Social Science and
Everant Journal
Humanities Journal

ISSN: 2456-2653
Volume 08 Issue 10 October 2024

https://sshjournal.com/
Impact Factor: 2024: 6.576
2023: 5.731

DOI: https://doi.org/10.18535/sshj.v8i10.1421

Cybersecurity in Tanzanian Maritime Operations: Exploring Global Best Practices and Their Local Adaptation Using the Cybersecurity Capability Maturity Model (C2M2)

[1]Mayala L. Patrick | [2] Edrick J. Mugisha | [3] Keneth O. Mbaga | [4] Mansour Likamba

[1,2,3,4] Dar es Salaam Maritime Institute

Received 13-09-2024
Revised 14-09-2024
Accepted 24-10-2024
Published 26-10-2024

Abstract:

The increasing integration of digital technologies in maritime operations has significantly enhanced efficiency in cargo tracking, port management, and communication systems. However, this digital transformation also introduces substantial cybersecurity risks, particularly in developing regions like Tanzania, where technological infrastructure and specialized skills may lag behind global standards. This study evaluates the cybersecurity readiness of three key Tanzanian maritime organizations Tanzania Ports Authority (TPA), Tanzania Shipping Agency Corporation (TASAC), and SINOTASHIP using the Cybersecurity Capability Maturity Model (C2M2). Through a detailed assessment across ten C2M2 domains, the study identifies existing strengths and critical gaps in areas such as risk management, asset management, and incident response. The findings reveal that while basic cybersecurity practices exist, they are largely reactive, with most domains scoring between Level 1 (Initial) and Level 3 (Defined). This lack of advanced, proactive measures poses significant risks to Tanzania's maritime infrastructure, particularly given the strategic role of ports like Dar es Salaam in regional trade. The study highlights the need for tailored improvements, including enhanced asset management, continuous workforce training, and real-time monitoring systems, to bridge the gap between global standards and local practices. By implementing these measures, Tanzanian maritime operations can strengthen their resilience against cyber threats, ensuring secure and efficient port operations in an increasingly interconnected world.

Keywords: Cybersecurity, Maritime Operations, Risk Management, Cyber Resilience

1. Introduction:

The maritime industry has experienced a profound transformation with the rise of digital technologies, improving efficiency in operations, cargo tracking, and communication. However, this digital revolution also comes with its own set of vulnerabilities. As global maritime systems become increasingly dependent on interconnected digital platforms, they also become prime targets for cyber threats. In Tanzania, the ports of Dar es Salaam serve as critical gateways for East African trade, the reliance on digital infrastructure without comprehensive cybersecurity measures may poses significant risks. A report by the International Maritime Organization (IMO) highlights the global rise in cyberattacks on maritime operations, warning that these threats can disrupt supply chains, compromise sensitive data, and lead to substantial financial losses (IMO, 2020).

While global best practices such as those recommended by the IMO’s Resolution MSC.428(98) provide essential guidance for integrating cybersecurity into maritime safety management systems, the local adaptation of these practices in Tanzania presents unique challenges. Studies show that Tanzania, like many developing nations, faces limitations in technological infrastructure and a shortage of specialized cybersecurity professionals (Mwangoka & Mtenzi, 2019). This gap between global standards and local capabilities leaves Tanzanian maritime operations vulnerable to a growing array of cyber risks, including ransomware attacks, malware, and phishing schemes, which have already caused significant disruptions in more advanced maritime sectors (Jones & Tam, 2019).

To bridge this gap, this study applies the Cybersecurity Capability Maturity Model (C2M2) to evaluate the current state of cybersecurity in Tanzanian maritime operations. The C2M2 framework has been successfully used in various industries to assess cybersecurity maturity across multiple domains, such as risk management and incident response (DOE, 2014). By applying C2M2 to Tanzanian ports and maritime organizations, this study aims to uncover specific areas where global best practices can be tailored to local realities, offering a roadmap to improve cybersecurity resilience in the maritime sector.

2. Literature Review:

2.2 The Rising Importance of Cybersecurity in Maritime Operations:

The integration of advanced technologies such as automation, the Internet of Things (IoT), and artificial intelligence (AI) has undeniably revolutionized the maritime industry, leading to increased operational efficiency, enhanced cargo tracking, and streamlined port management. However, these same technologies have also expanded the sector’s vulnerability to cyber threats. With vessels, ports, and logistics systems becoming increasingly interconnected, the maritime industry's attack surface has significantly grown, exposing it to a variety of cyber risks, including ransomware, malware, and phishing attacks (BIMCO, 2021). Recent high-profile cyber incidents, such as the ransomware attack on A.P. Moller-Maersk, which led to operational disruptions and financial losses estimated at $300 million, underscore the severity of these risks (Kaspersky, 2018).

