Faculty of Natural and Applied Sciences Journal of Computing and Applications
Print ISSN: 3026-8133
www.fnasjournals.com
Volume 2; Issue 1; September 2024; Page No. 58-65.

Cyber Threat Intelligence Sharing: A Review of Concepts, Platforms, and Legal Considerations

***[1]Keyamo, C.A., [2]Attoh, O.M., [3]Edun, O.P., [4]Adeoye, A.E., [5]Ashioba,N.C., & [6]Yoro, R.E.**
[1,4,5]Department of Computer Science, Dennis Osadebay University, Asaba, Nigeria
[2,3,6]Department of Cyber Security, Dennis Osadebay University, Asaba, Nigeria

***Corresponding author email**: clement.keyamo@dou.edu.ng

Abstract
There is a need for a collaboration-based response to check sophisticated attacks on computer-based systems by Cyber criminals through the sharing of relevant information between related targets of these criminals. The sharing of such information is referred to as Cyber Threat Intelligence sharing. This paper aims to introduce useful information to practising stakeholders and their organizations that can assist and convince their participation in Cyber Intelligence Sharing activities. The Rapid Literature Review (RLR) method is used to gather relevant data to answer key research questions including: What is Cyber Threat Intelligence? What are the terminologies and concepts that help to understand Cyber Threat Intelligence and the sharing of same? How is Cyber Threat Intelligence shared and what technology is used for sharing? And what are the legal matters arising in the sharing of Cyber Threat Intelligence? The paper focuses on defining key terminologies and concepts in the area, introducing Threat Intelligence Platforms used in sharing relevant information and explaining some legal matters arising from sharing Cyber Intelligence.

Keywords: Cyber Threat Intelligence, CTI sharing infrastructure, Threat Intelligence Platforms, Open Source Intelligence (OSINT)

Introduction

Information Technology (IT), the Application of computers in human business and activities, has positively impacted all areas of human life. The positive use of IT in human endeavour can be ascribed to the ever-evolving versatility of computers and associated technology. Unfortunately, this versatility is what empowers criminals in the digital space to perpetuate sophisticated crimes. These activities of criminals in the realm of computers and networks using computer-based technology and skills is what is called Cybercrime. Over the years, there has been a marked increase in Cybercrimes (crimes involving the direct or indirect use of computers and associated technologies). Specifically, attacks on computer systems for financial and other gains have increased in sophistication and quantity, resulting in huge damage across different segments of human society including educational, financial and health sectors (Faiella et al., 2019). To ameliorate these attacks and their impact, diverse countermeasures and procedures have been instituted over the years. These countermeasures and procedures, however, require timely and accurate information to be available to organizations to properly guide the IT infrastructure. Such information is referred to as Cyber Threat Intelligence (CTI) and the sharing of such information between entities is referred to as Cyber Threat Intelligence Sharing or CTI sharing (Mavroeidis & Bromander, 2017; Homan et al., 2019).

CTI sharing has been suggested by Jasper (2017) to be a sensible response to Cybercrimes. Sophisticated Cyber-attacks may be part of coordinated campaigns that target related organizations. In some cases, countries have been known to sponsor such crimes for diverse reasons. It, therefore, makes some sense that related organizations should band together to defend themselves from these attacks through the sharing of Cyber Threat Intelligence. This allows organizations to respond quickly to malicious activities that could threaten their networks and organizations. However, The sharing of Cyber Threat Information introduces some challenges. Homan et al. (2019) and Albakri et al. (2019) identified some challenges in Cyber Threat Intelligence Sharing including the potential for leakage of sensitive and identifying data (such as existing vulnerabilities, IP and email addresses and so on) that can expose sharing parties to attacks. Also, damage to reputation and loss of revenue can follow this leakage. Furthermore, Inherent trust barriers

Cite this article as:
Keyamo, C.A., Attoh, O.M., Edun, O.P., Adeoye, A.E., Ashioba,N.C., & Yoro, R.E. (2024). Cyber threat intelligence sharing: a review of concepts, platforms, and legal considerations. *FNAS Journal of Computing and Applications, 2*(1), 58-65.

