ALAM JOURNAL OF MARITIME STUDIES

ISSN: 2590-4345 e ISSN: 2976-3843 Volume 5 Issue 1 Year 2024

The Impact of Cybersecurity on the Maritime Industry and its Solutions

Mohammad Monir Hossain
Centre for Professional Studies, Akademi Laut Malaysia

Abstract - The maritime industry, a critical component of global trade and commerce, has become increasingly dependent on digital technologies for operations, navigation, and communication. This growing reliance has exposed the industry to a range of sophisticated cyber threats, from ransomware attacks to GPS spoofing, phishing, and data breaches. These threats have the potential to disrupt operations, compromise safety, and lead to significant financial losses. This review article explores the impact of cybersecurity on the maritime industry and examines various solutions to mitigate these risks. The discussion covers the evolving nature of cyber threats, the implications for maritime operations, and the strategic measures implemented to enhance cybersecurity. Through a comprehensive analysis of existing literature, this article aims to provide insights into the current state of maritime cybersecurity and propose future directions for research and practice. This review highlights the necessity for robust cybersecurity frameworks to ensure the safety and efficiency of maritime operations.

Keywords: Cybersecurity, Cyber Threats, Cyber Risk, Digital Technologies Mitigation, Maritime Industry

Email address: Mohammad.Monir@alam.edu.my

1.0 INTRODUCTION

The maritime industry, integral to global trade and commerce, is increasingly dependent on digital technologies. This reliance, while enhancing operational efficiency, also introduces significant cybersecurity vulnerabilities (Mednikarov et al., 2020, Akpan et al., 2022). Maritime cybersecurity encompasses the protection of shipborne systems, shore-based operations, and communication networks against cyber threats (Melnyk et al., 2023). These threats can disrupt operations, endanger lives, and cause substantial financial losses (Caprolu et al., 2020).

Cyber threats in the maritime sector have evolved, with attackers employing sophisticated methods to exploit vulnerabilities. Incidents such as the 2017 NotPetya attack, which severely impacted Maersk's operations across multiple ports and resulted in financial losses estimated at $300 million, highlight the maritime sector's vulnerability to cyber threats (Meyer-Larsen & Müller, 2018). The increasing integration of Internet of Things (IoT) devices further exacerbates these vulnerabilities (Ashraf et al., 2023). As maritime operations become more digitized, the potential for cyber-attacks grows, necessitating robust cybersecurity measures (Caprolu et al., 2020). Table 1 which is adapted from Akpan et al. (2022) presents examples of recent cyber incidents in the maritime transport sector.

Table 1. Examples of recent cyber incidents

Year	Incident	Consequences
2016	GPS jamming attack in South Korea	280 vessels were affected
2017	Cyberattack against the navigation system	Hijack of the vessel for 10 h
2017	Cyberattack against the navigation system	U.S. Navy ship collided with a boat
2017	NotPetya malware attack	Affected shipping infrastructures

2018	GPS spoofing attack against ships in the Black Sea	Deviation of 20 ships to an airport
2018	Remotely compromising onboard computers	Stealing sensitive data
2018	GPS spoofing attack	Manipulation of the ship position
2018	ECDIS was infected by a virus	Delay in the ship sailing
2019	Malware attack targeted a U.S. vessel	Critical credential mining
2020	Ransomware Hermes 2.1. attack on 2 ships	Infection of the whole network
2020	Ransomware attack “Mespinoza/Pysa”	Maritime infrastructures infected
2021	Ransomware attack on shipping companies	All their files were encrypted
2022	Installation of malicious code	Gain access to the port network

Table 1. Examples of recent cyber incidents in the maritime transport sector (Adapted from Akpan et al., 2022)

Effective cybersecurity in the maritime industry involves a multi-faceted approach, including technological, organizational, and regulatory strategies (Farah et al., 2023). Technological measures such as encryption, intrusion detection systems, and secure communication protocols are essential for enhancing cybersecurity in maritime systems (Walid et al., 2017). Organizational strategies include training personnel in cybersecurity best practices and developing incident response plans (Chowdhury et al., 2022).Regulatory frameworks at national and international levels play a crucial role in standardizing and enforcing cybersecurity practices (Faria, 2020).

