CYCON), 2012 4th International Conference on.

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

Gil-Garcia, J. R., Chengalur-Smith, I., & Duchessi, P. (2007). Collaborative e-Government: impediments and benefits of information-sharing projects in the public sector. *European Journal of Information Systems, 16*(2), 121-133.

Gil-García, J. R., & Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. *Government Information Quarterly, 22*(2), 187-216.

Grover, V. (1993). An empirically derived model for the adoption of customer-based interorganizational systems. *Decision sciences, 24*(3), 603-640.

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

Hart, P., & Saunders, C. (1997). Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organization science, 8*(1), 23-42.

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

Herman, M. (1996). *Intelligence power in peace and war*: Cambridge University Press.

Hilsman, R. (1952). Intelligence and policy-making in foreign affairs. *World Politics, 5*(01), 1-45.

Jain, A. K., Murty, M. N., & Flynn, P. J. (1999). Data clustering: a review. *ACM Computing Surveys (CSUR), 31*(3), 264-323.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. *NIST Special Publication, 800*, 150.

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 AIS, 2*(1es), 7.

Kolini, F., & Janczewski, L. (2015). "Cyber Defense Capability Model: A Foundation Taxonomy," Paper presented at the CONF-IRM 2015 Proceedings paper 32, Canada

Kolini, F.,& Janczewski, L. (2017). Clustering and Topic Modelling: A New Approach for Analysis of National Cyber security Strategies.Paper Presented at the PACIS 2017 Proceedings , Malaysia

Kuan, K. K., & Chau, P. Y. (2001). A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework. *Information & Management, 38*(8), 507-521.

Landsbergen Jr, D., & Wolken Jr, G. (2001). Realizing the promise: Government information systems and the fourth generation of information technology. *Public administration review*, *61*(2), 206-220.

Lin, H.-F., & Lin, S.-M. (2008). Determinants of e-business diffusion: A test of the technology diffusion perspective. *Technovation*, *28*(3), 135-145.

Lips, A. M. B., O'Neill, R. R., & Eppel, E. A. (2011). Cross-agency collaboration in New Zealand: An empirical study of information sharing practices, enablers and barriers in managing for shared social outcomes. *international Journal of public Administration*, *34*(4), 255-266.

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.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192-222.

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

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

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, *88*(5), 879.

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

Robinson, N., & Disley, E. (2012). Incentives and Challenges for Information Sharing in the Context of Network and Information Security.

Rogers, E. M. (2010). *Diffusion of innovations*: Simon and Schuster.

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

Rutkowski, A., Kadobayashi, Y., Furey, I., Rajnovic, D., Martin, R., Takahashi, T., . . . Hird, M. (2010). CYBEX: the cybersecurity information exchange framework (x. 1500). *ACM SIGCOMM Computer Communication Review*, *40*(5), 59-64.

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.

Swanson, E. B., & Ramiller, N. C. (2004). Innovating mindfully with information technology. *MIS QUARTERLY*, 553-583.

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *Processes of technological innovation*: Lexington Books.

Tornatzky, L. G., & Klein, K. J. (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on engineering management*(1), 28-45.

Verizon. (2017). *2017 Dara Breach Investigation Report*.

Wang, P. (2010). Chasing the hottest IT: effects of information technology fashion on organizations. *MIS QUARTERLY*, *34*(1), 63-85.

Yang, H., Osterweil, E., Massey, D., Lu, S., & Zhang, L. (2011). Deploying cryptography in Internet-scale systems: A case study on DNSSEC. *Dependable and Secure Computing, IEEE Transactions on*, *8*(5), 656-669.

Yang, T.-M., & Maxwell, T. A. (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.

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.

Zhu, K., Kraemer, K. L., & Xu, S. (2006). The process of innovation assimilation by firms in different countries: a technology diffusion perspective on e-business. *MANAGEMENT SCIENCE*, *52*(10), 1557-1576.