# Towards a Comprehensive Cybersecurity Information Sharing Framework

**Unarine Manari, Sipho Ngobeni, Mpho Letshwenyo, Kedimotse Baruni, Nomalisa Ndhlovu and Senamela Pertunia**
Council for Scientific and Institutional Research, Pretoria, South Africa

umanari@csir.co.za
sngobeni@csir.co.za
mletshwenyo@csir.co.za
kbaruni@csir.co.za
nndhlovu@csir.co.za
psenamela@csir.co.za

**Abstract:** In today's digital age, cybersecurity has become a critical concern for nations around the world. With South Africa facing a significant cybersecurity challenge, ranking as the most targeted country on the African continent. The number and sophistication of cyber-attacks such as ransomware attacks, data breaches, phishing and pharming attacks have been steadily rising in recent years with the public sector and financial institutions being highly prone to these attacks. As cyber threats grow in sophistication and frequency, the need for robust defences and proactive measures is of high importance. Information sharing helps organizations and governments to analyse and understand existing cyber-attack trends and use the intelligence gathered to prevent future cyber-attacks, this helps to improve their overall security posture. It is evident from several scholars that organizations that share cybersecurity information have a high probability of reducing cyber-attacks within their environments. Most scholars agrees that, generally, information sharing, and collaboration may greatly reduce cybersecurity risk while ensuring resilience. But confusion and controversy remain around the following particulars such as: Who should share information? What should be shared? When should it be shared? What is the quality and utility of what is shared? How should it be shared? Why is it being shared? What can be done with the information? This paper therefore seeks to analyse the existing Cybersecurity information sharing frameworks, highlight the gaps and propose a comprehensive framework. Firstly, the paper formulates metrics that are used to evaluate the various identified frameworks, then compare and contract them. We then formulate a comprehensive information sharing framework building from the identified gaps. The proposed framework will then be adopted and used by various stakeholders, such as cybersecurity organizations, government bodies, and security experts who intend to share cybersecurity information.

**Keywords:** Information sharing, Framework, Threat intelligent, Cybersecurity, Information exchange

## 1. Introduction and Background

In this digital era, data has grown to be a valuable currency due to data being mined and processed to help make critical business decisions with the use of technology. In today's digital age, cybersecurity has become a critical concern for nations around the world. With South Africa facing a significant cybersecurity challenge, ranking as the most targeted country on the African continent. The number and sophistication of cyber-attacks such as ransomware attacks, data breaches, phishing and pharming attacks have been steadily rising in recent years with the public sector and financial institutions being highly prone to these attacks. As cyber threats grow in sophistication and frequency, the need for robust defences and proactive measures is of high importance. Information sharing helps organizations and governments to ana-lyse and understand existing cyber-attack trends and use the intelligence gathered to prevent future cyber-attacks, this helps to improve their overall security posture (Rohan et.al., 2023). The demand for shared threat-intelligence has risen and as a result has prompted the development of several cybersecurity information sharing frameworks.

According to Klimburg (2012), frameworks are guiding principles that lay a foundation for creating something and achieving a specific objective. A cybersecurity framework is a structure that is made up of various security standards, guidelines and best practices for managing and maintaining cybersecurity (Goodwin and Nicholas Paul, 2016).

In the context of Cyber Threat Intelligence (CTI) information sharing, frameworks are a structured approach that outlines how cyber threat information is collected, shared and stored using various threat intelligence platforms. CTI sharing frameworks have many benefits, however there's also disadvantages amongst those being data integrity, data privacy and data accuracy. Due to the information being gathered and shared across different sectors, with different platforms being utilized and different guidelines and protocols of sharing being followed, the validity of this information has raised critical concern.

By exchanging cybersecurity information and best practices with each other, owners, operators and security experts of firms (regardless of their size) not only can pro-mote security and safety level of their organizations but also can mitigate and limit impacts of a threat or an attack (DHS, 2016). One of the successful samples of an information sharing platform is Information Sharing and Analysis Centers (ISACs) whose concept have been designed for nearly two decades. ISACs are a good way for organizations, public, private and owners of critical infrastructures to engage in with each other in information sharing in a proper and trusted platform. In this paper, we examine the various information sharing platforms and the existing cyber security information sharing frameworks to propose a comprehensive framework for use by the public and private sector.

