

Communications of the IIMA

Manuscript 1450


Cyber Threat Intelligence Sharing in Nigeria

Muhammad Abubakar Nainna

Julian Bass

Lee Speakman

Follow this and additional works at: <https://scholarworks.lib.csusb.edu/ciima>

 Part of the [Digital Communications and Networking Commons](#), and the [Management Information Systems Commons](#)

Cyber Threat Intelligence Sharing in Nigeria

Muhammad Abubakar Nainna

Department of Computer Science and Software Engineering University of
Salford, Manchester, United Kingdom

43 Crescent, Salford M5 4WT a.n.muhammad@edu.salford.ac.uk

Julian M Bass

Department of Computer Science and Software Engineering University of
Salford, Manchester, United Kingdom

43 Crescent, Salford M5 4WT j.bass@salford.ac.uk

Lee Speakman

Department of Computer Science and Software Engineering University of
Salford, Manchester, United Kingdom

43 Crescent, Salford M5 4WT l.speakman@salford.ac.uk

ABSTRACT

Cybersecurity challenges are common in Nigeria. Sharing cyber threat intelligence is essential in addressing the extensive challenges posed by cyber threats. It also helps in meeting regulatory compliance. There are a range of impediments that prevent cyber threat intelligence sharing. We hypothesise that we want to maximise this cyber threat intelligence sharing to resist malicious attackers. Therefore, this research investigates factors influencing threat intelligence sharing in Nigeria's cyber security practitioners. To achieve this aim, we conducted research interviews with 14 cyber security practitioners using a semi-structured, open-ended interview guide, which was recorded and transcribed. We analysed the data using an approach informed by grounded theory. We coded the data, organised the data into categories, and used constant comparison to check our code's consistency and accuracy. We developed memos from which our descriptive grounded theory emerged. After a detailed study, we found that cybersecurity practitioners in Nigeria are enthusiastic about collaborating to exchange and receive cyber threat intelligence. However, we discovered two impediments to sharing. Firstly, the existence of competing standardisation in cyber threat intelligence sharing and, secondly, the lack of practitioner's skills in data protection. These barriers inhibit cyber security practitioners from disseminating such cyber threat intelligence sharing inside Nigeria. Based on our findings, we conclude that overcoming these impediments will help cybersecurity practitioners share more cyber threat intelligence in Nigeria.

Keywords: Cyber threat intelligence sharing, Cyber security practitioners, Nigeria, Frameworks, Grounded theory.

INTRODUCTION

Cybersecurity challenges are common in Nigeria (Ibrahim, 2016). Online scams and digital extortion are the country's highest-reported and most pressing cyber threats (INTERPOL, 2022). Many Nigerian businesses do not implement cybersecurity protocols (Abubakar et al., 2014). Threat actors exploit weaknesses without these protocols as they develop new cyberattack channels, resulting in substantial financial losses (Alexander, 2020; Deloitte, 2022). On the other hand, cyber security practitioners in Nigeria know the importance of sharing and receiving cyber threat intelligence. However, some factors influence their behaviour. This paper's primary research question is: What factors influence cyber security practitioners sharing cyber threat intelligence in Nigeria?

We conducted research interviews with 14 cyber security practitioners using semi-structured, open-ended, recorded and transcribed questions to answer this question. We analysed the data using an approach informed by grounded theory. We coded the data, organised the data into themes, and used constant comparison to check our code's consistency and accuracy. We developed memos from which our descriptive theory emerged.

After a detailed study, we found that cybersecurity practitioners in Nigeria are willing to exchange and receive cyber threat intelligence. However, the research uncovers two significant impediments to sharing. Firstly, the existence of competing standardisation in cyber threat intelligence sharing and, secondly, the lack of practitioner's skills in data protection. These factors inhibit cyber security practitioners from sharing cyber threat intelligence in Nigeria.

Based on our findings, we conclude that overcoming these impediments will help cybersecurity practitioners share more cyber threat intelligence in Nigeria.

This paper is structured as follows: Section 2 reviews the previous research on cyber threat intelligence sharing while offering a brief overview of cyber threat intelligence sharing in Nigeria. Moving forward, Section 3 outlines the research methodology employed in this study, encompassing details on the selected research sites, data collection procedures, and the adopted data analysis approach.

The investigation outcomes are presented in Section 4, where the study's findings are systematically unveiled and analysed. Section 5 delves into a comprehensive discussion of the results, offering deeper insights and interpretations. Finally, Section 6 serves as the study's conclusion, summarising the three primary research findings and their implications.

RELATED WORK

This section discussed an overview of cyber threat intelligence (CTI). It also defines CTI from the literature and gives a historical background of CTI. The section also discussed the Nigerian cyber security infrastructure and the importance of sharing CTI. Lastly, the existing frameworks and challenges in sharing CTI in Nigeria were highlighted.

Overview of Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence involves collecting, analysing, and transmitting information about current or potential cyber threats (Abu et al., 2018; Ainslie et al., 2023). Organisations use CTI to uncover potential threats' motives, methods, and objectives (Nainna et al., 2024). This intelligence improves organisations' overall security measures (Nainna et al., 2024). More specifically, there are three types of CTI: strategic, operational, and tactical intelligence (Tounsi & Rais, 2018).

