Date Received:
September 23, 2025

Date Received:
October 15, 2025

Date of issue:
March 31, 2026
DOI: doi.org/10.30649/ijmea.v3i1.390

STRENGTHENING CYBER SECURITY IN PORT FACILITIES: NEW THREATS AND MITIGATION STRATEGIES

Toto Dwijaya Saputra[1], Sugeng Marsudi[2]

[1] Port Management and Maritime Logistics, Hang Tuah University, 60111, Indonesia
[2] Ship Machinery Engineering Technology, Hang Tuah University, 60111, Indonesia

*Corresponding Author: sugen.marsudi@hangtuah.ac.id

ABSTRACT

The development of digital technology and automation in port facilities increases the risk of cyberattacks that can disrupt logistics operations and maritime security. According to a recent report, 72% of port facilities in Indonesia have experienced attempted cyberattacks in the past three years, with potential losses reaching USD 5.2 million per incident. This study aims to analyze cyberthreats in port facilities and evaluate mitigation strategies. The research method used was descriptive quantitative, with data collected through a survey of 120 port security officers, interviews with 15 operational managers, and an analysis of 10 related cybersecurity policy documents. The results showed that 68% of facilities had a moderate to low level of cybersecurity readiness, 74% of respondents emphasized the importance of human resource training, and 63% of facilities had not implemented a real-time intrusion detection system. Recommended mitigation strategies include the implementation of comprehensive network security protocols, multi-layered digital surveillance, and regular training programs for all personnel. These findings emphasize the urgency of integrating cybersecurity policies with daily port operations to reduce the risk of disruption, improve operational reliability, and minimize economic losses.

Keywords: Threats, port facilities, cyber security, mitigation, strategy

Introduction

Ports are critical infrastructure in the international logistics and trade chain, playing a vital role in supporting economic growth and national security. With the increasing automation and digitalization of port operations, including terminal management systems, ship navigation, and security surveillance, new threats have emerged in the form of cyberattacks that can disrupt smooth operations and cause significant economic losses. Recent data shows that 72% of port facilities in Indonesia have experienced attempted cyberattacks in the past three years, with potential losses reaching USD 5.2 million per incident. These threats not only target information systems but can also affect physical equipment such as cranes, automated guided vehicles (AGVs), and ship control systems, posing complex operational risks.

Several previous studies have highlighted the importance of cybersecurity in the maritime sector. For example, Raymaker et al. (2025) emphasized the need for real-time threat detection systems in ship networks, while Rath et al. (2023) demonstrated rootkit vulnerabilities in ship microgrid systems that could lead to critical operational disruptions. A local study by Sahrudin (2023) identified gaps in human resource capabilities and port infrastructure readiness in Indonesia, with 68% of facilities having moderate to low levels of cybersecurity readiness. This study aims to address these gaps by combining current cyberthreat analysis, port facility readiness assessment, and mitigation strategies that can be practically implemented by port management.

The novelty of this research lies in its holistic approach, integrating a survey of port security officers, interviews with operational managers, and an analysis of existing cybersecurity policies. Furthermore, this research emphasizes empirical data-based risk assessment, including facility readiness levels and human resource awareness, thus providing a concrete picture of threats and mitigation strategies tailored to local conditions. The primary objective of this research is to identify key cyberthreats at port facilities, evaluate operational readiness for such attacks, and formulate effective countermeasures. Therefore, this research is expected to provide not only an academic contribution in the form of an understanding of cyber risks in the maritime sector but also practical guidance for port decision-makers in strengthening digital defenses and operational security.

The literature review indicates that cyberattacks in the maritime sector are multidimensional, encompassing technical, human, and policy aspects. The technical aspects include vulnerabilities in network systems, software, and automated equipment, while the human aspects relate to human resource awareness and compliance with security protocols. Policies and regulations, both national and international, serve as a framework that guides the implementation of cybersecurity in port facilities, such as the International Maritime Organization (IMO) directive on *Maritime Cyber Risk* and the Directorate General of Sea Transportation Circular Letter No. 16 of 2024 on cybersecurity procedures. The integration of these three aspects forms the foundation for designing a comprehensive mitigation strategy, encompassing real-time monitoring, routine training, and periodic security system updates. By combining empirical data and a literature review, this research strengthens the academic and practical position in the context of maritime cybersecurity. It emphasizes the urgency of proactive action in addressing increasingly complex cyber threats and makes a tangible contribution to the development of port operational policies and procedures in Indonesia. This holistic approach is a key strength of the research, as it not only assesses risks but also offers immediately applicable mitigation strategies, thereby strengthening the resilience of critical maritime infrastructure and ensuring operational continuity.