This article aims to provide a comprehensive review of the impact of cybersecurity on the maritime industry and the solutions implemented to address these challenges. By analyzing current literature, this review will identify key trends, highlight effective practices, and propose future research directions.

2.0 CYBERSECURITY THREATS IN THE MARITIME INDUSTRY

Cyber threats in the maritime industry can take various forms, including malware, phishing, ransomware attacks, Denial-of-Service (DoS) attacks, GPS spoofing, and data breaches (Ashraf et al., 2023; Caprolu et al., 2020; Androjna et al., 2020). These threats can disrupt navigation systems, compromise cargo security, and lead to financial losses.

Malware and phishing attacks are common in the maritime industry. These attacks often target email systems and can lead to unauthorized access to sensitive data. Notably, the NotPetya attack in 2017, which affected Maersk's operations, highlighted the devastating impact of cyber-attacks on maritime logistics, causing an estimated financial loss of $200–300 million (Meyer-Larsen & Müller, 2018).

Ransomware attacks involve encrypting a company's data and demanding payment for its release. In the maritime sector, such attacks can halt operations, delay shipments, and result in significant financial losses (Pawelski, 2023). The impact is amplified by the interconnected nature of global supply chains.

GPS spoofing involves sending false signals to a vessel's navigation system, causing it to deviate from its intended course. This can lead to collisions, groundings, and other maritime accidents (Androjna & Perkovič, 2021; Wang et al., 2022). The vulnerability of navigation systems to spoofing attacks underscores the need for robust cybersecurity measures. Denial-of-service attacks, on the other hand, overwhelm systems with traffic, causing disruptions (Akpan et al., 2022). These attacks can delay shipments and increase operational costs.

Data breaches in the maritime industry can expose sensitive information, including cargo manifests, crew details, and financial transactions (Mednikarov et al., 2020; Akpan et al., 2022). Such breaches not only pose security risks but also damage the reputation of maritime companies.

Human error and insider threats are significant concerns in maritime cybersecurity. Unintentional mistakes or malicious actions by employees can lead to security breaches. Training and awareness programs are essential to mitigate these risks (Amoresano & Yankson, 2023). Table 2 which is adapted from Ukwandu et al. (2022) presents the distribution types of Cyber Attacks.