Strategic CTI analyses the whole picture available to decision-makers (Yang & Maxwell, 2011). Operational intelligence includes data about particular campaigns and threat actors (Yang & Maxwell, 2011). Finally, tactical intelligence refers to narrow operations and can inform organisations about partly discovered threats and relevant areas, including new types of malware and malware-created methods of attacks (Chris et al., 2016; Yang & Maxwell, 2011).

Definition of Cyber Threat Intelligence

Abu defines CTI as knowledge based on facts and includes context, mechanisms, indicators, implications, and advice that can be used to deal with current or new threats to assets (Abu et al., 2018). It focuses on lowering risks and helping people understand the goals, motivations, and actions of people who pose a threat (Sauerwein et al., 2019). This intelligence is about knowing how dangerous the goal of possible threats is and then acting in line with that knowledge (Abu et al., 2018; Ainslie et al., 2023).

Cyber Threat Intelligence, as Tounsi calls it, is the organised gathering, analysis, and sharing of information about an organisation's activities in cyberspace (Tounsi, 2019). By using this kind of data and information to understand and evaluate the threat landscape, organisations can better understand the threats they face and make better decisions about being more proactive about cybersecurity (Tounsi, 2019; Tounsi & Rais, 2018).

Historical Perspective of CTI Sharing Globally.

As cyber threats got more complicated, the approach to CTIS that used collaborative defence strategies had to be changed (Drake et al., 2004; Yang et al., 2012). CTIS frameworks like Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) made it possible for everyone to have equal access. This led to more development, which made the problem seem more reasonable (Kampanakis, 2014; Ponemon Institute, 2018; Sullivan & Burger, 2017).

Legislation like the Cybersecurity Information Sharing Act (CISA) of 2015 was also crucial in making CTI sharing easier (Tran, 2016). It was easier for organisations to work together by giving them legal protections when they shared cyber threat information with the federal government and each other (Shin & Lowry, 2020; Yang et al., 2020).

Aside from that, global partnerships and public-private alliances were used to promote CTI sharing (Zibak & Simpson, 2019). These were meant to help find threats and respond more quickly, strengthening the overall cyber defence (ENISA,

2020). There are strong networks of peers and knowledgeable organisations that handle the massive flow of accurate and up-to-date threat intelligence data thanks to the work of cybersecurity firms, governments, and international authorities.

Nigeria's Cybersecurity Infrastructure

The Office of the National Security Adviser (ONSA) set up the Nigerian Computer Emerging Response Team (CERT), along with CERTs from the National Information Technology Development Agency (NITDA), (Agbali et al., 2020; NITDA, 2022; ONSA, 2022) This shows Nigeria's cyber security ecosystem is ready to deal with cyber security problems (Ibrahim, 2016).

However, Nigeria is suffering from significant changes in the country's cybersecurity infrastructure aiming at combating newly arisen threats (Deloitte, 2022; Ibrahim, 2016). The Cyber Security Experts Association of Nigeria (CSEAN) highlights the increasing tendency of insider threats (Morufu et al., 2019). They also highlight vulnerabilities and security gaps in online government assets. Recent collaborative efforts, such as between Mastercard and the Committee of e-Banking Industry Heads (CeBIH), enabled the expansion of anti-cybercrime defences and the minimisation of online fraud (Deloitte, 2022; Malinka et al., 2022).

The Importance of CTI Sharing

CTI sharing is among the ultimate prerogatives for national security; it renders numerous advantages (Nainna et al., 2024). Firstly, better situational awareness presupposes real-time data for the taking, which in the contemporary landscape naturally directs towards threats (Gil-Garcia & Sayogo, 2016).

A proactive approach to gathering resources to counter impending attacks may yield the most valuable first-strike advantage (Gil-Garcia et al., 2019).

Secondly, formally establishing strategies for cross-government, private and international, essentially leads to a single standard defence policy (Karlsson et al., 2017; Sauerwein et al., 2019). Thirdly, the swift development of CTI-sharing also provides a safety guarantee by revealing weaknesses for swift mitigation

(Chris et al., 2016). Lastly, such a comprehensive approach facilitates far superior policy development for cybersecurity (Yang & Maxwell, 2011).

Existing CTI Frameworks and Platform

As previously mentioned, several CTI frameworks and platforms are available in the current state of literature (Jasper, 2017). For example, Jasper et al. (2017) have simulated CTI-sharing effectiveness to compare multiple frameworks with existing systems (Jasper, 2017); Yang (2014) reviewed CTI standards and platforms, analysing potential research gaps (Yang et al., 2014). Abu (2018) examined the emerging and most critical challenges of CTI with blockchain technology (Abu et al., 2018). Additionally, Samtani et al. utilise the framework of AI use cases by NIST to approach the classification of AI use (Samtani et al., 2022). These publications contribute to understanding the CTI tactical environment.

Globally, CTI sharing initiatives have shown promising impacts (Solansky & Beck, 2021). For example, the Cyber Threat Alliance aimed at a shared platform for cybersecurity companies to collaborate, share resources to research, and combat sophisticated cyber threats (Zrahia, 2018). Another example of a CTI sharing initiative is the Financial Services Information Sharing and Analysis Center (FS-ISAC), which enables information sharing between financial institutions and enhance the sector to respond more appropriately to cyber threats (Information Sharing and Analysis Centers ISACs, 2022; Liu et al., 2014). ISAC's participation in different sectors has been created to provide a platform for sharing threat intelligence with partners to defend against attacks more effectively (Liu et al., 2014). Nevertheless, CTI sharing is not easy, and many challenges may be associated with it. Current CTI sharing in Nigeria is characterised by difficulties preserved (Ibrahim, 2016).