existing between sharing parties can inhibit sharing and discourage participation by some parties. The above and other limitations imply that sharing parties should have a firm grasp of the fundamental issues that pertain to CTI sharing to maximize its benefits and minimize the inherent challenges. Previous research outputs have presented relevant findings that can assist stakeholders to benefit more from CTI sharing, but to the best of our knowledge, there still is the absence of research output covering fundamental areas in CTI sharing that can be easily understood by stakeholders such as non-IT staff who have little knowledge in the area and some entry-level scholars and field professionals desiring introductory level information in the area.

This research aims to introduce useful information to practising stakeholders and their organizations that can assist and convince their participation in Cyber Intelligence Sharing activities. The paper presents and succinctly explains the key concepts and issues in Cyber Threat Intelligence sharing, including Trust Classification, sharing standards, CTI Trust and sharing platforms and sharing Laws and Regulations. It is believed that grasping these issues by stakeholders can further increase the tendency of organizations to share intelligence, better manage the sharing process and thus increase their effectiveness in checking Cyber-attacks on their organizations. Also, scholars can find the material relevant to their work as the material is presented in a succinct manner and with clarity for easy assimilation.

The remaining parts of this paper are thus structured: section 2 covers the Research Method and Materials; Section 3 covers the Definition of Key Terms and Concepts; Section 4: Sharing Platforms, Standards and Trusts; Section 5 covers: Sharing Laws and Regulations; Section 6: Conclusion and Recommendation.

Research questions

To meet the aim of the research, a Rapid Literature Review (RLR), (Smela et al., 2023) is used to answer the following guiding questions that aid the accumulation of relevant information:

1. What is Cyber threat intelligence?
2. What are the terms and concepts that help to understand Cyber threat intelligence and the sharing of same?
3. How is threat intelligence shared and what technology is used for sharing?
4. And what are the legal matters arising in the sharing of Cyber threat intelligence?

Methods and Materials

A total of 34 articles were downloaded from searches in journal databases using Google. The search terms applied included but were not limited to: Cyber Threat Intelligence, Information Sharing, General Data Protection Regulation GDPR, CTI sharing infrastructure, CTI indicators, information security, information sharing, Threat Intelligence Platforms, Open Source Intelligence (OSINT), legal issues, CTI sharing, GDPR, and so on. A manual search of the reference list of the collected articles was then carried out to identify other relevant works. Articles were then excluded that did not meet the needs of the research after their abstracts had been viewed. The data gathered is then used to develop a narrative in sections ahead.

Cyber Threat Intelligence (CTI) Sharing: What is it?

De Melo e Silva et al. (2020) provided a detailed explanation of the concept of Cyber threat intelligence sharing. The desire of individuals and organizations to better protect themselves from sophisticated Cyber attacks has introduced the need for the sharing of relevant information that can be used to effect such protection. Information or analyzed data that can identify and classify threats to a computer system is called Cyber Threat Information. When this kind of information is processed or analyzed further to useful states such that it can be applied directly for the protection of Cybersystems, such information is known as Cyber Threat Intelligence (CTI). The dissemination of this analyzed and contextualized threat information to parties that utilize it is what is called Cyber Threat Intelligence (CTI) Sharing. To better comprehend the CTI sharing concept, figure 1 identifies five stages explaining CTI sharing.

Cite this article as:
Keyamo, C.A., Attoh, O.M., Edun, O.P., Adeoye, A.E., Ashioba,N.C., & Yoro, R.E. (2024). Cyber threat intelligence sharing: a review of concepts, platforms, and legal considerations. *FNAS Journal of Computing and Applications, 2*(1), 58-65.