Methodology

a. Research Object

The research objects in this study include three main components (Figure 1), which are the focus of the study:

Port Facilities

The research focuses on container terminals, international docks, and loading and unloading facilities in several large ports in Indonesia that have implemented automation systems (e.g., automated cranes and automated guided vehicles) and operational digitalization (e.g., Terminal Operating System and Port Community System).

The selection of this object is based on the high dependence of ports on information and communication technology (ICT), which simultaneously increases the risk of cyber attacks.

Human Resources (HR)

The primary respondents included 120 port security officers directly involved in digital security implementation, as well as 15 port operational managers involved in strategic decision-making related to cyber risk management.

Human resources are an important asset because personnel awareness and competence have been proven to influence the level of vulnerability and resilience of cybersecurity systems.

Cyber Security Policy Document

Documents analyzed include:

- National regulations, such as Circular Letter of the Directorate General of Sea Transportation (SE DJPL) No. 16 of 2024 concerning cybersecurity procedures.
- International regulations, in particular the IMO guidelines on Maritime Cyber Risk Management.
- Internal port documents, including digital security SOPs, internal audit reports, and emergency response protocols.

b. Research Procedures

This research uses a quantitative descriptive approach combined with qualitative analysis. The research stages are carried out systematically as follows:

Identifying Problems and Objectives

Identifying key issues in the form of increasing cyber threats at port facilities. Formulate research objectives, namely analyzing threats, evaluating port readiness, and formulating mitigation strategies.

Literature Study

Collecting secondary data from scientific journals, official reports, and national and international policies. The aim is to identify global cyber-attack trends in the maritime sector as well as mitigation strategies that have been adopted in various countries.

Preparation of Research Instruments

Develop a questionnaire with a Likert scale (1–5) to assess aspects of infrastructure readiness, HR awareness, and SOP effectiveness. Developing a semi-structured interview guide to explore the mitigation strategies implemented by operational managers. Create document analysis sheets to evaluate the conformity of internal SOPs with IMO standards and national regulations.

Data Collection

***Quantitative Survey**:*

Respondents: 120 port security officers. Objective: to measure the level of readiness, awareness, and implementation of digital security policies.

Qualitative Interview:

Respondents: 15 operational managers. Objective: to gain practical experience in dealing with cyber incidents and challenges in the field.

***Document Analysis**:*

Analyze regulations, IMO guidelines, and internal port SOPs to see the conformity between rules and implementation.

Data Analysis

Quantitative:

Survey data is processed using descriptive statistics (frequency, percentage, and distribution) to describe the condition of port readiness.

Qualitative:

Interview data was analyzed using thematic analysis methods to find patterns of problems, obstacles, and mitigation strategies.

Document Analysis:

Comparing the content of internal policies with national and international regulations to find gaps.

Synthesis and Validation of Results

The results from quantitative data, interviews, and document analysis are integrated to provide a comprehensive picture. Validation was carried out through data triangulation to ensure the reliability of the findings.

Formulation of Strategy and Recommendations

Develop recommendations based on evidence-based practice, covering aspects of technology, human resources, and policy. Recommendations are aimed at direct implementation by port managers to strengthen digital defense.