Information sharing platforms although a good way to exchange and share threat intelligence and other cyber security information, they come with their own challenges such as: Who should share information? What should be shared? When should it be shared? What is the quality and utility of what is shared? How should it be shared? Why is it being shared? What can be done with the information? In this paper, we have carefully studied the types of data sources, types of information sharing, information sharing guidelines and protocols, existing information sharing frameworks and information sharing challenges, imposed laws and regulations. Upon investigating the types of data sources, a broad understanding of how cyber threat intelligence is shared was explored. The analysis of the existing frame-works gives a high-level overview of the methodologies and sharing platforms being utilised, this provides a baseline for understanding their benefits and limitations and to explore future improvements that can be implemented.

We have then proposed a comprehensive cybersecurity information sharing framework. The proposed cybersecurity information sharing framework addresses the information sharing challenges, technical concerns, gaps in the current frameworks and accordingly. Lastly, the last section of the paper presents conclusion and briefly outlines future work that is planned.

## 2. Methodology

This paper followed a literature analysis methodology. We firstly conducted a critical analysis and summary of existing Cybersecurity Information Sharing Framework. The then classify and contrast these frameworks with a purpose to understand their strengths and weaknesses. Our methodology also includes critical analysis of the literature with a purposed develop our own metrics that were used to evaluate the existing information sharing frameworks. For each of the presented framework, we critically check if meets the conditions of the formulated metrics for measuring information sharing frameworks. A detailed presentation of the of the analysis and results of the information sharing framework is presented in Section 4.

## 3. Existing Cybersecurity Information Sharing Framework

According to Buckley et al. (2024) a framework is a general guideline that can be adopted by organisations, and it covers many components or domains though it is not prescriptive in terms of the steps and details that must be taken. In addition, a framework only provides a general description as a basis for building something or achieving a big, useful goal. Moreover, it is used to summarize the achievement of objectives, describe the scope, guide implementation and evaluation, and determine the quality standards to be achieved. Below we provide a brief description of the existing Cybersecurity Information sharing frameworks. These frameworks analysed in this paper were selected based on their widespread adoption across industry regulatory environments and their effectiveness in facilitating subsequent information sharing. An extensive review informed the selection process of academic literature industrial white papers and governmental services security recommendations. These frameworks were chosen based on their performance in industry-based processes, their regulatory endorsements and their inclusion in International Security strategies.

Several studies and reports indicate that frameworks such as the MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) and National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), ISACs, Control Objectives for Information and Related Technologies 5 (COBIT 5) Framework are among the most referenced models for cybersecurity information sharing. The NIST cybersecurity framework is widely implemented across public and private sectors in the United States and internationally (Goodwin and Nicholas, 2015). The Cybersecurity and Infrastructure Security Agency (CISA) framework, developed by the US Department of Homeland Security, has been extensively adopted by federal agencies and critical infrastructure sectors (Al-Fatlawi et al., 2021). The information sharing and analysis centers (ISACs) model is frequently used in the financial healthcare and critical industries, ensuring collaboration and great intelligence sharing among organizations (Buckley et al., 2024). Operationally the MITRE ATTA&CK framework is an industry-recognized knowledge base that documents tactics and techniques used by cyber

adversaries, making it a vital reference for cyber security professionals worldwide (Riza et al., 2018). Below, we formulate metrics to evaluate if these frameworks are comprehensive enough for information sharing purposes:

