CYBER HEALTH METRICS - ESTABLISH CYBER HEALTH FRAMEWORK

SADIA ANIKA MUMU
ID: 222476471

Contents

Introduction:

In the rapidly evolving landscape of cyberspace, the importance of effective cyber security measurement and management cannot be overstated. As organizations, especially small and medium-sized enterprises (SMEs) and those operating in developing economies, increasingly rely on digital technologies, they face a myriad of security challenges that demand proactive and strategic approaches. The literature review conducted in this study sheds light on the complexities of cyber security metrics and frameworks, offering valuable insights into the current state of cyber security practices and the need for continuous assessment and improvement.

The paper by Yavor Valentinov Papazov provides a comprehensive overview of cyber security metrics, emphasizing the significance of measuring and managing security in today's digital age [1]. Furthermore, the comparison between the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and other prominent frameworks highlights the need for a structured approach to cyber security measurement and management. By integrating insights from these sources, this study aims to develop a framework tailored to the unique challenges faced by SMEs and developing economies, particularly in the context of the Deakin Threat Mirror project. This framework will serve as a guide for organizations to effectively measure and manage their cyber security posture, ultimately enhancing their resilience against cyber threats.

Literature Review:

The paper on cybersecurity metrics by Yavor Valentinov Papazov provides a comprehensive overview of the field, emphasizing the importance of measuring and managing security in the rapidly evolving cyberspace domain. It delves into the definitions of metrics, frameworks for metric selection, and the structure of a metrics program [1].

The document highlights the challenges faced in securing diverse IT infrastructures against sophisticated attackers and stresses the need for continuous assessment and improvement. By focusing on metrics programs rather than individual metrics, the paper aims to guide organizations in establishing effective security measurement strategies. It also addresses the gaps in current approaches and suggests areas for further research to enhance cybersecurity practices. Overall, the paper serves as a valuable resource for understanding the complexities of cybersecurity metrics and navigating the landscape of security measurement in today's digital age [1].

This paper presents a detailed comparison between the NIST Cyber Security Framework (CSF) and other prominent frameworks such as COBIT, ISO/IEC 27001, and ISF. It identifies key information security processes addressed in some frameworks but not in NIST CSF, proposing a new Capability Maturity Model (CMM) to measure NIST CSF implementation progress [2]. The NIST CSF is viewed as a risk-based framework comprising a framework core, risk tiers, and framework profile. The framework core includes cyber security activities, and organizations use capability maturity models to assess their capabilities and make informed decisions on investment strategies for information security [2].

The study evaluates the comprehensiveness of NIST CSF to ensure it covers all necessary aspects and reviews various maturity models for applicability with NIST CSF, focusing on mapping NIST CSF control objectives with assessed areas. Three information security frameworks (ISO 27001, ISF, COBIT5) and four maturity models (ISF, PAM, SSE CMM, ONG C2M2) are considered in this evaluation. Additionally, the paper discusses the Baldrige Excellence Framework and Builder, emphasizing their role in evaluating cyber security risk management effectiveness [2]. The proposed Information Security Maturity Model for NIST CSF aims to enhance organizations' cyber security risk management efforts by providing a structured approach to measuring implementation progress and aligning with industry best practices [2].

Methodology:

Metrics Programs Overview:

In terms of metrics programs, the paper offers an overview of the components that constitute a comprehensive approach to cybersecurity measurement. It likely details the life cycle of a metrics program, starting from the initial selection of metrics that are relevant to the organization's security goals. The document may delve into the processes involved in data collection, monitoring, and establishing feedback loops to continuously assess and improve security metrics [1]. By focusing on the holistic view of a metrics program, the paper guides organizations on how to effectively implement and manage their cybersecurity measurement strategies for ongoing security enhancement.

Frameworks for Metric Selection:

The paper discusses established frameworks for selecting appropriate metrics in cybersecurity. It emphasizes the importance of methodologies and criteria that align with organizational goals and security objectives. By utilizing these frameworks, organizations can effectively measure and monitor their cybersecurity posture. The document likely provides insights into specific frameworks such as PRAGMATIC and QuERIES, which offer structured approaches to quantifying operational cybersecurity risk and selecting performance indicators [1]. These frameworks help organizations identify relevant metrics that provide meaningful insights into their security posture and enable informed decision-making.

NIST and CIS Framework:

In the paper, the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) is a key focus for organizations within critical infrastructure sectors to mitigate cyber security risks. The NIST CSF provides guidance on managing and reducing these risks through a risk-based approach, consisting of a framework core, risk tiers, and framework profile. It is emphasized that the NIST CSF is not a maturity framework, highlighting the need to adopt or create a maturity model to measure CSF implementation progress effectively [2].