As maritime systems are further integrated into global supply chains, the need for robust cybersecurity frameworks has become more urgent. A report by Allianz (2020) noted a sharp rise in the number of cyber incidents targeting the shipping industry, with threats evolving in complexity and scale. The International Maritime Organization (IMO) has also emphasized the importance of addressing cyber risks through its Resolution MSC.428(98), which mandates that cybersecurity be incorporated into maritime safety management systems by 2021 (IMO, 2017). However, studies suggest that many maritime organizations, particularly in developing regions, are still lagging in cybersecurity preparedness, highlighting the urgent need for comprehensive and tailored cyber risk management strategies (Chalya & Mkoma, 2020).

2.3 Nature of Cyber Threats in the Maritime Sector:

The maritime sector is increasingly vulnerable to a broad spectrum of cyber threats, including ransomware, malware infections, phishing schemes, and unauthorized access to critical control systems. These threats can severely disrupt port operations and vessel navigation, leading to significant financial and operational setbacks. For instance, the NotPetya malware attack in 2017, which affected Maersk, caused massive operational disruptions across its global network, ultimately costing the company up to $300 million in recovery efforts (Maersk, 2018). Similarly, a study by Allianz (2020) highlighted the rising sophistication of cyber-attacks in the maritime industry, noting that many port authorities and shipping companies are increasingly becoming targets due to inadequate cybersecurity measures.

In addition to financial repercussions, cyber threats can also compromise safety in maritime operations. For instance, unauthorized access to navigation systems can lead to vessel misdirection, creating both safety hazards and potential environmental damage, especially in congested or sensitive waters (BIMCO, 2021). Moreover, phishing attacks targeting maritime staff can exploit human vulnerabilities, often leading to the theft of sensitive information or the introduction of malicious software into critical systems. A report by BIMCO noted that over 40% of shipping companies had been victims of cyber-attacks, with the majority of incidents going unreported due to concerns over reputational damage (BIMCO et al., 2018). This underscores the urgent need for the maritime industry to enhance its cybersecurity frameworks and build resilience against such threats.

2.4 Global Best Practices in Maritime Cybersecurity:

Global organizations have recognized the growing cyber threats facing the maritime industry and have developed comprehensive frameworks to address these risks. The International Maritime Organization (IMO) has been at the forefront of these efforts, with its Resolution MSC.428(98) mandating that shipping companies incorporate cyber risk management into their safety management systems by 2021 (IMO, 2017). This resolution urges maritime operators to adopt proactive strategies that identify, mitigate, and manage cyber risks across all levels of operations. The IMO's approach underscores the importance of embedding cybersecurity within the broader framework of maritime safety, acknowledging that cyber incidents can have consequences as severe as traditional safety breaches. Additionally, the Network and Information Systems (NIS) Directive from the European Union serves as a critical regulatory framework aimed at enhancing cybersecurity resilience across essential sectors, including maritime transport (European Commission, 2016).

In addition to regulatory frameworks, industry organizations such as BIMCO have developed practical guidelines to assist shipowners and operators in managing cyber risks. BIMCO's "Guidelines on Cyber Security Onboard Ships" (2018) provide a roadmap for implementing cybersecurity measures tailored to the maritime context, covering everything from identifying vulnerabilities to establishing incident response plans (BIMCO et al., 2018). These guidelines highlight the necessity for a risk-based approach, encouraging organizations to assess their unique vulnerabilities and implement controls based on the likelihood and impact of potential threats. Countries like Singapore have taken these recommendations further by launching initiatives like the Maritime Cybersecurity Programme, which fosters collaboration between the public and private sectors to bolster cyber resilience in maritime infrastructures (MPA, 2019). These global best practices provide invaluable insights that can be adapted to different national contexts, including Tanzania, to mitigate evolving cyber threats in maritime operations.