Challenges in CTI Sharing in Nigeria

Challenges in CTI sharing in Nigeria are multifaceted (Ibrahim, 2016; Pantserev, 2022). The challenges are associated with a standard for networks, protocols, and platforms for effectively and efficiently providing CTI sharing (Deloitte, 2022).

Another problem of CTI sharing is the absence of trust and agreement based on data privacy concerns, competitive market advantages, and data sovereignty (Agbali et al., 2020).

The third problem is that organisations lack the knowledge and resources to participate fully in CTI-sharing initiatives (Ibrahim, 2016). To solve these problems, everyone in Nigeria's cybersecurity ecosystem must work together to build robust trust frameworks and improve capacity building. These obstacles make it harder for different parties involved in Nigeria's cybersecurity to share information and work together effectively. This review stresses how important CTI sharing is for protecting Nigeria's national security and digital infrastructure.

Considering this, the current study endeavours to understand how Nigerian cyber security practitioners share cyber threat intelligence and the impediments that prevent them from sharing. This phenomenon has not been studied much in Nigeria; therefore, there is a knowledge gap.

METHODOLOGY

Patton (2014) and Creswell (2014) advise researchers to choose appropriate methodologies and strategies that align with the research's objectives. This methodology can significantly impact the effectiveness of the overall plan. The research chose the qualitative approach because qualitative methods facilitate the study of issues in depth and detail and are used in a descriptive term to a layman's understanding (Creswell, 2014; Glaser et al., 1968; Patton, 2014). Also, the study chooses grounded theory data analysis because it offers a robust framework for understanding complex phenomena by systematically deriving theory from data without preconceived notions or bias (Glaser et al., 1968). The method allows the study to explore the data's nuances, patterns, and interactions, leading to insights and theory development (Birks et al., 2019). Fourteen (14) interviews with cyber security practitioners were conducted, as shown in Table 1.

Table 1. Description of participants' academic qualifications, years of experience and organisations in the study

Participant	Academic Qualification	Years of Experience	Organization Size
IS Auditor J	Postgraduate	12 Years	Medium Enterprise
Cyber security analyst S	Postgraduate	9 Years	Large Enterprise
Cyber security engineer I	Postgraduate	10 Years	Large Enterprise
Cyber security instructor H	Postgraduate	17 Years	Medium Enterprise
Cyber security consultant O	Postgraduate	15 Years	Small Enterprise
Cyber security engineer P	Graduate	6 Years	Small Enterprise
Pen tester I	Graduate	5 Years	Small Enterprise
Cyber threat analyst O	Postgraduate	16 Years	Large Enterprise
Chief of security & digital trust M	Postgraduate	9 Years	Large Enterprise
Cyber threat analyst G	Postgraduate	8 Years	Small Enterprise
Cyber threat analyst L	Graduate	7 Years	Medium Enterprise
Chief of security & digital trust E	Graduate	11 Years	Large Enterprise
Cyber security engineer C	Postgraduate	8 Years	Small Enterprise
Cyber security consultant T	Postgraduate	12 Years	Large Enterprise

Research Sites

I have got 14 cyber security practitioners from a collection of 10 research sites in Nigeria. The research sites are all types of organisations: governments, privates, large enterprises, medium enterprises, and small enterprises. The study interviewed cyber security practitioners from different organisations of different sizes to get triangulated data (Lemon & Hayes, 2020).

Nigeria was chosen as the research site for this study. Nigeria is the largest economy in Nigeria (Michael, 2023). Africa is home to the second-highest fixed wired internet subscriptions and the highest mobile broadband subscriptions (International Telecommunication Union). Theoretical sampling was applied to select the cyber security practitioners from whom the data was collected in Nigeria. Glaser et al. (1968) state that theoretical sampling is the data collection process for generating theory (Glaser et al., 1968). Also, the snowballing technique was applied to select more cybersecurity practitioners. All participants have years of experience in either computer emerging response teams (CERT), security operation centres (SOC), or their equivalence.

Data Collection

Open-ended and semi-structured interviews were used to get information from the remote research sites (MS Teams). Participants were given an interview guide outlining the subject matter (see Appendix 1) and a consent form permitting them to be quoted anonymously in the study before each interview (see Appendix 2). Patton's qualitative interview strategies were used to model the structure of these open-ended interviews and this guide (Patton, 2014). Although the basic questions were planned ahead of time and asked of all participants, the exact wording and order of the questions were changed during the interviews. The anonymity of any data used for publication was guaranteed to the participants. Fourteen (14) cyber security practitioners were interviewed: 3 cyber threat analysts, 3 cyber security engineers, 2 chiefs of security and digital trust, 2 cyber security consultants, a penetration tester, a cyber security analyst, a cyber security auditor, and a cyber security instructor.

Table 1 shows a summary of this distribution, and each participant was given a number to make them easier to find. The interviews were conducted online using

Microsoft Teams in English. All participants spoke English well, even though it wasn't their first language. Interviews lasted between 40 and 60 minutes. All but one of the interviews were recorded, but one of the practitioners refused to be recorded. Notes were taken and written up during and right after that person's sessions.