On the other hand, the Centre for Internet Security (CIS) framework is not explicitly discussed in the provided excerpts. However, the CIS Controls are a set of best practices for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. These controls are organized into three categories: Basic, Foundational, and Organizational, and are regularly updated to address emerging threats and technologies [2]. The CIS Controls are widely recognized in the cybersecurity industry for their practicality and effectiveness in enhancing an organization's security posture.

While the paper primarily focuses on the NIST CSF and its alignment with other frameworks and maturity models, the inclusion of the CIS framework could further enrich the discussion on comprehensive cyber security strategies. The CIS Controls could complement the NIST CSF by offering specific technical controls and implementation guidance to enhance an organization's overall cyber security resilience [2].

Cyber Metrics Focusing on NIST and CSF:

To implement cyber metrics focusing on the NIST Cyber Security Framework (CSF), organizations can follow these steps:

- **Understand the NIST CSF Categories and Subcategories:** Familiarize yourself with the five core functions (Identify, Protect, Detect, Respond, Recover) and the corresponding categories and subcategories within the NIST CSF [2]. These provide a structured approach to organizing cyber security activities.

- **Identify Key Performance Indicators (KPIs):** Determine which metrics align with the specific categories and subcategories of the NIST CSF. For example, for the "Protect" function, KPIs could include the number of security controls implemented or the percentage of systems with up-to-date patches [2].

- **Establish Baselines and Targets:** Set baseline measurements for each KPI to understand the current state of cyber security maturity. Define target values that indicate the desired level of performance for each metric [1].

- **Implement Monitoring Tools:** Utilize security information and event management (SIEM) tools, vulnerability scanners, and other monitoring solutions to collect data relevant to the identified KPIs. These tools can help track and analyse security events and performance indicators [2].

- **Regularly Measure and Analyse Metrics:** Continuously monitor and measure the selected KPIs to track progress and identify areas for improvement. Analyse the data to gain insights into the effectiveness of security controls and processes.

- **Report and Communicate Findings:** Create reports that summarize the performance of cyber security metrics based on the NIST CSF [2]. Communicate these findings to relevant stakeholders, including senior management, IT teams, and compliance officers.

- **Iterate and Improve:** Use the insights gained from the metrics to refine cyber security strategies and enhance the organization's overall security posture [2]. Continuously iterate on the metrics based on changing threats, technologies, and business requirements.

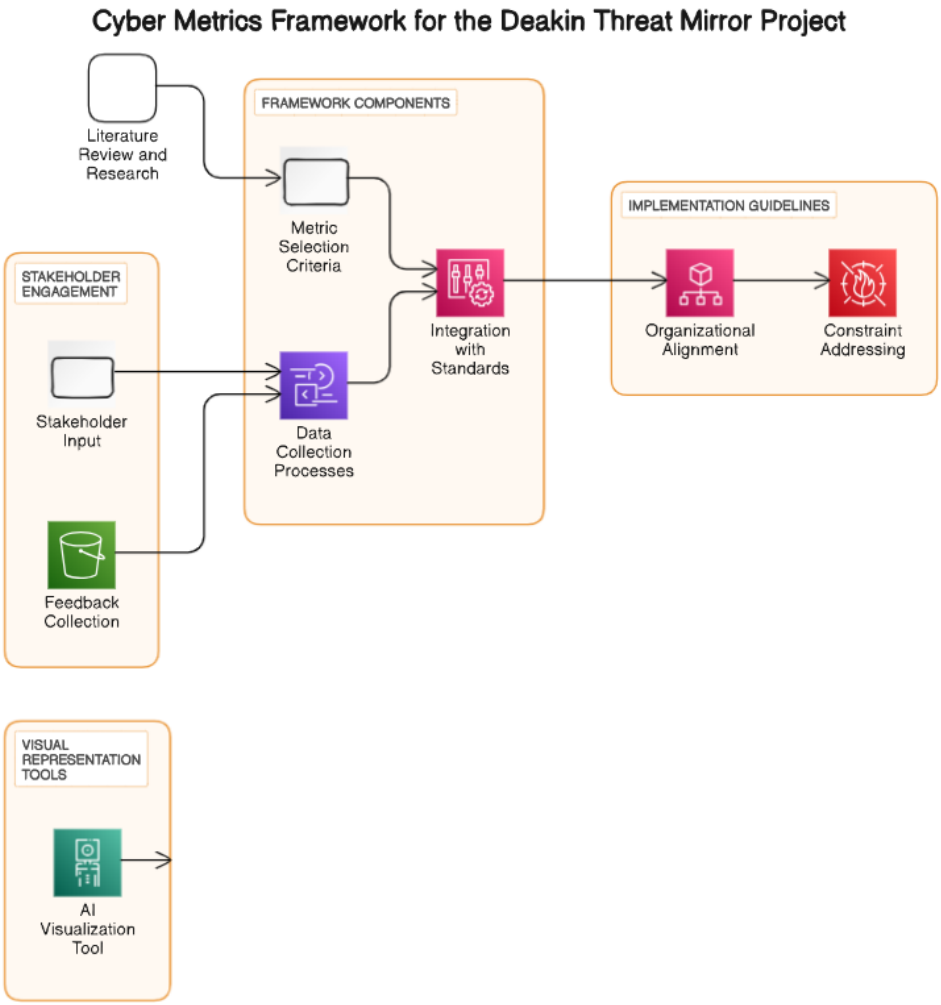
By implementing cyber metrics aligned with the NIST CSF, organizations can effectively measure their cyber security maturity, identify areas of strength and weakness, and make informed decisions to enhance their security capabilities.