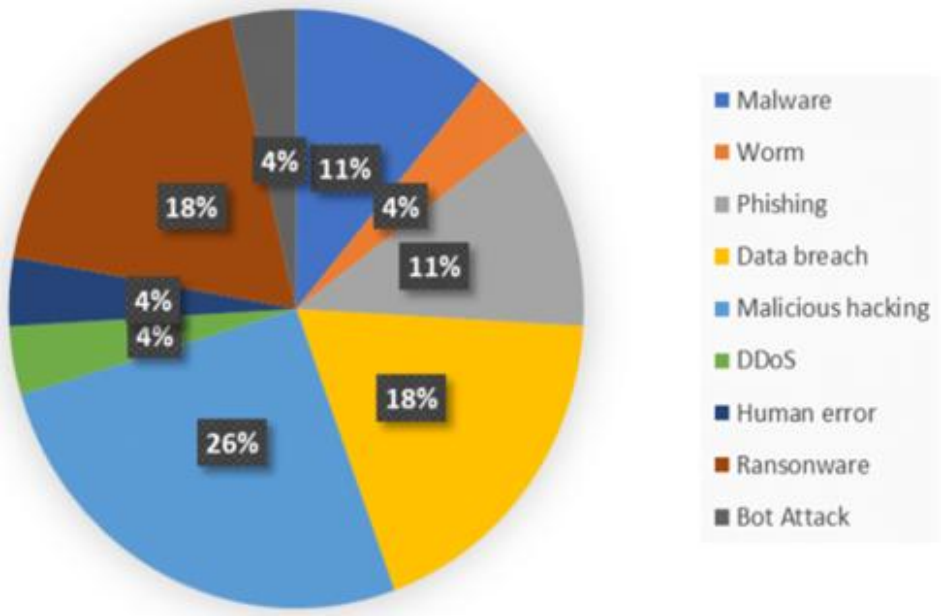

Figure 1: Distribution of Cyber Attacks by Type (Adapted from Ukwandu et al., 2022)

3.0 VULNERABILITIES IN MARITIME INFRASTRUCTURE

The maritime industry's growing reliance on digital systems for managing operations, navigation, and communications has led to significant vulnerabilities that are increasingly being exploited by cyber attackers. This dependence on digital technologies is compounded by the widespread use of legacy systems, a lack of standardization, and inadequate cybersecurity policies, all of which contribute to the sector's susceptibility to cyber threats. The maritime industry is highly interconnected, and any breach in a single system can have widespread implications across the global supply chain. This makes it essential to address the underlying issues that expose the industry to cyber risks (Mednikarov et al., 2020).

One of the primary challenges faced by maritime companies is the continued use of outdated software and hardware systems. Many maritime organizations operate with legacy systems that were not designed to withstand modern cyber threats. These systems are often more prone to attacks due to inherent security weaknesses, including vulnerabilities that are no longer supported by software updates or patches (Ashraf et al., 2023). Updating these systems is a complex and costly process, requiring significant investment in both technology and personnel. However, failing to update these systems leaves critical maritime infrastructure vulnerable to cyberattacks that could disrupt operations, cause financial losses, and even compromise the safety of vessels and ports.

The lack of standardization across the maritime industry further exacerbates these vulnerabilities. This absence of standardized cybersecurity measures creates inconsistencies in how companies approach cybersecurity, with some organizations implementing more rigorous protections than others. As a result,

gaps in security across the industry make it easier for cybercriminals to exploit weaknesses in the global maritime infrastructure (Finley & Harkiolakis, 2018). Establishing international cybersecurity standards is crucial for mitigating these risks.

Another critical vulnerability is the absence of comprehensive cybersecurity policies across many maritime companies. Without robust policies that outline clear cybersecurity protocols, response plans, and mitigation strategies, these organizations remain highly vulnerable to attacks (Akpan et al., 2022). It is essential that maritime companies not only develop but also rigorously implement detailed cybersecurity policies tailored to their specific operational needs.

4.0 SOLUTIONS TO ENHANCE MARITIME CYBERSECURITY

Addressing cybersecurity within the maritime industry is a complex challenge that requires a comprehensive and multifaceted approach. The maritime sector is highly interconnected and relies on a combination of digital technologies for operations, communications, and navigation. As such, a broad set of strategies must be implemented to adequately defend against the increasing sophistication and frequency of cyber threats. Key components of this approach include the integration of advanced technological solutions, the development of strong regulatory frameworks, and fostering collaboration between industry stakeholders (Hopcraft & Martin, 2018).

One of the most critical aspects of improving cybersecurity in the maritime sector is the implementation of advanced technological solutions. Technologies such as intrusion detection systems (IDS), encryption, and blockchain have become essential tools in protecting maritime assets from cyberattacks. Intrusion detection systems help monitor and identify suspicious activities within networks, enabling rapid response to potential breaches. Encryption technologies ensure that data transmitted between systems, whether onshore or at sea, is protected from unauthorized access, thus preserving data integrity. Blockchain technology adds an additional layer of security by enabling secure, tamper-proof transactions and communications (Caprolu et al., 2020; Sanober et al., 2022; Meng et al., 2018). These technologies are vital in safeguarding sensitive information, maintaining operational continuity, and reducing the risk of cyberattacks that could disrupt maritime operations. By employing these advanced cybersecurity technologies, maritime organizations can better protect critical systems from being compromised.