- **Cooperative Cyber Defense Centre of Excellence (CCDCOE) Cybersecurity Framework** – is model developed by the Cyber Defense Capability Development Centre of Excellence to help organizations under-stand and improve the sharing of information by providing guidelines (Zhao and White, 2012).
- **Microsoft Cybersecurity Framework (CSF)** – serves as a guideline for organizations across various sectors to improve their cybersecurity posture. It outlines best practices for sharing cyber threat information in a secure and collaborative way (Bull et al., 2023).
- **Cybersecurity and Infrastructure Security Agency (CISA)** – this framework was established by the Department of Homeland Security to assist various sectors to share threat information, to understand how and where to share the information and what could be the repercussions for sharing and receiving threat intelligence information (Al-Fatlawi et al., 2021).
- **Information Sharing and Analysis Centers (ISACs)** – is a group of organizations from various sectors that share cyber threat intelligence information to enhance their cybersecurity knowledge and improve the overall security of their in-dividual organizations (Kwon et al., 2020).
- **Cyber Security Maturity Model (CCSMM)** – was developed to assist various sectors with information sharing. To help them identify the cyber threats. The main objective was to facilitate collaborative information security sharing (Piasecki et al., 2021).
- **SABSA (Sherwood Applied Business Security Architecture)** – is a comprehensive methodology for developing business-driven, risk-focused security architectures. The SABSA framework avoids that potential for failure by baking the requirement to clearly define the business, its information security needs, and its goals and objectives right into the very first layer of the foundation that all other layers will frame around (Bauer et al., 2020).
- **MITRE ATT&CK (MITRE Corporation Adversarial Tactics, Techniques, and Common Knowledge)** – is a comprehensive knowledge base that documents the tactics, techniques, and procedures (TTPs) used by cyber adversaries throughout the lifecycle of an attack (Azmi et al., 2018).
- **COBIT internal control framework** – is one of the most critical IT governance developments. This framework aims to set best practices in the governance and auditing of electronic information systems and related technologies. COBIT organizes IT governance objectives and best practices into domains and processes, linking them to business requirements. It was developed by the Information Systems Audit and Control Association (ISACA), founded in 1967 in the USA in response to growing computer systems concerns (McIntosh et al., 2024).
- **ITU-GCA** – is a framework aimed at enhancing cybersecurity globally through cooperation among ITU member states. ITU-GCA, has a broad scope, which can only work in international circumstances that need positive interdependence be-tween each entity, such as through international cooperation and collaboration (Forain and Sousa, 2022).
- **World Economic Forum Framework (WEF)** – the WEF Framework, is intend-ed for its members who focus on securing economic relationships. However, the principles and guidelines in the framework can potentially be adopted globally by any organization (Kemp et al., 2020)

## 4. Analysis of Existing Cybersecurity Information Sharing Framework

The section highlights a comprehensive comparison of the identified information sharing frameworks in cybersecurity. Through a detailed analysis of key metrics and points of comparison, this section evaluates the effectiveness, practicality, and scalability of these frameworks.

### 4.1 Chosen Points of Comparison for the Identified Frameworks

The comparison will touch on objectives, participants, governance, security measures, trust models, and other critical factors, with a focus on practical implementation, legal compliance, and the ability to foster collaboration across different sectors and borders. Furthermore, it will provide a comprehensive understanding of how the identified different frameworks operate and how they might be improved or adapted to meet emerging cybersecurity challenges. This section of the paper aims to compare the identified cybersecurity information sharing frameworks based on key criteria that are essential to understanding their effectiveness, practicality, and scalability. To achieve this the following points of comparison have been selected to offer a comprehensive analysis of the frameworks.

- **Objectives, Scope and Coverage**

A cybersecurity information-sharing framework's objectives help outline its main goal and the results that participants might expect. The focus of each framework may vary slightly, ranging from strategic policy formation to real-time threat intelligence to overall threat mitigation. While frameworks like Information Sharing and Analysis Centers (ISACs) may emphasize long-term strategic intelligence sharing, encouraging sector-wide collaboration to identify emerging trends, the Cybersecurity and Infrastructure Security Agency (CISA) framework assists various sectors to share, understand how and where to share the information and the repercussions for sharing and receiving threat intelligence information.

The MITRE ATT&CK, for example, primarily focuses on real-time sharing of technical indicators of compromise (IOCs) to help prevent cyberattacks. If we look at frameworks such as Cyber Security Maturity Model (CCSMM) you find that it was developed to assist various sectors with information sharing and its main objective being to facilitate collaborative information security sharing and on the other hand frameworks like the CCDCOE Cybersecurity Framework provide guidelines on how to improve cybersecurity sharing of information by providing guidelines.

- **Effectiveness and Impact**

This study will assess the effectiveness of each framework in achieving its objectives which includes improving threat intelligence, reducing the impact of cyber incidents, and enhancing the overall cybersecurity posture of participating organizations. Available data on the measurable outcomes of information sharing under each framework will be examined.