Detailed transcriptions of the interviews were made. The audio recordings were reviewed again to ensure accuracy, and the transcripts were checked for errors. Maintaining the integrity of the data collected required meticulous attention to detail during the transcription process. This systematic approach ensured that the collected qualitative data was accurate and reliable, laying the groundwork for the following parts of the research.

Data Analysis

Four primary components comprised the data analysis for this study.

Open Coding

In this study, interview transcripts were analysed sentence by sentence. A brief descriptive sentence represented each code. This method provided a quick and straightforward way to begin the analysis process by identifying preliminary codes, which were subsequently compiled (Charmaz & Belgrave, 2012).

The initial codes at the early stage were provisional and underwent a rapid evolution as data analysis advanced. Concept classification was applied to categorise the vast amount of data; as data collecting continued, the categories became saturated (Creswell, 2014). This classification served as the foundation for the grounded theory that followed.

Memoing

The researcher records his thoughts and ideas by creating memos that detail the codes and their interrelationships. Memo writing was employed to capture and refine ideas identified through open coding as they evolved into categories (Glaser & Strauss, 2014). Every memo contained a brief essay on the subject and a few quotes that served as crucial evidence. Writing memos aids in the clarification,

amplification, and sharpening of categories, which change as more transcript data is added (Rashina Hoda et al., 2011).

Constant Comparison

In grounded theory, constant comparison means comparing data as it is being gathered and analysed to find trends and groups (Urquhart & Fernández, 2013). The researcher repeatedly compares new data with data that have already been collected to improve ideas and build theories. This method ensures that theoretical insights come from the data, not from ideas already thought of.

The constant comparison allows the study to develop a theory based on reality (Creswell, 2014).

Saturation Period

In grounded theory, the term "saturation period" describes the moment data collection reaches a degree of redundancy, meaning that adding new data no longer significantly advances the emerging theory (Glaser & Strauss, 1967). When a researcher has collected enough different kinds of data to get a complete picture of the thing they are studying, this is called "data saturation" (R Hoda et al., 2011). Saturation guarantees the integrity and reliance of the research findings by ensuring that empirical data fully substantiates and supports the emergent theory. Using this method, researchers can safely draw conclusions and build theoretical frameworks from their gathered data.

FINDINGS

Sharing cyber threat intelligence is essential for cyber security practitioners who want to be better prepared for cyber threats, lower risks, help other practitioners, and meet regulatory compliance requirements. Cybersecurity practitioners in Nigeria are enthusiastic about sharing and receiving cyber threat intelligence.

However, certain barriers hinder or limit their involvement in disseminating such cyber threat intelligence inside Nigeria. This study showed obvious patterns among the cyber security practitioners who took part. The subsequent section will examine the patterns.

This section delves into three memos concerning cyber threat intelligence sharing. The first memo portrays practitioners who share cyber threat intelligence.

In the second memo, we encounter practitioners who indicate a lack of standardisation as Nigeria's cybersecurity practitioners' main challenge in sharing cyber threat intelligence. Lastly, the third memo outlines practitioners who want to share cyber threat intelligence but have Data privacy concerns.

Collaborative Sharing of Cyber Threat Intelligence

Collaboratively sharing cyber threat intelligence in Nigeria is essential in enhancing the country's collective cybersecurity posture and resilience. The collaboration promotes a culture of transparency and trust among stakeholders within Nigeria. The willingness to share cyber threat intelligence in Nigeria is rooted in recognising cyber threats evolving and interconnected nature.

During research interviews, some respondents expressed the importance of freely sharing and receiving cyber threat intelligence with other practitioners in Nigeria. According to a practitioner, *"There are a lot of benefits because the importance of sharing threat intelligence is to minimise cyber-attacks, reduce threats, and guide against the techniques of the threat actors"* (IS Auditor J).

Also, (Cyber security analyst S) said, *"Knowledge sharing is very key in our organisation."* Another practitioner said, *"Cyber security intelligence sharing helps organisations work together to protect themselves against cyber-attacks, detect and respond to threats"* (Cyber security expert I). Practitioner (Cyber security instructor H) said, *"Cyber threat intelligence sharing helped me to have an idea of what I am going in for ... the kind of thing that I should expect ... What the threat actors would be doing, the kind of tools that the threat actors use."*

Another practitioner is of the opinion that sharing and receiving cyber threat intelligence is not only beneficial to their organisation but the whole world, *"Cyber threat intelligence sharing keeps organisation abreast of malicious actions that are not only peculiar to them but global"* (Cyber security consultant).

Collaborative cyber threat intelligence sharing is necessary in today's interconnected digital landscape. It serves as a cornerstone for building resilience against evolving cyber threats, fostering a community-driven approach to cybersecurity that is greater than the sum of its parts. As cyber threats continue to escalate in complexity and scale, embracing collaborative intelligence sharing is imperative to safeguarding digital assets and preserving the integrity of digital infrastructure.

In conclusion, collaborative cyber threat intelligence sharing within Nigeria is fundamental to the country's cybersecurity. It is a proactive strategy driven by collectively recognising shared threats and responsibilities. This collaborative approach enhances the country's overall resilience and underscores the importance of a cohesive and cooperative cybersecurity community in Nigeria.