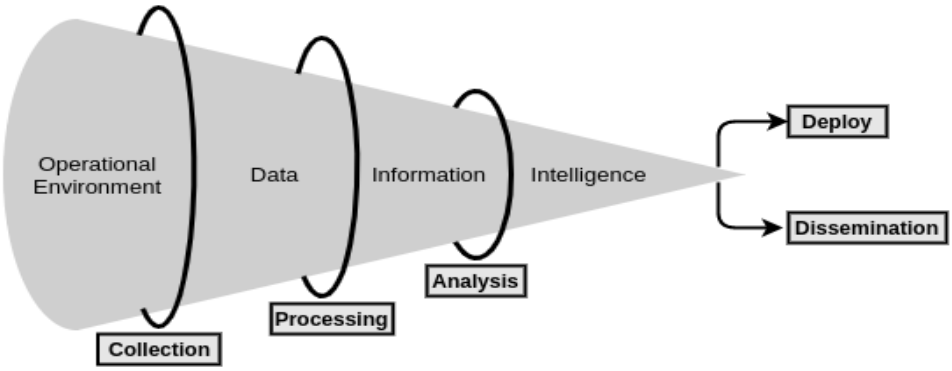

Fig 1: CTI production and Dissemination (De Melo e Silva et al., 2020)

From the diagram, the following are explained further:
Collection: here data relating to threats to computer-based systems are gathered through relevant procedures and devices. The data so gathered are called threat indicators or facts.
Processing: this step involves trying to answer questions by combining indicators in relevant ways. Questions answered at this stage try to meet initial requirement specification questions before the collection of facts takes place. Questions answered could be: what kind of techniques do known attackers use? What are the vulnerabilities commonly being exploited presently by criminals? And so on. The product of processing indicators is what is called threat information.
Analysis: this involves the uncovering of patterns from the evaluation of both indicators or raw facts or data and processed information. The overall goal here is to determine what will happen next using what has happened, what is happening and why it happened or is happening. Huge amounts of raw data and information are often analyzed in this step. The product of this step is what is called threat intelligence.
Deployment: this covers the relevant decision-making process where decision is made on: when, where, and how the intelligence is to be deployed. Determining how threat Intelligence will be consumed affects the collection and processing of initial indicators. Producers of CTI should have a knowledge of what and how their output will be utilized and disseminated as this will determine formats and types of CTI. Relevant application areas for the gathered intelligence may be classified at this stage.
Dissemination: sharing past, current, and future CTI to final consumers is what is known as CTI dissemination. This is the stage where the CTI is shared with interested parties, stakeholders and communities using appropriate intelligence-sharing mechanisms and platforms like the TIPs and the variant TISPs.
In CTI sharing, three important things to consider are trust between sharing parties, standard formats for sharing CTI and tools for sharing CTI. These three will be covered in later sections. Also, Some basic terms that further help to understand the CTI sharing concept are listed in subsection below.

Definition of some Basic Concepts in CTI Sharing
Johnson et al. (2016) identified key concepts as applicable to CTI sharing including:
Cyber threats: these are circumstances or events that have the potential to negatively impact organizational operations and assets or individuals and Nations through a computer-based system. Here, natural disasters are also considered cyber threats since they also have the potential to cause damage to such organisation's computer-based systems.
Threat actors: these are the individuals that pose a threat to other individuals, organizations or nations via Cyberspace. For instance, any individual who can access an organization's computer system or network illegally (popularly known as a hacker) and cause damage to the system is a threat actor.
Cyber Threat Information: Include information that is related to Cyber threats and threat actors that individuals, organizations and nations can use to protect themselves from the activities of threat actors. This information can include individuals or groups that are known to perpetuate cyber attacks, the tactics, Techniques, and procedures they use to perpetuate their attacks, targets and vulnerabilities, known countermeasures against, and so on.
Tactics, Techniques, and Procedures (TTPs): these together describe a threat actor's behaviour in Cyberspace. Tactics refer to the overall behavioural pattern of a specific threat actor.it is regarded as a high-level behaviour pattern.

Cite this article as:
Keyamo, C.A., Attoh, O.M., Edun, O.P., Adeoye, A.E., Ashioba,N.C., & Yoro, R.E. (2024). Cyber threat intelligence sharing: a review of concepts, platforms, and legal considerations. *FNAS Journal of Computing and Applications, 2*(1), 58-65.

