Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849 e-ISSN: 2548-1398
Vol. 10, No. 3, Maret 2025

ANALYSIS OF THE INFLUENCE OF FACTORS ON MARITIME CYBER RESILIENCE ON BOARD WITH INTERVENING MARITIME CYBER SECURITY AWARENESS

Arizal Hendriawan[1], Idris Gautama[2], Denny Siahaan[3], Kurniawan[4]
Institut Transportasi Dan Logistik Trisakti, Indonesia[1,2,3,4]
Email: arizal1975@gmail.com[1], igautama@binus.ac.id[2], ladensi@yahoo.com[3], kurniawan@nusaputra.ac.id[4]

Abstract

Indonesia plays a crucial role in sustaining the global maritime industry, with its growing potential to supply a skilled workforce through improved maritime education and international certifications. However, cybersecurity has become a critical challenge, with rising cyberattacks causing financial losses, operational disruptions, and diminished trust among stakeholders. Limited digital literacy, outdated technology, and inadequate cyber threat training exacerbate vulnerabilities, threatening maritime operations, national security, and economic stability. This study evaluates maritime cybersecurity management systems and assesses the readiness of Indonesian seafarers in addressing cyber threats. A quantitative approach is employed, using questionnaires distributed to officer-level seafarers holding Certificates of Endorsement (COE). A sample of 396 respondents, determined through the Slovin formula and purposive sampling, was analyzed using Structural Equation Modeling (SEM) with Partial Least Squares (PLS). The results show that Digital Literacy significantly enhances Maritime Cybersecurity Awareness but does not directly impact Cybersecurity Resilience. In contrast, System & Technology Availability has a direct and significant influence on Resilience, particularly through enhanced infrastructure and security measures. Maritime Cybersecurity Awareness also mediates the relationship between Digital Literacy and Resilience, emphasizing its critical role in improving preparedness.The study recommends enhancing digital literacy through targeted training, upgrading technological infrastructure, conducting specialized cybersecurity programs, and enforcing stricter regulatory policies. These steps are crucial to strengthening maritime cybersecurity resilience and fostering a secure, adaptive maritime ecosystem in Indonesia.

Keyowords: Digital Literacy, System & Technology Availability, Cyber Security Awareness, Cyber-Security Resilience

Introduction

Indonesia plays a crucial role in maintaining the sustainability and efficiency of the global maritime industry. According to a reference from (BIMCO, 2021) Indonesia has the potential to increase the number of officers working on international vessels, as the quality of maritime education and international certification improves.

	All Seafarers	Officers	Ratings
1	Philippines	Philippines	Philippines
2	Russian Federation	Russian Federation	Russian Federation
3	Indonesia	China	Indonesia
4	China	India	China
5	India	Indonesia	India

Source: Country Questionnaire, 2021

Figure 1. World's Largest Seafarer Officer Suppliers

Cybersecurity in the maritime sector has become a critical issue at both the national and international levels (Afenyo & Caesar, 2023). This is due to several cyberattacks that have resulted in financial losses, the loss of important assets, and trust issues between clients and service providers in affected organizations. According to the World Economic Forum (2020), cyberattacks have caused significant financial losses, particularly in the technology sector. Furthermore, the global ransomware attack in 2017 also caused substantial financial losses (Alotaibi, 2022).

For example, the 2017 cyberattack on Maersk led to losses of approximately USD 300 million (Karas, 2023). Although the recent blockage of the Suez Canal was not related to a cyberattack, the resulting cost amounted to 12% of global trade0020 suggesting that cyberattacks on ships in the Suez Canal could cause similar losses. In 2017, major ports around the world experienced about 12 attacks per day. Additionally, the average ship owner paid approximately USD 3.1 million in ransom due to maritime cyberattacks (Editorial Team, 2022).

The limited knowledge possessed by individuals regarding the impacts of these activities represents a potential cyber threat. This is reflected in previous research, which indicates that knowledge has an influence on cyber threat awareness (Zwilling et al., 2022). The lack of digital literacy makes it difficult for individuals to distinguish between valid information and hoaxes, which can be exploited by cybercriminals to launch attacks.

The limited technological infrastructure in the maritime sector, such as outdated navigation and communication systems, makes it vulnerable to cyberattacks. The insufficient implementation of security technologies aboard ships is a major challenge in maintaining maritime cybersecurity resilience (Putri & Burhanuddin, 2024). Seafarers often do not receive adequate training on cyber threats, resulting in low awareness of cyberattack risks. This can lead to a lack of vigilance and improper responses when facing cyber threats.(Agbo-ola, 2022).

The lack of attention to cybersecurity in the maritime sector increases vulnerability to cyberattacks. This can have significant implications for national security, the economy, and the operational safety of ships (Putri & Burhanuddin, 2024) .Cyberattacks targeting maritime infrastructure, including navigation systems, communication, and ship control, are on the rise. This indicates that the maritime sector has become an attractive target for cybercriminals. This study aims to evaluate and analyze the current maritime cybersecurity management systems in place, as well as assess the readiness and competence of Indonesian seafarers in facing maritime cyberattacks. The findings of this study will be used to provide recommendations on necessary regulations, proposed course designs for maritime cyber training, and the development of an effective maritime cybersecurity management system model.