2.5 Challenges and Adaptation in Tanzania:

Despite the availability of global cybersecurity frameworks, Tanzanian maritime operations face significant challenges in adopting and implementing these standards. One of the primary issues is the country's insufficient technological infrastructure, which hinders the effective deployment of advanced cybersecurity measures. Many maritime organizations still rely on outdated systems, making them vulnerable to a wide range of cyber threats (Chalya & Mkoma, 2020). The maritime sector in Tanzania struggles with a shortage of skilled cybersecurity professionals. This shortage limits the ability of ports and shipping companies to manage and respond to cyber threats effectively. Research shows that many Tanzanian maritime organizations lack formal cybersecurity policies, leaving them exposed to risks that could disrupt critical trade operations (Mwangoka & Mtenzi, 2019). These challenges are further compounded by the lack of sector-specific regulations that address the unique cybersecurity needs of maritime operations.

To tackle these challenges, this study employs the Cybersecurity Capability Maturity Model (C2M2) to evaluate the maturity of cybersecurity practices within Tanzanian maritime organizations. The C2M2 framework assesses cybersecurity capabilities across various domains, such as risk management, asset management, and incident response (DOE, 2014). By leveraging C2M2, this study offers a structured approach to identifying gaps in cybersecurity maturity and provides a roadmap for capability development. The framework not only helps in benchmarking current practices against global standards but also tailors' solutions to fit the local Tanzanian context, addressing the unique constraints of the maritime sector. Through this detailed evaluation, the study aims to enhance the resilience of Tanzanian maritime operations against evolving cyber threats.

3. Methodology:

The methodology for this study revolves entirely around the use of the Cybersecurity Capability Maturity Model (C2M2) to assess the cybersecurity capabilities of Tanzanian maritime organizations. C2M2 provides a structured, domain-based evaluation to measure cybersecurity maturity and identify areas for improvement. The methodology involves four key phases: preparation, assessment using the C2M2 domains, scoring based on the model's maturity levels, and the development of a roadmap for capability improvement.

3.1 Overview of the Cybersecurity Capability Maturity Model (C2M2):

The (C2M2) is a robust framework developed to evaluate and enhance the cybersecurity practices of organizations. Originally created by the U.S. Department of Energy in collaboration with industry stakeholders, the model was designed to improve the cybersecurity posture of critical infrastructure sectors such as energy, but it has since been adapted for use across various industries, including maritime operations (DOE, 2014). The C2M2 framework consists of 10 domains that assess key areas such as risk management, asset management, threat and vulnerability management, and incident response. Each domain is evaluated on a maturity scale from Level 1 (Initial), where cybersecurity practices are minimal or non-existent, to Level 5 (Optimized), where cybersecurity is fully integrated into the organization's operations with continuous improvement processes in place. The model provides organizations with a structured approach to identifying gaps in their cybersecurity defences, managing risks, and developing targeted strategies for improvement, making it a valuable tool in today’s digital landscape

Table 1. C2M2 Domains and Definitions

Domain	Description
Risk Management	Identifying, assessing, and managing cybersecurity risks across the organization.
Asset Management	Managing IT and OT assets to ensure they are protected from cyber risks.
Cybersecurity Architecture	Ensuring the organization’s systems and networks are secure by design and continually improved.
Workforce Management	Developing and maintaining cybersecurity skills and awareness within the organization.
Cybersecurity Program Management	Managing the overall cybersecurity program, ensuring continuous alignment with strategic objectives.
Threat and Vulnerability Management	Proactively identifying and mitigating cybersecurity threats and vulnerabilities.
Situational Awareness	Continuously monitoring and understanding the cybersecurity posture of IT/OT environments.
Event and Incident Response	Ensuring timely and effective response to cybersecurity incidents, minimizing damage and ensuring recovery.
Dependency Management	Managing cybersecurity risks associated with external parties, including third-party vendors.
Information Sharing and Communications	Sharing and communicating relevant cybersecurity information both internally and with external stakeholders.

3.2 Implementation of C2M2 in Tanzanian Maritime Operations

The C2M2 model is applied directly to Tanzanian maritime organizations to evaluate their cybersecurity maturity. The model does not rely on external data collection but rather assesses internal cybersecurity practices across the 10 domains. The following steps were taken:

C2M2 Domain Assessment: Each organization's internal cybersecurity processes were reviewed and categorized according to the C2M2 domains. For each domain, the organization's existing cybersecurity capabilities were mapped against the model's requirements for maturity at levels 1 through 5.