Techniques are the tactics of a Threat actor broken down into more detailed steps. Techniques describe tactics in more detail. While Procedures are step-by-step descriptions of Threat actor techniques. They provide a highly detailed description of a threat actor's behavioural pattern.

Indicators: these are signposts to an imminent attack or ongoing attack. They are observables that can be used to detect potential and ongoing attacks such as a suspicious domain name, or Uniform Resource Locator (URL) that is known to reference malicious content.

Trust: this is seen as the assurance that stakeholders in a sharing community treat the CTI shared with confidentiality when specified and do not use the same for malicious purposes.

Trust Mechanisms: These are the policies put in place in Threat Intelligence Platforms (TIPs) to guide and safeguard sharers and consumers of CTI within a community.

Actionability: this describes the quality attributes of CTI including attributes of relevance, completeness, timeliness, trustworthiness, and accuracy. Actionability is directly related to the usability of CTI.

Benefits and Challenges of CTI Sharing

Some of the benefits and challenges associated with Cyber threat Intelligence Sharing as identified by researchers (Johnson et al., 2016; Wagner et al., 2018; De Melo e Silva et al., 2020) are summarized here.

For the benefits, CTI sharing empowers organizations/stakeholders to take advantage of the shared knowledge, experience, and specialized skills of their sharing partners to enhance their defensive standings. A relevant addition to observations about a threat actor to a community can make a great difference to the security standing of stakeholders. Secondly, the Sharing of CTI enables stakeholders to gain a better understanding of the threat landscape. This enables them to better improve on the risk management practices. They can use the shared intelligence to improve the databases of their perimeter security tools like Intruder Detection Systems (IDS). Thirdly, the pooling of seemingly unrelated information can enable information maturity through the enhancement of relationships existing between indicators and thus help to increase the security posture of the sharing organizations. Finally, sharing of CTI enables participating organizations to be better informed about the ever-changing strategies of threat actors. Threat actors are known to constantly change their attack strategies to evade detection, outwit security controls, and exploit new weaknesses. The pooling of CTI plays a huge role in countering this frequent metamorphosis of attack strategies. On the challenges to CTI sharing, trust plays an important role here. Trust is the fundamental prerequisite for sharing information. Organizations are often afraid of giving potential competitors information that represents their weak links. The establishment and maintenance of trust relationships requires continuous communication using phone calls, and social media (and so on) on a personal level, to hasten trust building between organizations. A second challenge in CTI sharing is the establishment of automation and interoperability. CTI requires standard data formats and protocols for increased speed of sharing and automation of the sharing process. The implementation of these standards is however expensive and time-consuming. The purchase of new tools is a present challenge to organizations in this regard. Thirdly, the sharing of sensitive information exposes the sharing parties to risks of disclosure of sensitive information relevant to the protective or detective capacities of the organizations. Security and information such as security logs and scan results can become exposed to the wilder Cyberspace if sharing partners poorly safeguard them. Other challenges are, that accessing classified CTI information from government sources requires clearances that may be time-consuming and expensive, and limitation or disparity of processing capacities by sharing partners can overwhelm such organization's facility in cases where high-frequency and high-volume information exchanges are involved.

CTI Sharing Platforms and Infrastructures

Software tools called Threat Intelligence Platforms (TIPs), and the variant Threat Intelligence Sharing Platforms(TISP), have been crafted to help manage CTI sharing. The main goal of these tools is to assist incidence response entities, such as Intrusion Detection Systems (IDS), make correct decisions regarding Cyber Attacks (De Melo e Silva et al., 2020). TIPs are digital tools used by organizations for the retrieval of Intelligence data (structured or unstructured) from external sources to bridge the gaps in conventional security monitoring and detection systems such as IDSs and SIEMs (Faiella et al., 2019; Sauerwein et al.,2017). TIPSs are designed as secondary sources of data for organizations and security tools and can perform filtering, normalization, aggregation, detection, analysis and enrichment. They are effective for gathering open source intelligence (OSINT), for storage, and for sharing and integration with other organizations and specialized tools. Also, TIPs can be viewed as specialized software systems that can collect, process, analyze, integrate and deploy (display and disseminate) the internal and external threat intelligence of an organization or community of CTI collaborators (De Melo e Silva et al., 2020). They became necessary response measures due to the emergence of a new threat landscape. By new threat landscape, we mean the