- **Legal and Regulatory Considerations**

The governance structures and legal frameworks underlying each information-sharing model are very important to ensure compliance with laws, regulations, and standards. A vast number of frameworks are influenced by national and international laws that specify the proper handling, sharing, and protection of data. Privacy frameworks/legislations such as the General Data Protection Regulation (GDPR) and Protection of Personal Information Act (POPIA) frameworks impose stringent requirements for data protection and privacy when sharing information. While frameworks like NIST Cybersecurity Framework (CSF), Control Objectives for Information and Related Technology (COBIT) focus less on regulatory compliance and more on best practices and voluntary guidelines. A comparison of governance and legal frameworks shows how regulatory environments influence the scope and operational feasibility of cybersecurity information sharing. The analysis will examine how each framework addresses legal and regulatory challenges, including data privacy concerns, intellectual property rights, and national security considerations.

- **Stakeholder Involvement**

Collaboration between a variety of stakeholders, such as governmental entities, private businesses, industry-specific associations, and occasionally even multinational organizations, must be facilitated by an effective information-sharing system. The participant composition of each framework influences the level of cooperation, trust, and information flow.

Sector-Specific ISACs such as the Financial Services ISAC (FS-ISAC), primarily focuses on private financial institutions and facilitates information sharing about cyber threats, vulnerabilities and incidents among financial institutions globally, whereas the Cybersecurity and Infrastructure Security Agency (CISA) covers all critical infrastructure sectors by providing a central hub for threat information and incident response coordination comprising both public agencies and private-sector participants. Comparing the types of participants allows for an understanding of how frameworks foster collaboration and how inclusive they are in providing access to critical threat information. This study will assess the level of stakeholder involvement in each framework, including the roles and responsibilities of government agencies, private sector organizations, and academic institutions in the information sharing process.

- **Types of Information Shared**

Understanding the scope of a framework and its ability to combat cyber-attacks hinges highly on the types of information that are shared within the framework. Cybersecurity frameworks usually enable the exchange of strategic intelligence such as emerging threat patterns, global cybersecurity trends, technical data such as malware hashes, IP addresses, tactical information such as attack methods or threat actors.

MITRE ATT&CK and ISACs promote the sharing of strategic information to improve resilience across critical infrastructures, whereas Threat Sharing Platforms like Malware Information Sharing Platform (MISP) facilitate the exchange of highly technical IOC data. The operational distinctions and constraints present in frameworks designed for particular threat situations are brought to light by the comparison of information types. The study will investigate the specific mechanisms for information sharing employed by each framework, such as secure data feeds, collaborative platforms, and threat intelligence feeds and evaluate their effectiveness and security.

- **Information Security and Privacy Measures**

Certain laws and regulations depending on a country might require high standards for data privacy/encryption for sharing IOCs, whereas frameworks in less regulated regions and countries might not have such stringent privacy controls. Identifying and understanding the security measures incorporated in each framework allows for a clear understanding of how well participant data is safeguarded against misuse, breach and leaks.

Comparing security measures (like encryption, anonymization, and access control) and privacy protections (like making sure shared data is anonymized to prevent re-identification) is essential to determining how well each framework protects the confidentiality and integrity of shared data because sharing sensitive information can expose organizations to new risks. Frameworks such as NIST-CSF as detailed as they are in terms of security controls there's still lacking security controls more related to information sharing and have limited actionable direction on control implementation

- **Trust Models**

In order to lay the groundwork for cooperation, a trust model is essential as organizations need to trust each other to share accurate and actionable data without compromising their own security.

Given the inherent risks associated with information sharing, frameworks must include procedures that ensure participant confidence.

To ensure that parties can trust the shared information, the UK's Cyber Information Sharing Partnership (CISP), for example, employs a trust mechanism based on pre-vetted private enterprises and confirmed government organizations. The Global Forum on Cybersecurity (GFCE), on the other hand, places a greater emphasis on fostering diplomatic trust in order to promote global collaboration. The scalability and longevity of a framework's capacity to foster sustained involvement and collaboration can be assessed by comparing trust models for example a trust-based model might involve a certification process to ensure that participants are legitimate and adhere to specific security practices. Comparing trust models helps to assess how frameworks build and maintain trust among participants, whether through certifications, third-party audits, or mutual agreements.

- **Scalability and Adaptability**

The framework needs to have the ability to expand as the volume of data grows or as new participants come onboard and further be able to adapt and respond to new types of threats or emerging technologies.

While some frameworks may have a more constrained ability to expand or adapt, frameworks like MITRE ATT&CK, are made to manage massive amounts of data and can swiftly scale to accommodate more participants. An understanding of the lifespan and applicability of various frameworks in the face of evolving cybersecurity challenges can be gained by comparing their scalability and adaptability.