Scoring and Maturity Levels: Each domain is scored based on its current cybersecurity maturity level using the C2M2 scoring system, which is organized into five levels:

Level 1: Initial – Basic or no formal cybersecurity practices.

Level 2: Managed – Some cybersecurity measures in place, generally reactive.

Level 3: Defined – Formal cybersecurity policies and procedures implemented consistently.

Level 4: Quantitatively Managed – Performance metrics are used to measure and manage cybersecurity efforts.

Level 5: Optimized – Cybersecurity practices are fully integrated into the organization's operations and continuously improved.

3.3 Domain Scoring and Maturity Results

Each of the 10 domains was assessed and assigned a maturity level based on the current state of cybersecurity in Tanzanian maritime operations. The results are shown below:

Table 2. C2M2 Domain Maturity Scores for Tanzanian Maritime Operations

Domain	Current Maturity Level	Description of Current State
Risk Management	2 (Managed)	Basic risk management practices are in place but are mostly reactive.
Asset Management	1 (Initial)	No formal processes to track or protect critical assets, significant room for improvement.
Cybersecurity Architecture	2 (Managed)	Basic security measures are implemented, but architecture lacks formal planning and design.
Workforce Management	1 (Initial)	Very limited cybersecurity training or awareness among staff, resulting in vulnerability to human error.
Cybersecurity Program Management	2 (Managed)	Cybersecurity program exists but is not integrated into overall strategic objectives.
Threat and Vulnerability Management	2 (Managed)	Some processes for threat identification, but these are often outdated or not comprehensive.
Situational Awareness	1 (Initial)	Little to no real-time monitoring of cybersecurity posture, leading to delayed responses to incidents.
Event and Incident Response	3 (Defined)	Formal incident response plans are in place, but coordination between teams is inconsistent.
Dependency Management	2 (Managed)	Some third-party risks are recognized, but formal processes for managing vendor cybersecurity risks are lacking.
Information Sharing	1 (Initial)	Very limited sharing of cybersecurity information internally or with external stakeholders.

3.4 Development of a Roadmap for Capability Improvement

Based on the C2M2 domain assessments, a roadmap was developed for improving cybersecurity capabilities in Tanzanian maritime operations. The roadmap focuses on achieving higher maturity levels across all 10 domains, with specific actions tailored to each organization's current status.

Table 3. Roadmap for Enhancing Cybersecurity Maturity in Tanzanian Maritime Operations

Domain	**Current Maturity Level**	**Target Maturity Level**	**Actions to Achieve Target Level**
Risk Management	2 (Managed)	4 (Quantitatively Managed)	Develop formal risk management strategies, use performance metrics to evaluate and improve risk responses.
Asset Management	1 (Initial)	3 (Defined)	Implement asset tracking systems, classify assets, and introduce protection protocols for critical infrastructure.
Cybersecurity Architecture	2 (Managed)	4 (Quantitatively Managed)	Design a comprehensive cybersecurity architecture that aligns with industry standards.
Workforce Management	1 (Initial)	3 (Defined)	Introduce formal cybersecurity training programs across all levels of the organization.
Cybersecurity Program Management	2 (Managed)	4 (Quantitatively Managed)	Align the cybersecurity program with organizational strategy and continuously measure progress.
Threat and Vulnerability Management	2 (Managed)	4 (Quantitatively Managed)	Establish real-time threat intelligence and vulnerability assessment systems.
Situational Awareness	1 (Initial)	3 (Defined)	Introduce continuous monitoring systems for detecting anomalies in IT and OT environments.
Event and Incident Response	3 (Defined)	4 (Quantitatively Managed)	Improve incident coordination and integrate real-time analysis tools for faster response.
Dependency Management	2 (Managed)	3 (Defined)	Establish formal procedures to manage cybersecurity risks from third-party vendors and partners.
Information Sharing	1 (Initial)	3 (Defined)	Set up internal cybersecurity information-sharing mechanisms and encourage collaboration with external stakeholders.

4. Results and Findings:

This section presents the findings from the application of the Cybersecurity Capability Maturity Model (C2M2) to assess the cybersecurity maturity of three key Tanzanian maritime organizations: the Tanzania Ports Authority (TPA), Tanzania Shipping Agency Corporation (TASAC), and The Tanzanian Joint Shipping Company (SINOTASHIP). The evaluation was conducted across the 10 C2M2 domains, and the results highlight the current cybersecurity capabilities, maturity levels, and areas requiring improvement.