Cite this article as:
Keyamo, C.A., Attoh, O.M., Edun, O.P., Adeoye, A.E., Ashioba,N.C., & Yoro, R.E. (2024). Cyber threat intelligence sharing: a review of concepts, platforms, and legal considerations. *FNAS Journal of Computing and Applications, 2*(1), 58-65.

emerging threats, including the Advance Persistent Threats (APTs) characterized by their capacities to establish prolonged and undetected footholds in their targets, and the Polymorphic Threats with inherent capacities to modify self and thus stay undetected for lengthy periods since detection is complicated by their inherent ability to change.

Classification of TIPs

According to Tounsi and Rais, (2018), TIPs can be classified based on several features including the following:

Import/Export format they support: some TIPs support diverse data formats. For example, the Malware Information Sharing Platform (MISP) can work with PDF, doc, xls, txt, JSON, XML, and Structured Threat Information eXpression (STIX) formats as its input and output. Such TIPs have capacities for the extension of modules, allowing modifications that accept specialized CTI-sharing data formats like STIX. Some TIPs such as the Collective Intelligence Framework (CIF) are not that open when involving specialized standards for data importation and exportation.

Integration with Common Security Tools: some TIPs can connect seamlessly with standard security tools like IDSes while some cannot. For the TIPs that support connectivity, their Application Programming Interfaces (APIs) are designed for interaction with such tools.

Collaboration Type support: Centralized / server-client collaboration, or decentralised / Client-client collaboration or both are possible with TIPs depending on their design. Centralized-type TIPs can share the same type of CTI among members of the same trusted community. Decentralized type TIPs can connect on a peer-to-peer basis to share instances on a many-to-many basis. Some TIPs like the MISP have inbuilt capacities for both.

In addition, Watson (2021) classified TIPs into two broad groups: TIPs that result in modification of CTI and those that do not. The structure of TIPs and the kind of data they act on can determine their output. Many TIPs are designed to accept or reject certain data formats. They only process data that falls within a predefined profile. This limits the kind of CTI that could be available from these kinds of TIPs since their input data is classified. Other TIPs can map all kinds of data to their preferred indigent format and have capacities to accept several kinds of threat data and information for onward processing to CTI.

CTI Sharing Models of TIPs

An important aspect of CTI sharing is collaboration between related stakeholders for which TIPs play a major role. According to Wagner (2019), CTI collaboration is based on three models: the peer-to-peer, the peer-to-hub and the hybrid models.

Peer-To-Peer Model: In the peer-to-peer model, collaborators share CTI directly without recourse to a third-party platform. That is between two parties without a middle party. Figure 2 illustrates this sharing model.

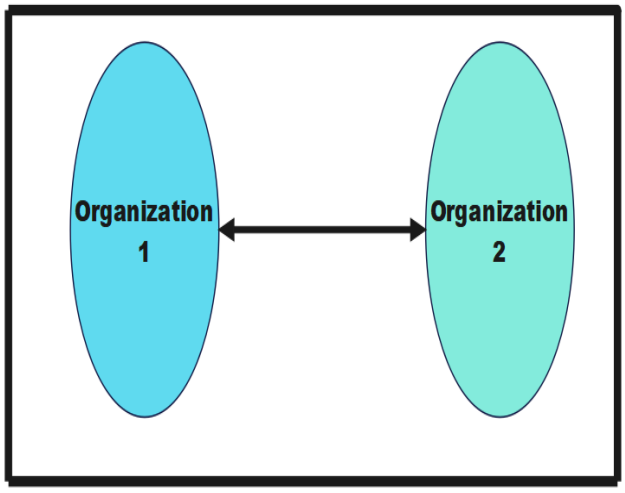

Figure 2: Peer-Peer Model

Peer-To-Repository Model: In this model, organizations can connect to a shared repository to access CTI. Figure 3 illustrates the model. The repository serves as a central server managed by a third party and may include mandatory or advisory instruction by the government for organizations to contribute their CTI data.