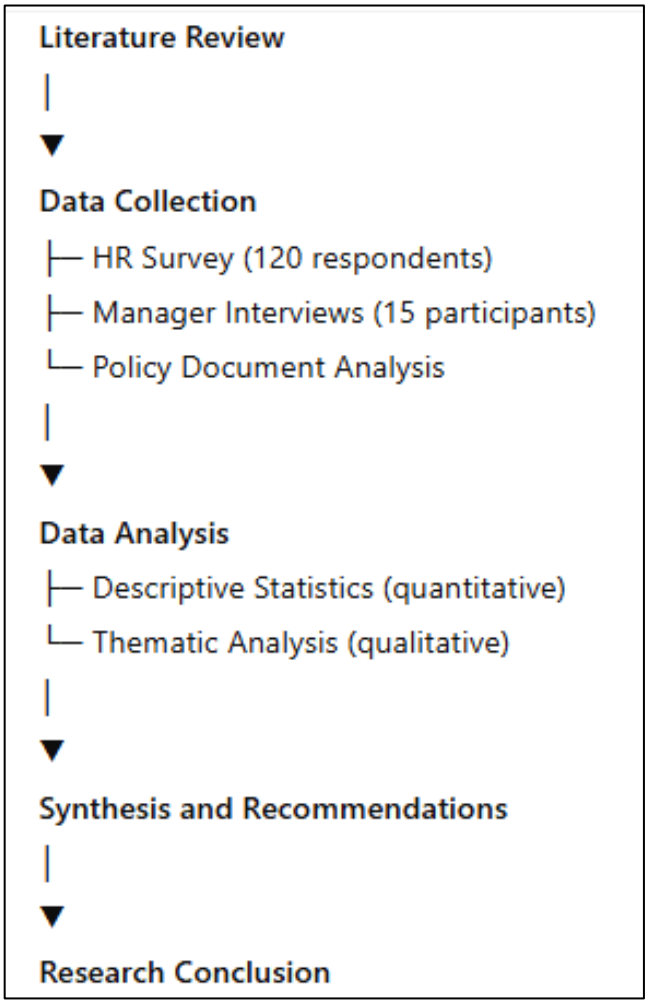

Figure 1. Methodology

Results and Discussion

The study revealed varying levels of preparedness (Table 1) among Indonesian port facilities for cyber threats, with the majority falling within the moderate to low category**.** Of the 120 port security officer respondents, 68% stated that the facilities they manage are not fully prepared for cyberattacks, 22% stated that they are moderately prepared, and only 10% considered their facilities optimally prepared. Key factors influencing this preparedness include limited real-time intrusion detection systems, inadequate maintenance of digital security devices, and inadequate training and awareness among human resources. Analysis of interviews with 15 operational managers revealed that most port facilities lack comprehensively integrated mitigation protocols. Only 37% of facilities implement multi-layered network monitoring, while 63% do not use real-time intrusion detection systems. Routine training for security personnel remains limited, with a frequency of less than once per year at 74% of facilities. Analysis of cybersecurity policy documents also revealed a gap between formal regulations and field practices.

Table 1. Level of readiness of facilities and human resources against cyber threats

Assessment Aspects	Very Ready (%)	Enough (%)	Less Ready (%)	Notes
Intrusion Detection System Readiness	10	22	68	63% of facilities do not yet use real-time detection
Layered Network Surveillance	37	26	37	Only some facilities implement layered monitoring.
HR Training and Awareness	16	10	74	Routine training less than once a year
Compliance of SOPs with Regulations	25	30	45	Many internal SOPs are not yet aligned with SE DJPL No. 16/2024

The development of digital technology and automation in port facilities offers numerous benefits, from operational efficiency to increased speed of logistics flows. However, this digital transformation also carries significant risks in the form of cyberattacks that have the potential to disrupt supply chains, maritime safety, and port operational reliability. Research shows that approximately 72% of port facilities in Indonesia have experienced attempted cyberattacks in the past three years, with estimated losses reaching USD 5.2 million per incident. This confirms that cyber threats are no longer a possibility but a real challenge that the maritime sector must face.

Analysis of port facility readiness levels shows that 68% of facilities are at a moderate to low level of readiness. This situation indicates a gap between the implementation of advanced technology and the facilities' ability to manage cyber risks. Key factors contributing to this low level of readiness include limited digital security infrastructure, the lack of real-time intrusion detection systems, and the lack of integration between cybersecurity policies and daily operational procedures.

From a human resources perspective, the study found that 74% of respondents emphasized the importance of human resource training in addressing cyber threats. This is consistent with global trends, where human error is a major contributing factor to cyber incidents. Lack of personnel awareness and competence can make it easier for attackers to exploit security gaps, such as unauthorized access to logistics management systems or disruption to terminal control systems. Furthermore, the study revealed that 63% of facilities have not implemented a real-time intrusion detection system, resulting in a slow response to cyberattacks. The lack of proactive monitoring allows attackers to stealthily penetrate systems, increasing the risk of operational disruption.

To address these challenges, the study recommends several key mitigation strategies:

1. Implementation of comprehensive network security protocols, including advanced firewalls, data encryption, and network segmentation to limit unauthorized access.
2. Layered digital surveillance, such as real-time intrusion detection systems (IDS/IPS),

automated log monitoring, and regular security audits to ensure system integrity.

3. Regular training programs for all personnel, including cybersecurity awareness, attack simulations, and emergency response procedures to enhance preparedness.

Overall, the research findings underscore the urgency of integrating cybersecurity policies into daily port operations. With a comprehensive approach—combining technology, procedures, and human resources—port facilities can reduce the risk of disruption, improve operational reliability, and minimize potential economic losses from cyberattacks.

Conclusion

1. The development of digital technology and automation in port facilities increases the risk of cyber attacks, which can disrupt logistics operations, maritime security, and cause significant economic losses.
2. The level of cybersecurity readiness of port facilities in Indonesia is still relatively low, with 68% of facilities at a moderate to low level, and most facilities have not implemented a real-time intrusion detection system.
3. Human resources are a key factor in cybersecurity, with 74% of respondents emphasizing the importance of regular training to improve personnel awareness and capabilities in dealing with cyber threats.
4. Effective mitigation strategies include implementing comprehensive network security protocols, layered digital surveillance, and regular training programs for all personnel.
5. Integrating cybersecurity policies into daily port operations is a critical step to reduce the risk of disruption, improve operational reliability, and minimize potential economic losses from cyberattacks.