The overall cybersecurity maturity across the three organizations was found to range between Level 1 (Initial) and Level 3 (Defined), indicating that while basic cybersecurity measures are in place, there is a substantial need for improvement across all domains. The following table provides a summary of the maturity levels across the C2M2 domains for each organization:

Table 4. C2M2 Domain Maturity Scores for Tanzanian Maritime Organizations

Domain	TPA Maturity Level	TASAC Maturity Level	SINOTASHIP Maturity Level
Risk Management	2 (Managed)	1 (Initial)	2 (Managed)
Asset Management	1 (Initial)	1 (Initial)	2 (Managed)
Cybersecurity Architecture	2 (Managed)	1 (Initial)	2 (Managed)
Workforce Management	1 (Initial)	1 (Initial)	1 (Initial)
Cybersecurity Program Management	2 (Managed)	1 (Initial)	2 (Managed)
Threat and Vulnerability Management	2 (Managed)	1 (Initial)	2 (Managed)
Situational Awareness	1 (Initial)	1 (Initial)	1 (Initial)
Event and Incident Response	3 (Defined)	2 (Managed)	2 (Managed)
Dependency Management	2 (Managed)	1 (Initial)	2 (Managed)
Information Sharing	1 (Initial)	1 (Initial)	1 (Initial)

5. Discussion:

The study employed the Cybersecurity Capability Maturity Model (C2M2) to evaluate the cybersecurity maturity of three key Tanzanian maritime organizations: the Tanzania Ports Authority (TPA), the Tanzania Shipping Agency Corporation (TASAC), and SINOTASHIP. By focusing on ten specific C2M2 domains, the study provided a detailed assessment of each organization's current cybersecurity practices. These domains cover critical areas such as risk management, asset management, incident response, and workforce training. This approach allowed for a nuanced analysis of how each organization manages cybersecurity threats and their preparedness for potential incidents. The assessment helped to identify both strengths and areas that require improvement, providing a clear picture of the existing cybersecurity landscape in these vital maritime entities.

The findings indicate that the overall cybersecurity maturity in these organizations ranges from basic to moderate levels. Most of the domains scored between Level 1 (Initial) and Level 3 (Defined), revealing that while some foundational cybersecurity practices are in place, they tend to be reactive rather than proactive. For instance, TPA and SINOTASHIP demonstrated slightly more advanced capabilities, particularly in areas like risk management, compared to TASAC, which lagged in several domains. However, all three organizations showed significant gaps in areas such as asset management, workforce training, and real-time monitoring. This indicates a need for targeted enhancements to their cybersecurity frameworks to move from basic, ad-hoc practices towards more structured and proactive strategies that align with global standards. Addressing these gaps will be crucial for bolstering their resilience against evolving cyber threats.

5.1 Overview of Maturity Levels:

The overall maturity levels reveal significant limitations in the cybersecurity frameworks of the evaluated organizations, underscoring a predominant reliance on reactive measures rather than proactive and strategic defences. Despite the existence of some foundational cybersecurity practices, they lack the comprehensive, forward-looking strategies needed to build a resilient and robust cyber defence infrastructure. This deficiency leaves the organizations vulnerable to increasingly sophisticated cyber threats. A closer comparison among the organizations TPA, SINOTASHIP, and TASAC highlights notable disparities in cybersecurity maturity, even within the same sector, which raises concerns about consistency in managing cybersecurity risks across Tanzanian maritime operations.

TPA and SINOTASHIP demonstrated relatively better capabilities, managing to reach a Level 2 (Managed) status in critical domains such as Risk Management and Cybersecurity Architecture. This level suggests that while these organizations have some structured processes for managing risks and securing their digital infrastructure, their approach remains largely reactive and lacks the depth of continuous improvement. Conversely, TASAC lags significantly behind, with most of its cybersecurity practices still at Level 1 (Initial). This means that TASAC's cybersecurity measures are minimal, often ad hoc, and lack formal processes and policies, rendering it particularly vulnerable to cyber incidents. The contrast between the managed status of TPA and SINOTASHIP and the initial stage of TASAC underscores a pressing need for sector-wide initiatives aimed at elevating cybersecurity standards uniformly across all organizations.

5.2 Key Strengths:

Event and Incident Response: Among the three organizations, the Event and Incident Response domain received relatively higher scores, with TPA achieving Level 3 (Defined). This indicates that formal incident response plans are in place, providing a structured approach to managing cybersecurity incidents. Such preparedness is essential for minimizing disruption during cyber events.