Standardisation Challenges

Standardisation of cyber threat intelligence sharing is essential to improving the effectiveness of sharing valuable information among governments, organisations, and cybersecurity practitioners. However, the lack of standardised protocols and frameworks in Nigeria for cyber threat intelligence sharing creates numerous challenges for cybersecurity practitioners in Nigeria.

According to a practitioner, *"If there are no standardisation around, this will be a challenge for practitioners willing to share cyber threat intelligence"*

(IS Auditor J). Another practitioner affirms that Nigeria has no standard way of sharing cyber threat intelligence with other practitioners, *"There's no single adopted standardisation across how you can share information to several organisation."* (Pen tester)

A practitioner believes that adopting a single standard and platform for sharing cyber threat intelligence in Nigeria will help. *"Adopting common standards, formats, protocols, and platforms for exchanging threat intelligence will go a long way"* (Cyber Threat Analyst). Also, A practitioner (Cyber security expert I) said, *"Promoting the adoption of standard formats and protocols for sharing cyber threat intelligence is important."*

Adopting standardised protocols for sharing cyber threat intelligence is of utmost importance in bolstering the effectiveness of cybersecurity defence. This technology-enhanced information sharing within organisations enables them to promptly address potential threats and collaborate to manage and reduce cyber risks successfully.

Data Privacy Concerns

Data privacy preservation is a fundamental element of security and ethics, and its significance has grown considerably in the era of digital technology. However, data privacy concerns are a significant issue for Nigeria cybersecurity practitioners who share cyber threat intelligence.

A practitioner believed that scrutinising data privacy while sharing will help minimise data privacy concerns. *"They must put in into consideration the data privacy knowledge and see how best that can be resolved while sharing intelligence"* (Cyber security instructor H).

Another practitioner highlighted the classification of personal data as a challenge: *"Classification of sensitivity of the data or treat that is also an issue that arises many times"* (Cyber security Engineer P). Differences in legal and privacy law are another challenge other practitioners underline. *"Many countries have strict data protection and privacy laws that prohibit sharing sensitive data"* (Cyber security expert).

The practitioner said, *"There are also some legal concerns in terms of data privacy and protection."* (IS Auditor J). Another practitioner said the main challenge is a real lack of trust, *"The main challenge is really about trust; this is one of the major issues"* (Chief of Security & Digital Trust).

Data privacy concerns are one of the obstacles preventing Nigeria cybersecurity professionals from sharing cyber threat intelligence. To ensure that cyber threat intelligence sharing in Nigeria is effective and respectful. A combination of awareness, legal compliance and ethical best practices is required.

DISCUSSION

In the introduction, we stated the following research question: What factors influence cyber security practitioners sharing cyber threat intelligence in Nigeria? To answer this question, we conducted research interviews with 14 cybersecurity practitioners to analyse the data. Thus, at the end of the paper, we found that two impediments to cyber threat intelligence sharing in Nigeria:

Firstly, competing standards are a big problem for cyber threat intelligence sharing in Nigeria. With several different standards also present, usually some confusion and inefficiencies emerge. Cybersecurity practitioners in the public and private sectors long for standards to be followed in Nigeria. The inconsistency poses a significant barrier to the establishment of trust. Unless practitioners and organisations know that the information they exchange (primarily data) or services they use conform to universally accepted standards. This uncertainty makes cyber security practitioners lose confidence in sharing or receiving cyber threat intelligence.

With different standards, you get compatibility issues; there is a greater possible risk of data integrity loss. Because standards are inconsistent, and there are far too many of them—from the various lines at each major company to all government standardisations alone—cooperation is fractured. Such uncertainty increases operational risk without yielding a clear benefit while being costly and time-consuming.

Adopting standard protocols for sharing cyber threat intelligence in Nigeria is very important. It will make cybersecurity defence much more effective. Adopting these protocols may give cyber security professionals in the country the power to quickly improve the sharing of cyber threat intelligence to stop potential threats. Moreover, it will foster collaborative initiatives, ultimately leading to successful cyber risk management and reduction.

Secondly, Practitioners in Nigeria lack deep knowledge and skills about data privacy and are primarily opposed to sharing cyber threat intelligence. This knowledge gap raises concerns about sensitive data misuse, making collaboration difficult. The lack of data protection-related skills in many sectors prevents

effective cyber threat intelligence sharing in the country. Moreover, there is no awareness of what to do with data breaches at many organisations, which means people hold back on their willingness to share information.

Fortunately, recognising that these educational deficiencies must be addressed is essential for future times in a more collaborative cybersecurity environment; people will have the competence and resources to share intelligence effectively to combat cyber threats together.

Other papers have presented different problems of CTI sharing, such as the lack of standardised protocols and trust issues among organisations (Abu et al., 2018; Aliyu et al., 2020; Ampel et al., 2024; Knake, 2018). Furthermore, competing standards further aggravate these difficulties and hinder threat information sharing. These problems are especially compounded in Nigeria. Various standards represent a significant hurdle to CTI sharing in Nigeria. Additionally, the lack of data privacy skills for many Nigerian cyber security practitioners to fully understand and operate within data privacy regulations also adds to the problem. Solving these challenges highlights the need to create a framework of standard protocols, trust among stakeholders and knowledge skill transfer for cybersecurity practitioners in Nigeria.