When organizations need to share information across borders or sectors, the compatibility of various frameworks becomes a crucial point of comparison. Interoperability looks at how effectively a framework functions with other cybersecurity frameworks that are already in place. While some frameworks might function as stand-alone entities that require extra infrastructure to connect, others might be designed to effortlessly interface with already-existing government security information-sharing platforms.

- **Incident Response and Recovery Support**

The ability of an information-sharing framework to assist with incident response and recovery activities is another way to gauge its efficacy. Certain frameworks such as MITRE ATT&CK enable businesses to also swiftly and efficiently recover from attacks by offering not only intelligence but also tools for coordinated actions.

As far as our study we noted that although there's isn't a framework that facilitates real-time coordination and offers incident response expertise during ongoing cyberattacks. However, there are frameworks focused on strategic sharing such as those managed by sector-specific ISACs, which may offer post incident analysis and

recovery support. By comparing these support structures, we can assess how frameworks contribute to cyber resilience during and after an incident.

- **Technology and Infrastructure**

A strong set of technologies and infrastructure are necessary to offer an efficient framework for information sharing. Centralized platforms for data aggregation, analysis, and dissemination are crucial, often incorporating threat intelligence platforms (TIPs) and security information and event management (SIEM) systems are significantly important. Data storage solutions, including secure databases and data lakes, are needed to manage the volume and variety of shared information.

A well-defined and maintained IT infrastructure, including servers, networks, and endpoints, is critical for the reliable and secure operation of the framework. The study will look at the various technologies and infrastructure required to support the information sharing frameworks.

- **Costs and Resource Requirements**

The cost of participating in a cybersecurity information-sharing initiative is a practical consideration for many organizations. Smaller organizations may find it more difficult to use frameworks that demand large infrastructure investments, continuous maintenance, or full-time employment, while others may provide more affordable, easily accessible options.

Frameworks like CISA's Automated Indicator Sharing (AIS) may be cost-effective for government entities but less accessible to smaller private companies, which may find ISACs or open-source platforms like MISP more affordable and accessible. Comparing the costs and resource requirements allows stakeholders to assess the feasibility of participation based on available budgets and capacity.

Table 1 presents the strengths and weaknesses identified through the analysis of each of the frameworks

**Table 1: Analysis of the existing information sharing frameworks**

| Existing Information sharing frameworks | Strengths | Weaknesses (potential challenges of implementing and operating the framework) |
|---|---|---|
| **NIST-CSF** | • Incident response<br>• Real-time analysis<br>• Data protection<br>• Continuous monitoring and auditing | • Deficiency or lacking security controls<br>• Limited actionable direction on control implementation<br>• Security awareness and training<br>• Process automation<br>• Policy and compliance checks |
| **CCDCOE Cybersecurity Framework** | • Comprehensive coverage guidelines<br>• International collaboration<br>• Adaptability<br>• Focus on Capacity building | • Implementation challenges<br>• Rapid technological changes<br>• Resource intensive |
| **CISA** | • Collaboration and information sharing<br>• Sector-specific adaptability<br>• Comprehensive coverage<br>• Proactive measures<br>• Public awareness and education | • Resource constraints<br>• Rapidly evolving threat landscape<br>• Bureaucratic challenges |
| **ISACs** | • Enhanced Collaboration and information sharing<br>• Sector-specific focus<br>• Trusted community<br>• Proactive threat management | • Data privacy control<br>• Resource limitations<br>• Coordination challenges<br>• Information overload<br>• Dependency on voluntary participation |
| **SABSA** | • Business-driven<br>• Risk and opportunity focused<br>• Flexibility and customization<br>• Comprehensive Framework | • Complex implementation<br>• Resource intensive<br>• Steep learning curve |
| **MITRE ATT&CK** | • Structured approach<br>• Common Language for Cybersecurity<br>• Detailed Adversary Tactics and Techniques<br>• Versatility and applicability<br>• Continuous updates | • Data privacy concerns<br>• Complexity and overhead<br>• Integration challenges<br>• Resource intensive<br>• Focus on known techniques |

| Existing Information sharing frameworks | Strengths | Weaknesses (potential challenges of implementing and operating the framework) |
|---|---|---|
| **COBIT** | • Adaptable compliance measures<br>• Incident response<br>• Real-time analysis<br>• Data security and protection | • Process automation<br>• Continuous monitoring and auditing<br>• Policy and compliance checks |
| **World Economic Forum Framework (WEF)** | • Holistic approach<br>• Data-driven insights<br>• Focus on innovation | • Implementation challenges<br>• Resource intensive |