Risk Management Practices: Although generally at Level 2 (Managed), the risk management practices in TPA and SINOTASHIP show an awareness of the need to address cybersecurity risks. This suggests that these organizations have started to identify and manage risks, even if the processes are not yet fully integrated or proactive.

5.3 Major Gaps Identified:

Asset Management: All three organizations were found lacking in this domain, with scores at Level 1 (Initial) or Level 2 (Managed). This reflects an absence of formal processes to track and protect critical IT and operational technology (OT) assets. Without effective asset management, organizations are vulnerable to undetected cyber threats targeting unmonitored systems.

Workforce Management: A significant gap in workforce management was evident, with each organization scoring Level 1 (Initial). This highlights a limited focus on cybersecurity training and awareness programs for staff, increasing susceptibility to threats like phishing and social engineering.

Situational Awareness: The study found that situational awareness is minimal, with all three organizations at Level 1 (Initial). This lack of real-time monitoring means that potential cyber threats may not be detected early, delaying responses and increasing the potential damage from incidents.

5.4 Disparities Between Global Standards and Local Practices:

The study underscores a significant gap between global cybersecurity standards and the adaptation of these practices within Tanzanian maritime organizations. International frameworks, such as the International Maritime Organization's (IMO) Resolution MSC.428(98), stress the critical need to integrate cybersecurity measures into broader safety management systems. These standards emphasize a holistic, proactive approach to cybersecurity, aiming to embed robust risk management practices across all levels of maritime operations. However, translating these global standards into the Tanzanian context has proven challenging. The reality on the ground reveals a disconnect between the aspirations of these frameworks and the existing capabilities within local organizations. This gap creates vulnerabilities, as many Tanzanian maritime entities struggle to meet the rigorous requirements set out by international bodies. The inability to seamlessly adopt these standards not only puts Tanzanian ports at risk but also poses broader implications for the security and efficiency of regional trade routes reliant on these critical infrastructures.

The challenges Tanzanian maritime organizations face are multifaceted, rooted primarily in outdated technological infrastructure and a significant shortage of skilled cybersecurity professionals. Many of these organizations still rely on legacy systems that lack the resilience needed to counter modern cyber threats, making them particularly vulnerable to attacks. The scarcity of specialized cybersecurity expertise further compounds this issue, as it limits the capacity of these organizations to develop and maintain effective cyber defence strategies. Instead of adopting a forward-looking, anticipatory approach to cyber risk management, Tanzanian maritime operations often resort to reactive measures that address incidents after they occur. This reactive stance is a direct consequence of the constrained resources and expertise, which prevents the full realization of globally recommended cybersecurity practices. The study highlights the urgency of addressing these challenges to close the gap between international standards and local implementation, thereby enhancing the resilience of Tanzanian maritime operations against an evolving landscape of cyber threats.

5.5 Implications for Maritime Operations in Tanzania:

The findings of this study highlight significant implications for the security and stability of maritime operations in Tanzania. With cybersecurity maturity levels ranging from low to moderate across key organizations, the sector remains exposed to a rising tide of sophisticated cyber threats. This vulnerability is particularly concerning given the strategic role of Tanzanian ports, such as Dar es Salaam, which serve as crucial gateways for East African trade. A successful cyberattack on these ports could lead to severe disruptions in maritime logistics, delaying shipments and potentially causing bottlenecks in regional supply chains. Such disruptions would not only impact local businesses but could ripple across neighbouring countries that rely on these ports for the import and export of goods, resulting in substantial economic losses and diminished trade efficiency across the region.

The study's identification of critical gaps, particularly in areas like asset management and situational awareness, further emphasizes the urgency of addressing these vulnerabilities. Effective asset management is essential for protecting critical infrastructure, yet the current lack of formal systems means that many IT and operational technology assets remain inadequately monitored and secured. Similarly, the limited situational awareness prevents maritime organizations from detecting and responding swiftly to cyber threats, increasing the likelihood of prolonged and costly incidents. Without targeted investments to strengthen these areas, Tanzanian maritime operations risk falling behind in their ability to withstand the complex cyber challenges of the modern digital age. Addressing these gaps is not only crucial for safeguarding the integrity of Tanzania's maritime infrastructure but is also essential for maintaining the region's role as a reliable hub in global trade networks.