In addition to technological solutions, the establishment of robust regulatory frameworks is paramount for ensuring cybersecurity across the maritime sector. These frameworks provide a structured and enforceable approach to mitigating cyber risks by setting minimum standards for cybersecurity practices. For example, international regulatory bodies such as the International Maritime Organization (IMO) have developed guidelines on maritime cyber risk management, which provide a foundational set of standards that shipping companies, ports, and other maritime stakeholders can follow to enhance their cybersecurity measures. These guidelines address areas such as network security, data protection, and incident response, ensuring that cybersecurity is embedded within the broader safety management system of maritime organizations (Hopcraft & Martin, 2018; Faria, 2020).

Another critical element in addressing cybersecurity in the maritime industry is collaboration between different stakeholders, including maritime companies, cybersecurity firms, and governmental agencies. Cybersecurity is a collective responsibility, and no single entity can effectively mitigate cyber risks on its own. By fostering cooperation and collaboration across sectors, maritime organizations can share valuable information on threats, vulnerabilities, and best practices, helping to create a unified and coordinated defense against cyber threats. Collaborative efforts can take many forms, from joint cybersecurity exercises and incident response drills to sharing intelligence on emerging cyber threats and attack methodologies. (Caprolu et al., 2020). This collaborative approach not only strengthens the industry's overall cybersecurity posture but also helps in developing more resilient systems that are better equipped to withstand and respond to cyber incidents.

5.0 FUTURE DIRECTIONS AND RESEARCH

Future research in maritime cybersecurity should prioritize the development of more sophisticated and targeted technologies and strategies that address the specific needs and vulnerabilities of the maritime industry. The unique operational challenges of the maritime sector, including the integration of complex shipborne and shore-based systems, require tailored cybersecurity solutions that can mitigate risks and ensure the smooth functioning of global maritime operations. Advancements in cybersecurity technologies should not only focus on protecting these systems but also anticipate potential future threats, making proactive security a cornerstone of maritime operations (Farah et al., 2023).

In addition to technological advancements, continuous training and education for maritime professionals are critical for maintaining a high level of cybersecurity awareness. The rapidly evolving nature of cyber threats means that personnel must be regularly updated on the latest risks and best practices. Training programs must go beyond basic cybersecurity protocols to include in-depth education on the specific challenges faced by the maritime industry, ensuring that employees can respond effectively to cyber incidents and reduce the risk of human error, a common factor in security breaches (Kayisoglu et al., 2023; Canepa et al., 2021; Pyykkö et al., 2020).

Emerging technologies such as artificial intelligence (AI) and machine learning (ML) are poised to play a crucial role in enhancing cybersecurity within the maritime industry. These technologies offer promising solutions for the detection and mitigation of cyber threats by improving the capacity for real-time monitoring, threat detection, and rapid response. AI and ML technologies can analyze vast amounts of data to identify anomalies that may indicate potential threats, thus providing early warning systems that can help prevent cyberattacks before they occur (Kumar et al., 2023). These technologies can also be leveraged to automate certain aspects of cybersecurity, reducing the burden on human operators and allowing for more efficient responses to emerging threats.

Finally, the continuous development and refinement of cybersecurity policies are essential to keeping pace with the rapidly evolving cyber threat landscape. Cybersecurity policies should be regularly reviewed and updated to address new vulnerabilities and emerging threats. This process should include a comprehensive assessment of existing cybersecurity measures and the integration of new technologies and strategies that can enhance overall system security. Furthermore, cybersecurity policies must be aligned with international standards and best practices to ensure a coordinated and unified response to threats across the maritime sector (Finley & Harkiolakis, 2018). By maintaining robust and adaptive cybersecurity policies, the maritime industry can better protect its critical infrastructure from cyberattacks, ensuring the safety and efficiency of global maritime operations.