### 4.2 Defining Metrics for Evaluation

Below we propose and define seven metrics for determining a comprehensive information sharing framework. These metrics are then used to evaluate the existing cyber-security information sharing frameworks in the next section. The metrics are:

- **Actors involved** – This metric entails the actors involved in sharing cybersecurity-ty and related information. So, a comprehensive framework should essentially define who needs should be involved or who needs to share information, and who can resolve the issues that emerge.
- **Types of information exchanged** – Once we understand the actors that should be involved in information, we need to determine what information is being shared, and what is the purpose of sharing it. Examples, sharing actors can share information such as vulnerabilities, incidents, threats, best practices, indicators of compromise, to mention but a few.
- **Models of exchange** – This metric is more concerned with determining the impetus behind cybersecurity information sharing, in essence, we need to determine if the reason for sharing information if it is shared voluntarily or it is for fulfilling a regulatory requirement. For example, some sharing team may agree on the concept of "all or nothing". This suggests that, once an actor within a sharing team has been compromised, the actor needs to disclose all the events or indicators of compromise that led to the attack. This will then help the others sharing team to put controls in place to prevent their system from being compromised by the same ICT security threat.
- **Methods of exchange** – This metric is probably the most important one. This metric seeks to determine the organizational structure and governance for sharing information in each sharing actor or team.
- **Mechanisms of exchange** – It can be noted in Table 1 that there are various types of Cybersecurity data sources and information that could be shared among various information sharing actors. Each of the data sources may require one or more mechanisms for sharing it. This metric therefore ensures that a comprehensive information sharing framework should determine how the information is actually shared among the sharing actors or what mechanism is being used for information exchange.
- **Scope and operational purpose** – This metric seek to determine how an information exchange is structured. Defining how information exchange is structured is vital to ensure that it delivers the greatest value among the information sharing actors.
- **Data privacy –** This metric seeks to determine that all information shared via any platform has controls in place to protect the privacy of the data been shared through compliance with existing data protection laws such as General Data Protection Regulation (GDPR) in the case of the EU or Protection of Personal Information (POPI) Act, in the case of South Africa. Ensuring this will assist the sharing actors to minimize the probability of being fined or imprisoned by the supervising authority or Information Regulator in the event of a compromise of the information sharing platform.

### 4.3 Analysis

Table 2 presents a summary of the analysis results of the metric presented in Section 4.1 for evaluating existing Cybersecurity information sharing platform. This metric is depicted as "measured metric" in Table 1. The proposed CSISF is our proposed Com-prehensive framework against the existing ones presented in Section 3. The legend "✓" depicts that the measured criteria is MET and "X" depicts that the evaluated criteria is Not MET, while "(X)" depicts that the status is un-known. Though several information sharing frameworks were studied above, we chose to evaluate the ones mentioned in Table 2 because they are very close to the proposed CSISF.

**Table 2: Analysis of existing cybersecurity information sharing framework**

| Cybersecurity information sharing framework Measured Metric/Criterion | Proposed CSISF | CCDCOE | ISACS | CCSM | MITRE ATT&CK |
|---|---|---|---|---|---|
| Actors involved. | ✓ | ✓ | ✓ | ✓ | ✓ |
| Types of information exchanged | ✓ | ✓ | ✓ | ✓ | ✓ |
| Models of exchange | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mechanisms of exchange | ✓ | ✓ | ✓ | X | ✓ |
| Scope and operational purpose | ✓ | X | ✓ | ✓ | ✓ |
| Data privacy | ✓ | X | X | X | X |

### 4.4 Discussion

In this section, discuss the results from Tables 2. Is the proposed CSISF really comprehensive? What can we learn from it? What are some of the considerations that be added? What are the data privacy issues? Can this framework be adopted and used by FIRST (Forum for Incident Response and Security Teams www.first.org) members?