Cite this article as:
Keyamo, C.A., Attoh, O.M., Edun, O.P., Adeoye, A.E., Ashioba,N.C., & Yoro, R.E. (2024). Cyber threat intelligence sharing: a review of concepts, platforms, and legal considerations. *FNAS Journal of Computing and Applications, 2*(1), 58-65.

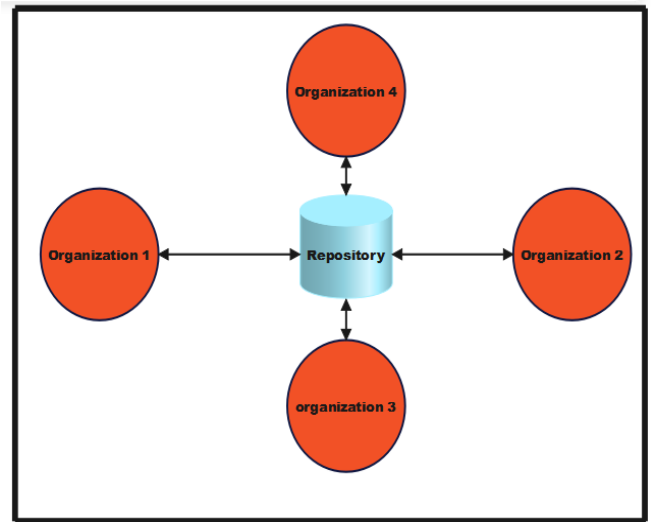

Figure 3: Peer-To-Repository Model

Hybrid Model: this model combines the attributes of the previous two. The model is illustrated using Figure 4

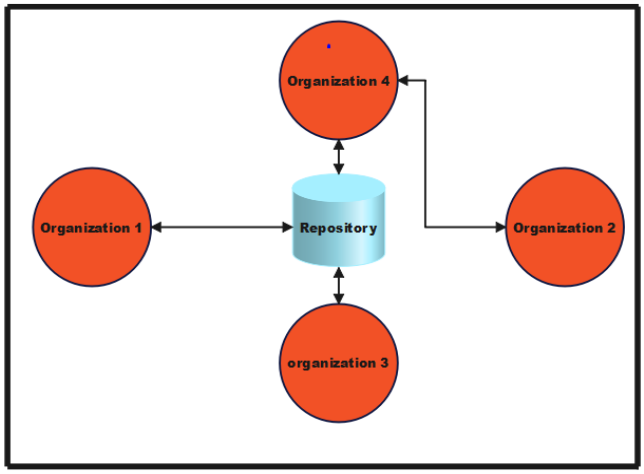

Figure 4: Hybrid Model

Trust and CTI sharing

Trust is reported to be the most important attribute of CTI sharing as without it sharing of CTI would be unthinkable. According to Wagner et al. (2018), trust is an assurance that stakeholders handle shared CTI with confidentiality and do not use it for malicious purposes. Trust in the CTI context also implies that trust communities share true and correct CTI without intending to harm co-members in any way. Trust is a very important attribute in CTI sharing as without it, stakeholders would abstain from participating in sharing and using CTI. Trust implies that stakeholders and the information they offer are sincere in the quest to assist the community fight Cybercrime. Indeed, without trust, it would be unthinkable for any right-thinking organization to share CTI with another, since such information may carry important data that can be used against the sharing party if put in the wrong hands. Wagner et al. (2018) introduced a trust taxonomy for CTI sources. Their work was intended to establish a trusted threat-sharing environment. They analyzed and compared 30 popular threat intelligence platforms/providers regarding trust functionalities, trust taxonomies were analyzed and compared also and Illustrative case studies were developed and analyzed applying their trust taxonomy. They concluded that their trust taxonomy shows how to establish trust between decentralized users.