Cyber Metrics focusing on Deakin Threat Mirror:

To develop a comprehensive framework on cyber metrics aligned with our project, the Deakin Threat Mirror, we can draw upon the insights gained from the literature review and methodological approaches discussed. The framework will focus on guiding organizations in effectively measuring and managing their cyber security posture, particularly tailored to the unique challenges faced by SMEs and developing economies. Below here, I have proposed a framework:

Metrics Programs Overview:

- Establish a structured approach to cybersecurity measurement, emphasizing the lifecycle of a metrics program.
- Define key components, including metric selection, data collection processes, monitoring mechanisms, and feedback loops for continuous improvement [2].
- Provide guidance on aligning metrics programs with organizational security goals and objectives, emphasizing the importance of continuous assessment and enhancement.



Frameworks for Metric Selection:

- Offer guidance on selecting appropriate metrics using established frameworks such as PRAGMATIC and QuERIES.
- Emphasize methodologies and criteria that align with organizational goals and security objectives, ensuring meaningful insights into security posture.
- Provide insights into specific frameworks and approaches for quantifying operational cybersecurity risk and selecting performance indicators relevant to SMEs and developing economies [2].

NIST and CIS Framework Integration:

- Integrate the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and the Centre for Internet Security (CIS) Controls into the framework.
- Provide guidance on leveraging the NIST CSF for risk-based cyber security management, focusing on its framework core, risk tiers, and framework profile [1].
- Highlight the practicality and effectiveness of the CIS Controls in enhancing an organization's security posture, particularly in addressing emerging threats and technologies.

Cyber Metrics Implementation Steps:

- Outline step-by-step instructions for implementing cyber metrics focusing on the NIST CSF within the Deakin Threat Mirror project.
- Provide guidance on understanding NIST CSF categories and subcategories, identifying key performance indicators (KPIs), establishing baselines and targets, implementing monitoring tools, and regularly measuring and analysing metrics [1].
- Emphasize the importance of reporting and communicating findings to relevant stakeholders and iterating on the metrics to continuously improve cyber security strategies.

By integrating these elements into a cohesive framework, the Deakin Threat Mirror project can effectively guide organizations in measuring and managing their cyber security posture, ensuring resilience against evolving threats and enhancing overall security capabilities in SMEs and developing economies.

Conclusion:

In conclusion, the literature review conducted in this study provides valuable insights into the field of cyber security metrics and frameworks, highlighting the importance of effective measurement and management in addressing the evolving threat landscape. The comparison between the NIST Cyber Security Framework (CSF) and other frameworks underscores the need for a comprehensive approach to cyber security that takes into account the unique challenges faced by organizations, especially SMEs and those operating in developing economies. By developing a framework aligned with the insights gained from the literature review, the Deakin Threat Mirror project aims to provide organizations with a practical guide for measuring and managing their cyber security posture. This framework will enable organizations to identify areas of strength and weakness, make informed decisions on resource allocation, and ultimately enhance their resilience against cyber threats. As organizations continue to navigate the complexities of cyberspace, a structured approach to cyber security measurement and management will be crucial in ensuring their long-term success and sustainability.

Reference:

[1] Y. V. Papazov, "Development and Current State of Cybersecurity and IT Security Metrics," in Proc. IEEE Int. Conf. Cybersecurity, pp. 1-18,

[2] Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for NIST Cyber Security Framework. In D. C. Wyld et al. (Eds.), ITCS, SIP, CST, ARIA, NLP - 2017 (pp. 51–62). CS & IT-CSCP. DOI: 10.5121/csit.2017.70305