Although qualitative research suffers considerable constraints in terms of subjectivity, limited generalizability, and serialised bias, it may be deemed rich in detail and context. To overcome subjectivity and ensure data accuracy, I triangulated the results, the audio recordings during the interviews were rechecked, and the transcripts were proofread to avoid potential errors. Furthermore, Interviewing cybersecurity experts gave me their insights and real-world experience, which added to the reliability of my data. The application of this multifaceted approach and data triangulation allowed the validity of the research to be strengthened and the depth of the analysis of cybersecurity practices increased.

CONCLUSIONS

The sharing of cyber threat intelligence is essential in addressing the extensive challenges posed by cyber threats. This study fills the literature gap in cyber threat intelligence sharing in Nigeria. We hypothesise that we want to maximise this cyber threat intelligence Sharing to resist malicious attackers. Therefore, this research investigates the factors that influence the cyber threat intelligence sharing of Nigeria's cyber security practitioners.

To achieve this aim, we conducted research interviews with 14 cyber security practitioners using a semi-structured, open-ended interview guide, which was recorded and transcribed. We analysed the data using an approach informed by grounded theory. We coded the data, organised the data into categories, and used constant comparison to check our code's consistency and accuracy. We developed memos from which our descriptive grounded theory emerged.

In answer to our research question, we found that cybersecurity practitioners in Nigeria are enthusiastic about exchanging and collaboratively receiving cyber threat intelligence. However, we discovered two critical impediments to sharing cyber threat intelligence in Nigeria. Firstly, the existence of competing standardisation in cyber threat intelligence sharing and, secondly, the lack of practitioner's skills in data protection. These barriers inhibit cyber security practitioners' involvement in disseminating such cyber threat intelligence sharing inside Nigeria. Based on our findings, we conclude that adopting a single cyber threat intelligence sharing framework to overcome the existence of competing standardisation will increase the sharing of cyber threat intelligence in Nigeria. Furthermore, cyber security practitioners' data privacy training and awareness are needed to bridge the gap in Nigeria's lack of practitioner skills in data protection. For further research, we are expanding data collection to create a more detailed taxonomy of factors that inhibit cyber threat intelligence sharing in Nigeria.

REFERENCES

- Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence—issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, 10(1), 371-379.
- Abubakar, A., Bass, J. M., & Allison, I. (2014). Cloud computing: Adoption issues for sub-saharan African SMEs. *The Electronic Journal of Information Systems in Developing Countries*, 62(1), 1-17.
- Agbali, M., Dahiru, A. A., Olufemi, G. D., Kashifu, I. A., & Vincent, O. (2020). Data Privacy and Protection: The Role of Regulation and Implications for Data Controllers in Developing Countries. In *Information and Communication Technologies for Development* (pp. 205-216). https://doi.org/10.1007/978-3-030-65828-1_17
- Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: a review and research agenda for practice. *Computers & Security*, 103352.
- Alexander, A. O. (2020). *Unveiling the cost of cybercrime in Africa*. <https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html>
- Aliyu, A., He, Y., Yevseyeva, I., & Luo, C. (2020). Cyber security decision making informed by cyber threat intelligence (CYDETI): IEEE CNS 20 poster. 2020 IEEE Conference on Communications and Network Security (CNS),
- Ampel, B. M., Samtani, S., Zhu, H., Chen, H., & Nunamaker Jr, J. F. (2024). Improving Threat Mitigation Through a Cybersecurity Risk Management Framework: A Computational Design Science Approach. *Journal of Management Information Systems*, 41(1), 236-265.
- Birks, M., Hoare, K., & Mills, J. (2019). Grounded theory: the FAQs. *International Journal of Qualitative Methods*, 18, 1609406919882535.

Charmaz, K., & Belgrave, L. (2012). Qualitative interviewing and grounded theory analysis. *The SAGE handbook of interview research: The complexity of the craft*, 2, 347-365.

Chris, J., Lee, B., David, W., Julie, S., & Clem, S. (2016). *NIST Guide to Cyber Threat Information Sharing*.
<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf>

Creswell, J. W. (2014). *Research Design Qualitative, Quantative and Mixed Methods Approaches*. SAGE.

Deloitte. (2022). *Nigeria Cybersecurity Outlook 2022*.
<https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/Nigeria-Cybersecurity- Outlook-2022.pdf>

Drake, D. B., Steckler, N. A., & Koch, M. J. (2004). Information Sharing in and Across Government Agencies. *SocialScience Computer Review*, 22(1), 67-84.
<https://doi.org/10.1177/0894439303259889> ENISA. (2020). *Cyber threat intelligence CTI overview*.

Gil-Garcia, J. R., Guler, A., Pardo, T. A., & Burke, G. B. (2019). Characterizing the importance of clarity of roles and responsibilities in government inter-organizational collaboration and information sharing initiatives. *Government Information Quarterly*, 36(4). <https://doi.org/10.1016/j.giq.2019.101393>

Gil-Garcia, J. R., & Sayogo, D. S. (2016). Government inter-organizational information sharing initiatives: Understanding the main determinants of success. *Government Information Quarterly*, 33(3), 572-582.
<https://doi.org/10.1016/j.giq.2016.01.006>

Glaser, B., & Strauss, A. (1967). *The discovery of grounded theory: strategies for qualitative research*.

Glaser, B., & Strauss, A. (2014). Applying grounded theory. *The Grounded Theory Review*, 13(1), 46-50.

Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). The discovery of grounded theory; strategies for qualitative research. *Nursing research*, 17(4), 364.