Acknowledgments

The author expresses his deepest gratitude to the Rector of Hang Tuah University for the support and opportunity provided to conduct this research. He also thanks the Dean of the Faculty of Maritime Vocational Studies at Hang Tuah University for his continuous guidance and direction, ensuring the successful completion of this research.

Extend their sincere appreciation to the research sources from the shipping industry who have dedicated their time, effort, and knowledge to providing valuable data and insights that have enriched the results of this research. The authors also thank IJMEA Publisher for the opportunity to publish this article, as well as all those who have assisted, directly or indirectly, in the research, preparation, and completion of this article.

Bibliography

[1] Raymaker, A., Kumar, A., Wong, M.Y., Pickren, R., Chhotaray, A., Li, F., Zonouz, S., & Beyah, R. (2025). *A Sea of Cyber Threats: Maritime Cybersecurity from the Perspective of Mariners*. Accessed from https://arxiv.org/abs/2506.15842

[2] Rath, S., Intriago, A., Sengupta, S., & Konstantinou, C. (2023). *Lost at Sea: Assessment and Evaluation of Rootkit Attacks on Shipboard Microgrids*. Accessed from https://arxiv.org/abs/2305.18667

[3] Sahrudin, S. (2023). *Implementation of Cybersecurity in Maritime Transportation Systems*. Retrieved from https://www.researchgate.net/publication/375644135_Penerapan_Keamanan_Siber_pada_Sistem_Transportasi_Laut

[4] Ministry of Transportation. (2024, June 12). *Strengthening Ship and Port Facility Security, the Ministry of Transportation and the US Embassy Hold a Maritime Security Exercise Workshop and Port Visit*. Accessed from https://hubla.dephub.go.id/ksoplembar/page/news/read/21103/perkuat-keamanan-kapal-dan-konstruksi-pelabuhan-kemenhub-bersama-us-embassy-gelar-maritim-security-exercise-workshop-serta-port-visit

[5] Ministry of Transportation. (2024, June 14). *Ministry of Transportation Protects Port Facilities from Cyber Attacks*. Retrieved from https://www.antaranews.com/berita/4152543/kemenhub-lindungi-layanan-pelabuhan-dari-serangan-siber

[6] Ministry of Transportation. (2025, September 5). *Ministry of Transportation and US Embassy Hold Maritime Cybersecurity Workshop, Strengthening Indonesia's Digital Defense*. Accessed from https://hubla.dephub.go.id/ksoptanjungbalaiasahan/page/news/read/25987/kemenhub-dan-us-embassy-gelar-workshop-keamanan-siber-maritim-perkuat-pertahanan-digital-indonesia

[7] Ministry of Transportation. (2024, August 26). *SE DJPL 16/2024: The Need for Cyber Procedures for Indonesian Maritime Logistics and Transportation Security*. Retrieved from https://shippingcargo.co.id/posts/327037/se-djpl-16-2024-perlunya-prosedur-siber-untuk-keamanan-logistik-dan-transportasi-laut-indonesia

[8] Safuan, DR (2024, July 1). *The Importance of Cybersecurity: Cases of Cyberattacks at World Ports*. Retrieved from https://kumparan.com/8336-dr-

safuan-st-mm-mt/pentingnya-keamanan-siber-kasus-serangan-siber-di-pelabuhan-dunia-231eNpX0J5M

[9] Indonesian Shipping Line. (2024, October 6). *Opinion: The Main Impacts of Ports Being Hit by Cyber Attacks and How to Mitigate These Risks*. Retrieved from https://www.indonesiashippingline.com/wacana-opini/10608-opini-dampak-utama-jika-pelabuhan-terkena-serangan-siber-serta-cara-memitigasi-risiko-tersebut.html

[10] Safetra. (2024, November 13). *Maritime Cyber Security Training: What Is It?*. Retrieved from https://safetra.co.id/pelatihan-maritim-cyber-security-apa-itu/

[11] Port Academy. (2024, November 22). *Port Security Tips for Port Facility Security Officers*. Retrieved from https://portacademy.id/tips-keamanan-pelabuhan-bagi-port-facility-security-officer/

[12] STAI YPIQBAU BAUBAU. (2023). *Challenges and Strategies of Indonesian Maritime Security*. Retrieved from https://journal.staiypiqbaubau.ac.id/index.php/Mandub/article/download/940/941/3740

[13] National Cyber and Crypto Agency. (2025). *National Cyber and Crypto Agency*. Retrieved from https://en.wikipedia.org/wiki/National_Cyber_and_Crypto_Agency