- **CCDOE** – similarly to the proposed CSISF, the CCDOE framework consists of most of the elements that constitute a comprehensive Cybersecurity information framework. However, the framework does clearly articulate the scope and operational purpose including data privacy.
- **ISACS** – this framework consists of almost all the elements that constitute a comprehensive cybersecurity information sharing framework except data privacy. This suggests that if sharing actors were to adopt this framework and the sharing platforms do not include data protection, the actors could be held for legal penalties if the sharing platform were to be a victim of data breach.
- **CCSM** – this framework can also be seen as comprehensive and organization are encouraged to adopt and use it their basis for sharing information, however, it does not clearly articulate the mechanism for sharing and data privacy issues.
- **MITRE and ATT&CK** – This framework is probably also one of the most widely used and comprehensive modelled around the detection, mitigation and prevention of future cyber-attacks. Despite the framework being comprehensive, it does not clearly articulate the data privacy issues which is its main drawback.

## 5. Conclusion

In order to exponentially reduce cybersecurity risk, it depends on information sharing and collaboration on a wide range of actors, including leveraging on many different factors particularly the metrics presented in this paper. Establishing an effective information sharing framework is a difficult undertaking. This paper presented several existing cybersecurity information sharing frameworks and proposed metrics to evaluate these frameworks. It was noted from the analysis that none of the existing sharing frameworks meets all the proposed metrics. Despite most of these frameworks being closely aligned with the proposed CSISF, they all do not extensively address data privacy, which is a great concern.

## References

Al-Fatlawi, Q.A., Al Farttoosi, D.S., & Almagtome, A.H. (2021). Accounting Information Security and IT Governance Under COBIT 5 Framework: A Case Study. Webology, 18(Special Issue on Information Retrieval and Web Search), pp. 294-310.

Azmi, R., Tibben, W. & Win, K.T., 2018. Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, 3(2), pp. 258-283. Doi: 10.1080/23738871.2018.1520271.

McIntosh, T.R. et al., 2024. An Analysis of Cybersecurity Frameworks. *Journal of Information Security and Applications*, 80, pp. 1-12. Doi: 10.1016/j.jisa.2024.1002694.

Bauer, S., Fischer, D., Sauerwein, C., Latzel, S., Stelzer, D. & Breu, R., 2020. Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. *Proceedings of the 53rd Hawaii International Conference on System Sciences*. Available at: https://hdl.handle.net/10125/63978 [Accessed 26 Jul. 2024].

Buckley R, Pasquale L, Nuseibeh B, Helfert M, IVI M (2024). A Review of Cyber Information Sharing in Information Sharing Analysis Centres (ISACs).

Bull, C., Galaz, L., & Rijal, D. (2023). Group Project 7.1 Enterprise Security Architecture for a Court Case Management System. Department of Cyber Security Operations and Leadership, University of San Diego. [Accessed: 25 July 2024].

Department of Homeland Security (2016). Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community.

Forain, R. de O., Albuquerque, R. & de Sousa, R.T., 2022. Towards System Security: What a Comparison of National Vulnerability Databases Reveals. *Iber. Conf. Inf. Syst. Technol. Cist.*, 2022-June(June), pp. 22–25. Doi: 10.23919/CISTI54924.2022.9820232.

Goodwin C, Nicholas Paul J (2015). A framework for cybersecurity information sharing and risk reduction, Microsoft.

Kemp, C., Calvert, C. & Khoshgoftaar, T.M., 2020. Detection methods of slow read dos using full packet capture data. In *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*. pp. 9–16.

Klimburg A. (2012). National Cybersecurity Cyber Security Framework Manual, NATO CCD COE Publication.

Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gourisetti, S.N.G. (2020). Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping. Pacific Northwest National Laboratory. [Accessed: 26 July 2024].

Piasecki, M., Urquhart, L., & McAuley, D. (2021). Cybersecurity Standards and Policies: Impact on E-Government Credibility. Electronics, 11(2181), pp. 177-207.

Rohan R, Papasratorn B, Chumtimaskul W, Hautamaki J, Funilkul S, Pal D (2023). Enhancing Cybersecurity Resilience: A Comprehensive Analysis of Human Factors and Security Practices Aligned with the NIST Cybersecurity Framework.

Sun, J. et al., 2021. Generating Informative CVE Description From Exploit DB Posts by Extractive Summarization. Available at: http://arxiv.org/abs/2101.01431.

Zhao W, White G (2012). A Collaborative Information Sharing Framework for Community Cyber Security.