Hoda, R., Noble, J., & Marshall, S. (2011). Developing a grounded theory to explain the practices of self-organizing Agile teams. *Empirical Software Engineering*, 17(6), 609-639. <https://doi.org/10.1007/s10664-011-9161-0>

Hoda, R., Noble, J., & Marshall, S. (2011). Grounded theory for geeks. Proceedings of the 18th conference on pattern languages of programs,

Ibrahim, S. (2016). Causes of socioeconomic cybercrime in Nigeria. 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF),

Information Sharing and Analysis Centers ISACs. (2022). *About Information Sharing and Analysis Centers*. <https://www.nationalisacs.org/about-isacs>

International Telecommunication Union. *World Telecommunication/ICT Indicators Database 2023 (27th edition/December 2023)*. <https://datahub.itu.int/data/?e=NGA>

INTERPOL. (2022). *Africancyberthreat assessment report*. Downloads/AfricanCyberthreatAssessment_ENGLISH.pdf

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

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

Karlsson, F., Frostenson, M., Prenkert, F., Kolkowska, E., & Helin, S. (2017). Inter-organisational information sharing in the public sector: A longitudinal case study on the reshaping of success factors. *Government Information Quarterly*, 34(4), 567-577. <https://doi.org/10.1016/j.giq.2017.10.007>

Knake, R. K. (2018). Sharing classified cyber threat information with the private sector.

Lemon, L. L., & Hayes, J. (2020). Enhancing trustworthiness of qualitative findings: Using Leximancer for qualitative data analysis triangulation. *The Qualitative Report*, 25(3), 604- 614.

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(1), 2.

Malinka, K., Hujňák, O., Hanáček, P., & Hellebrandt, L. (2022). E-Banking Security Study—10 Years Later. *IEEE Access*, 10, 16681-16699.

Michael, C. (2023). *Africa's powerhouses: 10 largest economies on the continent in 2023*. Retrieved 16 December 2023 from <https://businessday.ng/news/article/africas-powerhouses-10-largest-economies-on-the-continent-in-2023/#:~:text=Nigeria%20has%20Africa's%20largest%20economy,to%20global%20oil%20price%20changes.>

Morufu, O., Juliana, N., Abdulhamid, S. i. M., & Odey, P. (2019). Performance Analysis of Security Information and Event Management Solutions Detecting Web-Based Attacks.

Nainna, M. A., Bass, J. M., & Speakman, L. (2024). Factors Amplifying or Inhibiting Cyber Threat Intelligence Sharing. *Information Systems*

NITDA. (2022). *National Information Technology Development Agency, (NITDA). Computer Emergency Readiness and Response Team CERRT Report*. <https://nitda.gov.ng/computer-emergency-readiness-and-response-team-unit/>

ONSA. (2022). *Office of National Security Adviser, Nigeria*. <https://ctc.gov.ng/about-ctc/>

Pantserev, K. A. (2022). Malicious use of artificial intelligence in Sub-Saharan Africa: Challenges for Pan-African cybersecurity. *Vestnik RUDN. International Relations*, 22(2), 288-302.

Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice*. Sage publications.

Ponemon Institute. (2018). *Exchanging Cyber Threat Intelligence: There Has to Be a Better Way*.

Samtani, S., Chen, H., Kantarcioglu, M., & Thuraisingham, B. (2022). Explainable artificial intelligence for cyber threat intelligence (XAI-CTI). *IEEE Transactions on Dependable and Secure Computing*, 19(4), 2149-2150.

Sauerwein, C., Pekaric, I., Felderer, M., & Breu, R. (2019). An analysis and classification of public information security data sources used in research and practice. *Computers & Security*, 82, 140-155. <https://doi.org/10.1016/j.cose.2018.12.011>

Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the ‘Cyberthreat- Intelligence (CTI) capability’ that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security*, 92, 101761.

Solansky, S. T., & Beck, T. (2021). Interorganizational Information Sharing: Collaboration during Cybersecurity Threats. *Public Administration Quarterly*, 45(1).

Sullivan, C., & Burger, E. (2017). “In the public interest”: The privacy implications of international business-to-business sharing of cyber-threat intelligence. *Computer Law & Security Review*, 33(1), 14-29. <https://doi.org/10.1016/j.clsr.2016.11.015>

Tounsi, W. (2019). What is cyber threat intelligence and how is it evolving? *Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT*, 1-49.

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>

Tran, J. L. (2016). Navigating the cybersecurity act of 2015. *Chap. L. Rev.*, 19, 483.

Urquhart, C., & Fernández, W. (2013). Using grounded theory method in information systems: The researcher as blank slate and other myths. *Journal of Information Technology*, 28(3), 224- 236.

Yang, A., Kwon, Y. J., & Lee, S.-Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems*, 120(9), 1777-1794.

Yang, T.-M., Zheng, L., & Pardo, T. (2012). The boundaries of information sharing and integration: A case study of Taiwan e-Government. *Government Information Quarterly*, 29, S51-S60. <https://doi.org/10.1016/j.giq.2011.08.014>

Yang, T., & 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. <https://doi.org/10.1016/j.giq.2010.06.008>

Yang, T., Pardo, T., & Wu, Y. (2014). How is information shared across the boundaries of government agencies? An e-Government case study. *Government Information Quarterly*, 31(4), 637-652. <https://doi.org/10.1016/j.giq.2014.05.002>

Zibak, A., & Simpson, A. (2019). Cyber threat information sharing: Perceived benefits and barriers. Proceedings of the 14th international conference on availability, reliability and security,

Zrahia, A. (2018). Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views. *Journal of Cybersecurity*, 4(1), tyy008.