6.0 CONCLUSION

Cybersecurity is a crucial issue for the maritime industry, impacting every aspect of operations and safety. As digital technologies become more embedded in maritime infrastructure, the industry faces heightened risks from cyber threats. To effectively protect against these risks, it is vital to understand the nature of the threats, identify vulnerabilities, and implement robust security measures. This requires a multifaceted approach, including the adoption of advanced cybersecurity technologies, adherence to regulatory standards, and the development of comprehensive cybersecurity policies. Collaboration between industry stakeholders, cybersecurity experts, and governmental agencies is essential for building a unified defense, while ongoing research and innovation are critical for staying ahead of evolving cyber threats. Through collaboration, regulation, and continuous improvement, the maritime industry can enhance its cybersecurity posture and safeguard against future cyber-attacks.

REFERENCES

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. Network. Retrieved from https://www.semanticscholar.org/paper/Cybersecurity-Challenges-in-the-Maritime-Sector-

Akpan-Bendiab/f2345a08c082d163c2df2d227352ae7f2dbbf5e6

Amoresano, K., & Yankson, B. (2023). Human error - A critical contributing factor to the rise in data breaches: A case study of higher education. HOLISTICA – Journal of Business and Public Administration,14, 110-132. Retrieved from https://www.researchgate.net/publication/371849122_Human_Error_-_A_Critical_Contributing_Factor_to_the_Rise_in_Data_Breaches_A_Case_Study_of_Higher_Education

Androjna, A., Brcko, T., Pavić, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*. Retrieved from https://www.semanticscholar.org/paper/Assessing-Cyber-Challenges-of-Maritime-Navigation-Androjna-Brcko/ade029abe15ebcccb9c7619a461d69f9176cf740

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2023). A survey on cyber security threats in IoT-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems*, 24, 2677-2690. Retrieved from https://www.semanticscholar.org/paper/A-Survey-on-Cyber-Security-Threats-in-IoT-Enabled-Ashraf-Park/e9cb0dacf58f48a8498c33cf62a69912ef4bd89e

Canepa, M., Ballini, F., Dalaklis, D., & Vakili, S. (2021). Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. INTED2021 Proceedings. Retrieved from https://www.semanticscholar.org/paper/ASSESSING-THE-EFFECTIVENESS-OF-CYBERSECURITY-AND-Canepa-Ballini/c6ac0146a4b0d800e6fc2fa823eae5fb8419768f

Caprolu, M., Pietro, R. D., Raponi, S., Sciancalepore, S., & Tedeschi, P. (2020). Vessels cybersecurity: Issues, challenges, and the road ahead. *IEEE Communications Magazine*, 58, 90-96. Retrieved from https://arxiv.org/pdf/2003.01991

Chowdhury, N., Nystad, E., Reegård, K., & Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. *International Journal of Safety and Security Engineering*. Retrieved from https://ntnuopen.ntnu.no/ntnuxmlui/bitstream/handle/11250/3043529/12.03_04.pdf?sequence=1

Farah, M. B., Al-Kadri, M., Ahmed, Y., Abouzariba, R., Benfarah, M., Alkadri, O., Ahmed, Y., & Bellekens, X. (2023). Cyber incident scenarios in the maritime industry: Risk assessment and mitigation strategies. *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, 194-199. Retrieved from https://www.semanticscholar.org/paper/Cyber-Incident-Scenarios-in-the-Maritime-Industry%3A-Farah-Al-Kadri/ff7acd30a847a3cd3e71660da955d90e07571e79

Faria, D. L. (2020). The impact of cybersecurity on the regulatory legal framework for maritime security. Janus.net. Retrieved from https://www.researchgate.net/publication/347113237_The_impact_of_cybersecurity_on_the_regulatory_legal_framework_for_maritime_security