CTI Sharing Standards.

Mavroeidis and Bromander (2017) carried out some research on CTI sharing standards. In their work, they evaluated existing CTI-relevant sharing standards,

Their findings show that the Structured Threat Information eXpression (STIX) is one of the most used standards for

Cite this article as:
Keyamo, C.A., Attoh, O.M., Edun, O.P., Adeoye, A.E., Ashioba,N.C., & Yoro, R.E. (2024). Cyber threat intelligence sharing: a review of concepts, platforms, and legal considerations. *FNAS Journal of Computing and Applications, 2*(1), 58-65.

sharing threat information. They report STIX to be, "an expressive, flexible, and extensible representation language used to communicate an overall piece of threat information."
Also, they claim that STIX architecture comprises different cyber threat information elements such as cyber observables, indicators, incidents, adversaries' tactics, techniques, procedures, exploit targets, courses of action, cyber-attack campaigns, and threat actors. Furthermore, Mavroeidis and Bromander (2017) identified the Malware Attribute Enumeration and Characterization (MAEC) as another sharing standard. MAEC is said to be a "very expressive malware sharing language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviours, artefacts, and attack patterns." It can be used on its own as a standalone product or integrated with STIX.
Finally, they discussed OpenIOC (that is Open Indicator of Compromise), developed by Mandiant. OpenIOC is an extensible XML schema that enables one to describe the "technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise." OpenIOC covers information directly derived from enriched low-level atomic indicators, comprising indicators of compromise. This is said to cover the IOC category of the cyber threat intelligence mode.

CTI Sharing Laws and Regulations

There are legal restrictions on CTI sharing notwithstanding the relevance of sharing such information. According to Albakri1 et al. (2019), institutions must conform to Local and international legal and regulatory requirements for sharing CTI in the nations where they operate. Organizations, therefore need guidance on what to share and what not to share. Knowledge of relevant laws by stakeholders is key to this. Wagner et al. (2019), discussed the relevance of national laws and regulations governing CTI sharing. One important point regarding the sharing of CTI data was the difference in Laws and Regulations on CTI data sharing from country to country. For instance, the United Kingdom (UK) does not consider IP addresses of individuals as personal data while German law sees IP addresses as personal. This means that the laws of individual nations need to be considered in the sharing of CTI data, especially when it transcends national borders. The implication of this disparity in legal standing on CTI sharing as identified by Wagner et al. (2019), is that the constraints in local and international laws may impede stakeholders from sharing their intelligence. For example, internal data protection policies and country-specific data protection may obstruct the sharing process. In the US, the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA) are noted to have contributed to confusion regarding whether CTI can be shared. The acts have content that prohibits communications providers from voluntary disclosure of communications content.

Generally, antitrust law, intellectual property law, privacy and data protection law and the tort of negligence law, are laws that can stop or limit organizations from sharing CTI as they are common sources of liability (Nweke & Wolthusen, 2020). Organizations should sieve materials they intend to share to determine if they contain materials prohibited under these laws in their area of operation. However, laws exist that facilitate CTI sharing in some countries. For example, the General Data Protection Regulation (GDPR) regulation, Network and Information Systems (NIS) Directive and Cyber Security Act, are all laws in the European Union (EU) that regulate CTI sharing while facilitating the sharing of the same. The NIS is in place to encourage the sharing of CTI that can lead to the protection of critical infrastructure across the EU, while the GDPR is a legal directive that seeks to protect the privacy and data rights of EU citizens. Other note-worthy laws that influence CTI sharing are (Nweke & Wolthusen, 2020): the Japanese Personal Information Protection Act (PIPA), the Norwegian National Security Act, and the Cybersecurity Information Sharing Act of the United States. The Norwegian Act focuses on issues of national security. It covers security-rated information, information systems and critical infrastructure. The Cybersecurity Information Sharing Act of the United States provides provisions empowering organizations to protect themselves from external attacks, share data between themselves and regulate the sharing of CTI between government agencies and between government agencies and private organizations.