6. Recommendations Based on Findings:

Develop Comprehensive Asset Management Systems: All organizations must prioritize the establishment of formal asset management systems to monitor and secure critical IT and OT assets. This should include regular audits and the implementation of tools for real-time asset tracking and protection.

Implement Continuous Workforce Training Programs: A critical component of enhancing cybersecurity maturity is to educate and train employees at all levels. Organizations should develop cybersecurity awareness programs and ensure that employees understand common threats such as phishing and ransomware.

Enhance Incident Response Plans: Incident response plans should be updated and regularly tested across all organizations to ensure that employees are familiar with their roles during a cybersecurity event. Organizations should also invest in real-time incident detection tools to reduce the time it takes to respond to breaches.

Deploy Real-Time Monitoring Systems: Organizations need to implement real-time monitoring tools to improve situational awareness. These tools will provide greater visibility into the cybersecurity posture and enable proactive threat mitigation.

Establish Formal Information Sharing Protocols: Internal communication channels for sharing cybersecurity information should be strengthened, and external collaboration with industry peers and government agencies should be encouraged to stay informed about new threats and best practices.

Conclusion:

In navigating the digital tides that now shape the world's oceans, the Tanzanian maritime sector stands at a crossroads, where the promise of interconnected efficiency meets the peril of evolving cyber threats. This study has shed light on the intricate balance between adopting global cybersecurity best practices and adapting them to local realities. While the journey towards robust cybersecurity resilience may be filled with challenges outdated systems, limited expertise, and the pressure of global expectations there lies a unique opportunity for transformation. By embracing targeted improvements, Tanzanian maritime organizations can evolve from a reactive stance to a proactive force, safeguarding not only their digital waters but also the economic lifelines that flow through their ports. As the anchors of East African trade, these organizations have the potential to set a course toward a more secure and prosperous future, where digital threats are met with agility and resilience, ensuring that Tanzania's maritime gateways remain open, safe, and thriving amidst the waves of change.

References:

1. Allianz Global Corporate & Specialty (AGCS). (2020). *Rising Sophistication of Cyber Attacks in Maritime Industry*. Retrieved from https://www.agcs.allianz.com/news-and-insights/reports/shipping-review.html
2. Allianz Global Corporate & Specialty (AGCS). (2020). *Safety and Shipping Review 2020: Cyber Risks in Maritime Operations*. Retrieved from https://www.agcs.allianz.com
3. BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO. (2018). *Guidelines on Cyber Security Onboard Ships (Version 3)*. Retrieved from https://www.bimco.org
4. BIMCO, et al. (2018). *Guidelines on Cyber Security Onboard Ships*. Retrieved from https://www.bimco.org
5. BIMCO. (2018). *Over 40% of Shipping Companies Affected by Cyber-Attacks*. Retrieved from https://www.bimco.org
6. Chalya, S., & Mkoma, H. (2020). *Cybersecurity Preparedness in the Maritime Sector: A Case of Tanzania*.
7. European Commission. (2016). *The Network and Information Systems (NIS) Directive*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/nis-directive
8. International Maritime Organization (IMO). (2017). *Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems*. Retrieved from https://www.imo.org/en/MediaCentre/HotTopics/Pages/Guidelines-on-Maritime-Cyber-Risk-Management.aspx
9. International Maritime Organization (IMO). (2020). *Global Rise in Cyberattacks on Maritime Operations*. Retrieved from https://www.imo.org
10. Jones, P., & Tam, Y. (2019). *Impact of Cyber Threats on Global Maritime Trade*.
11. Kaspersky. (2018). *Ransomware Attack on A.P. Moller-Maersk: Case Study*. Retrieved from https://www.kaspersky.com
12. Maersk. (2018). *NotPetya Cyber Attack: Financial and Operational Impacts*. Retrieved from https://www.maersk.com
13. Maritime and Port Authority of Singapore (MPA). (2019). *Maritime Cybersecurity Programme: A Collaborative Initiative*. Retrieved from https://www.mpa.gov.sg
14. Mwangoka, J., & Mtenzi, F. (2019). *Cybersecurity Challenges in Developing Nations: A Tanzanian Perspective*.
15. U.S. Department of Energy (DOE). (2014). *Cybersecurity Capability Maturity Model (C2M2) Version 1.1*. Retrieved from https://www.energy.gov/c2m2