Finley, I., & Harkiolakis, N. (2018). Cybersecurity policies and supporting regulations for maritime transportation system in the USA. International Journal of Teaching and Case Studies, 9, 89. Retrieved from https://www.researchgate.net/publication/323979089_Cybersecurity_policies_and_supporting_regulations_for_maritime_transportation_system_in_the_USA

Kayisoglu, G., Bolat, P., & Duzenli, E. (2023). Modelling of maritime cyber security education and training. Pedagogika-Pedagogy. Retrieved from https://azbuki.bg/wp-content/uploads/2023/08/pedagogy_6s_23_gizem-kaysoglu.pdf

Kumar, P., Gupta, G. P., Tripathi, R., Garg, S., & Hassan, M. (2023). DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework in IoT-Enabled Maritime Transportation Systems. IEEE Transactions on Intelligent Transportation Systems, 24, 2472-2481. Retrieved from https://www.semanticscholar.org/paper/DLTIF%3A-Deep-Learning-Driven-Cyber-Threat-Modeling-Kumar-Gupta/fc8c89506a4782170037a112d2abfe7d482589c3

Hopcraft, R., & Martin, K. (2018). Effective maritime cybersecurity regulation – the case for a cyber code. Journal of the Indian Ocean Region, 14(3), 354-366. Retrieved from https://www.researchgate.net/publication/327588589_Effective_maritime_cybersecurity_regulation_-_the_case_for_a_cyber_code

Meyer-Larsen, N., & Müller, R. (2018). Enhancing the cybersecurity of port community systems. In Cybersecurity and Cyberforensics Conference. Retrieved from https://link.springer.com/content/pdf/10.1007/978-3-319-74225-0_43.pdf

Mednikarov, B., Tsonev, Y., & Lazarov, A. D. (2020). Analysis of cybersecurity issues in the maritime industry. Information & Security: An International Journal, 47, 27-43. Retrieved from https://www.semanticscholar.org/paper/Analysis-of-Cybersecurity-Issues-in-the-Maritime-Mednikarov-Tsonev/0ff150e96dc44aa7ce71b7083a8f5aa7814c3434

Melnyk, O., Onyshchenko, S., Onishchenko, O.A., Lohinov, O.V., & Ocheretna, V. (2023). Integral approach to vulnerability assessment of ship's critical equipment and systems. *Transactions on Maritime Science*. Retrieved from https://www.researchgate.net/publication/371220089_Integral_Approach_to_Vulnerability_Assessment_of_Ship%27s_Critical_Equipment_and_Systems

Pawelski, J. (2023). Cyber threats for present and future commercial shipping. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation. Retrieved from https://www.researchgate.net/publication/372003612_Cyber_Threats_for_Present_and_Future_Commercial_Shipping

Pyykkö, H., Kuusijärvi, J., Noponen, S., Toivonen, S., & Hinkka, V. (2020). Building a Virtual Maritime Logistics Cybersecurity Training Platform. Cybersecurity and Logistics, 223-246. Retrieved from https://www.semanticscholar.org/paper/Building-a-Virtual-Maritime-Logistics-Cybersecurity-Pyykk%C3%B6-Kuusij%C3%A4rvi/46129d80d50976048391dc5ba741e336ed8526ab

Sanober, S., Aldawsari, M., Karimovna, A. D., & Ofori, I. (2022). Blockchain integrated with principal component analysis: A solution to smart security against cyber-attacks. Security and Communication Networks. Retrieved from https://www.researchgate.net/publication/362627655_Blockchain_Integrated_with_Principal_Component_Analysis_A_Solution_to_Smart_Security_against_Cyber-Attacks

Walid, E., Newe, T., Ó. Eoin, & Gerard, D. (2017). Trust security mechanism for maritime wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 29. Retrieved from https://www.researchgate.net/publication/308274768_Trust_security_mechanism_for_maritime_wireless_sensor_networks