APPENDIX 1

INTERVIEW GUIDE

1. Research project title
Cyber threat intelligence sharing in Nigeria
2. Invitation
You are being invited to take part in this research project. Before you decide to do so, it is important that you understand why the research is being conducted and what it will involve. Please take the time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything not clear or if you would like more information.
3. What is the project's purpose?
The aim of the research is to identify and discover the relationships between barriers that prevent practitioners from exchanging cyber threat intelligence
4. Why have I been chosen?
You have been chosen because you are a practitioner with specialist skills and knowledge of cyber threat intelligence.
5. Do I have to take part?
It is up to you to decide whether or not to take part. If you do decide to take part, you will be able to keep a copy of this information sheet and you should indicate your agreement on the consent form.
6. What will happen to me if I take part?
You will be asked to be interviewed to find out more about your cyber threat intelligence sharing experiences and views.
7. What do I have to do?
You will be asked to answer questions in the interview either physically or virtually using MS Teams. You will then be asked to give responses based on your experience or your impressions.

8. What are the possible disadvantages of taking part?

Participating in the research is not anticipated to cause you any disadvantages or discomfort. The potential physical and/or psychological harm or distress will be the same as any experienced in everyday life.

9. What are the possible benefits of taking part?

Whilst there are no immediate benefits for research participants, the overall aim of the research, from the research perspective, is to improve the cyber threat intelligence sharing among cyber security practitioners.

10. Will my taking part in this project be kept confidential?

You will have the choice for your responses to be kept confidential. You will also have the choice to allow us to use your name, job title or affiliation by granting such permission on the consent form.

11. Will I be recorded, and how will the recorded media be used?

Interview participants will be audio recorded during the interview. Audio recordings will be kept confidential. The audio recording will be transcribed verbatim into a script describing your words. These words will be analysed and maybe quoted in presentations, publications or thesis. The quotes will be kept anonymous or attributed to you or your affiliation depending on the permission you grant on the consent form.

12. What type of information will be sought from me and why is the collection of this information relevant for achieving the research project's objectives?

The interview will ask you about your perceptions on cyber threat intelligent sharing current practices. Your experience is just what the research is interested in exploring.

13. What will happen to the results of the research project?

The result will be used in presentations, publications and thesis. (subject to confidentiality and dissemination contract clauses).

14. Who is organising and funding the research?

This project is being conducted by Abubakar Muhammad Nainna with funding from National Information Technology Development Agency (NITDA) Nigeria.

15. Who has ethically reviewed the project?

This project has been approved by the ethical review committee of the University of Salford, Manchester, United Kingdom.

16. Contacts for further information

Abubakar Muhammad Nainna
University of Salford
Computer Science and Software Engineering
New SSEE Building, Room 02.22
The Crescent
Manchester, M5 4WT
Telephone (external) +44 (0) 7733118265, +234 703 869 7569
email: a.n.muhammad@edu.salford.ac.uk

APPENDIX 2

PARTICIPANT CONSENT FORM

Thank you for agreeing to take part in this research titled cyber threat intelligence sharing in Nigeria. This participant consent form explains what will happen if you choose to take part in this evaluation, so you can make an informed choice about whether or not to take part. Participation is voluntary.

What will I be asked to do if I participate? Interviews will be conducted physically or virtually over Teams for up to 50-60 minutes.

What will happen to the information I provide? The meeting will be recorded with your consent (audio only) and transcribed. You have the option (below) to remain anonymous or allow your name to be associated with the data you provide. Data will be stored securely for 7 years before being destroyed and will only be used by the researcher conducting the evaluation at Computer Science and Software Engineering at University of Salford. You can request a copy of the data. Data will be analysed and may be used for related presentations, publications, and thesis. If you would like to receive a copy of the study when it is finalized, please indicate this below.

What if I want to withdraw from the evaluation? If you do consent to participate, you may withdraw within 7 days by contacting Abubakar Muhammad Nainna. You are free to leave the interview discussion at any time. You may also refuse to answer any questions that you do not wish to answer during the interview.

Who is conducting the evaluation? The evaluation is being led by Abubakar Muhammad Nainna under the supervision of Professor Julian M Bass and Dr Lee Speakman of the Computer Science and Software Engineering at University of Salford, Manchester, United Kingdom.

Please indicate your consent and sign overleaf.

Please tick, if you agree:

I have read the consent form Sheet and understand the purpose of the research

I am over 18 years of age

I freely agree to participate in this evaluation as described and understand that I am free to withdraw within 7 days of my interaction with the project

Please tick one:

I consent to being referred to by name in the research and any other publications relating to the research; or

I consent to being referred to by my place of work and title in the research and any other publications relating to the research; or

I consent to the information I provide being used for the purposes of the aforementioned study only if it is fully de-identified (anonymized)

Optional:

I would like to receive a copy of the research when it becomes publicly available

Name of Participant (please print):

Signature of Participant: _____

Date: _____

Declaration by Researcher:

I have given a verbal explanation of the research; its study activities and risks and I believe that the participant has understood that explanation.

Researcher Signature:

Date: _____