Conclusion

In this paper, we have reviewed three important issues regarding the sharing of Cyber Threat Intelligence: key concepts in the area, platforms used for the sharing of CTI and relevant legal concerns. A Rapid Literature Review technique was used to gather relevant information using some guiding questions. Among other relevant findings, we have seen that CTI sharing is important to the security of modern information systems and it is essential that stakeholders have a firm understanding of fundamental issues in this area to enable them to act effectively in the sharing of CTI data. Understanding What constitutes CTI and knowing how to share and choose appropriate sharing platforms is important for stakeholders and their organizations. Also, a firm grasp of legal issues about CTI sharing is necessary for safe and effective sharing of CTI between organizations.

Cite this article as:
Keyamo, C.A., Attoh, O.M., Edun, O.P., Adeoye, A.E., Ashioba,N.C., & Yoro, R.E. (2024). Cyber threat intelligence sharing: a review of concepts, platforms, and legal considerations. *FNAS Journal of Computing and Applications, 2*(1), 58-65.

Recommendations

Finally, we make the following recommendations based on our findings:

1. Stakeholders and their organizations plug into the sharing of CTI to better safeguard their computing infrastructure and also help protect cyberspace from Cyber criminals.
2. In choosing CTI sharing Platforms, organizations and stakeholders should carefully consider the technical and cost implications and choose platforms that better serve their financial and technical capacities.
3. Finally, organizations should be conversant with local applicable laws in other to share CTI legally.

References

Albakri, A., Boiten, E., & De Lemos, R. (2019). Sharing cyber threat intelligence under the General Data Protection Regulation. *Lecture Notes in Computer Science,* 28-41. https://doi.org/10.1007/978-3-030-21752-5_3

De Melo e Silva, A., Costa Gondim, J. J., De Oliveira Albuquerque, R., & García Villalba, L. J. (2020). A methodology to evaluate standards and platforms within cyber threat intelligence. *Future Internet, 12*(6), 108. https://doi.org/10.3390/fi12060108

Faiella, M., Gonzalez-Granadillo, G., Medeiros, I., Azevedo, R., & Gonzalez-Zarzosa, S. (2019). Enriching threat intelligence platforms capabilities. *In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications* (pp. 37-48). https://doi.org/10.5220/0007830400370048

Homan, D., Shiel, I., & Thorpe, C. (2019). A new network model for cyber threat intelligence sharing using blockchain technology. *In 2019 10th IFIP International Conference on New Technologies, Mobility and Security* (NTMS). https://doi.org/10.1109/ntms.2019.8763853

Jasper, S. E. (2016). U.S. cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence, 30*(1), 53-65. https://doi.org/10.1080/08850607.2016.1230701

Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. *National Institute of Standards and Technology.* https://doi.org/10.6028/nist.sp.800-150

Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In 2017 *European Intelligence and Security Informatics Conference (EISIC).* https://doi.org/10.1109/eisic.2017.20

Nweke, L. O., & Wolthusen, S. (2020). Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection. In 2020 12th International Conference on Cyber Conflict (CyCon). https://doi.org/10.23919/cycon49761.2020.9131721

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 the 13th International Conference on Wirtschaftsinformatik, St.Gallen, Switzerland,* 12–15 February 2017.

Smela, B., Toumi, M., Świerk, K., Francois, C., Biernikiewicz, M., Clay, E., & Boyer, L. (2023). Rapid literature review: Definition and methodology. *Journal of Market Access & Health Policy, 11*(1). https://doi.org/10.1080/20016689.2023.2241234

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security, 72,* 212-233. https://doi.org/10.1016/j.cose.2017.09.001

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589. https://doi.org/10.1016/j.cose.2019.101589

Wagner, T. D., Palomar, E., Mahbub, K., & Abdallah, A. E. (2018). A novel trust taxonomy for shared cyber threat intelligence. *Security and Communication Networks, 2018,* 1-11. https://doi.org/10.1155/2018/9634507

Watson, K. K. (2021). Cyber threat intelligence (CTI) sharing infrastructures. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/Preserving%20CTI%20Content_508c.pdf