Digital Literacy

Digital literacy (also known as cyber literacy) refers to a set of specific skills that help us navigate the digital space, understand the implications of our actions, and protect ourselves from cyber threats. Digital literacy is a broad term for the ability to effectively use computers and digital technologies

In the paper "The Role of Digital Literacy in Raising Cybersecurity Awareness" by Sholikhah (2022), it is stated that, in order to understand and protect personal data, society must evolve to adapt to the digital culture. Digital literacy is the ability to use digital technology safely and appropriately to access, manage, understand, integrate, communicate, evaluate, and create the information needed for work, employability, and entrepreneurship. It includes skills commonly referred to as computer literacy, information technology literacy, media literacy, and information literacy (Nancy Law et al., 2018). One of the issues is that internet users are not interested in developing their own digital skills, leading to problems such as data misuse, data breaches, or related cybercrimes. People recognize the importance of protecting physical assets and property, but they have not fully realized the risks associated with digital assets and the need for protective actions (Moallem, 2019).

System & Technology Availability

According to O'Brien (2003), a system is a collection of components that interact and work together to achieve a common goal. This system receives input and produces output through a structured transformation process. Meanwhile, Turban (2003) defines information as a collection of facts (data) organized in such a way that it becomes meaningful to the recipient. This information is designed to be easily understood by the intended audience.

Thompson and Cat-Baril (2003) explain that an information system is an integrated information technology-based system, designed to support operations, management, and decision-making within an organization. Information systems include an organized and integrated combination of people, hardware, software, communication networks, and data resources to fulfill these functions.

System redundancy refers to the ability of a ship's IT system to function optimally even if part of the system fails (Mersinas & Chana, 2022). This includes backup arrangements that are ready for use in emergency situations, such as during a cyberattack or technical failure. System redundancy is a key component in enhancing cybersecurity resilience, as it allows the ship's operations to continue even in the event of an attack or issue with the digital infrastructure. In this context, system redundancy encompasses supporting hardware and software, as well as the presence of automated protocols that ensure that if one part of the system fails, another can immediately take over its functions without causing significant downtime. The Contingency Planning Theory (Galbraith, 1973) explains that redundancy is crucial in ensuring operational continuity, especially under unexpected conditions (Catarina, 2020).

Cyber Security Awareness

Cybersecurity is a global, multidimensional, and interdisciplinary phenomenon(de Bruijn & Janssen, 2017). Cybersecurity breaches can vary from low-impact or limited damage to data theft and manipulation, or even the hijacking of systems that can cause physical damage (de Bruijn & Janssen, 2017). Whitman and Mattford (2019, p. 689) in the study by Agbo-ola (2022) define cybersecurity as "the protection of computerized

information, processing systems, and the data contained and processed within them." This definition is similar to the one provided by the UK National Cyber Security Centre (2021, para. 16), which states that cybersecurity is "the protection against theft or damage to devices, services, and networks, including the information contained within them.".

Cybersecurity involves both people and systems, where the concept of cybersecurity encompasses the knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values held by individuals regarding cybersecurity and how these are reflected in their behavior towards information technology (Georgiadou et al., 2022). Although almost everyone has heard of cybersecurity, the urgency level and public behavior do not yet reflect a high level of awareness(Agbo-ola, 2022). The need for effective cybersecurity awareness has become increasingly important with the introduction of the Internet of Things (IoT), which is becoming more integrated into daily life, and our ongoing dependence on information and communication technology.

Cyber-Security Resilience

Cybersecurity resilience is a concept that has evolved alongside the increasing complexity of threats in the digital world. According to Caralli et al. (2021), it is defined as the ability of an organization to maintain its operational functions effectively before, during, and after a cyberattack, while continuously adapting to evolving threats. This definition highlights the importance of operational continuity in the face of cyber disruptions. In research by Anderson et al. (2023), cybersecurity resilience is described as a holistic approach that integrates technology, processes, and human resources to create a robust security ecosystem. This approach focuses not only on preventing attacks but also on the ability to maintain critical services during periods of disruption. In research conducted by Anderson et al. (2023) on cyber security resilience, it is described as a holistic approach that integrates technology, processes, and human resources to create a resilient security ecosystem. This approach focuses not only on attack prevention, but also on the ability to maintain critical services during periods of disruption. Mitchell and Thompson (2022) provide a more technical perspective, defining cybersecurity resilience as the system's capacity to maintain an acceptable level of service when facing various disruptions, from cyberattacks to system failures. They stress the importance of designing systems with resilience in mind from the outset.

Research Method

This study is a quantitative research using a survey method through questionnaire distribution. The research respondents are seafarers holding officer-level positions on ships who possess a Certificate of Endorsement (COE). The COE holders are selected as the population because they represent the active sailing seafarers. The COE is only issued for officers working on ships and must be renewed every five years (PM 70, 2013; PM 26, 2022). The population in this study is estimated to be 34,348 Indonesian seafarers with a COE. The sample size for the study is determined using the Structural Equation Modeling (SEM) method based on components or Partial Least Squares (PLS). According to Ghozali (2015), the recommended sample size for this method ranges from 30 to 100 samples. Solimun (2002) also states that there are several requirements in determining the sample size for SEM data analysis. In this study, the sample size is calculated using the Slovin formula. Based on these calculations (Nalendra et al., 2021: 27–28), the determined sample size is 396 respondents. The sampling technique used is non-

probability sampling with a purposive sampling method. Sugiyono (2013) defines purposive sampling as a sampling technique based on specific purposes or considerations. Each subject is deliberately selected from the population according to the relevant characteristics needed for this research.

Results and Discussions

Validity Testing

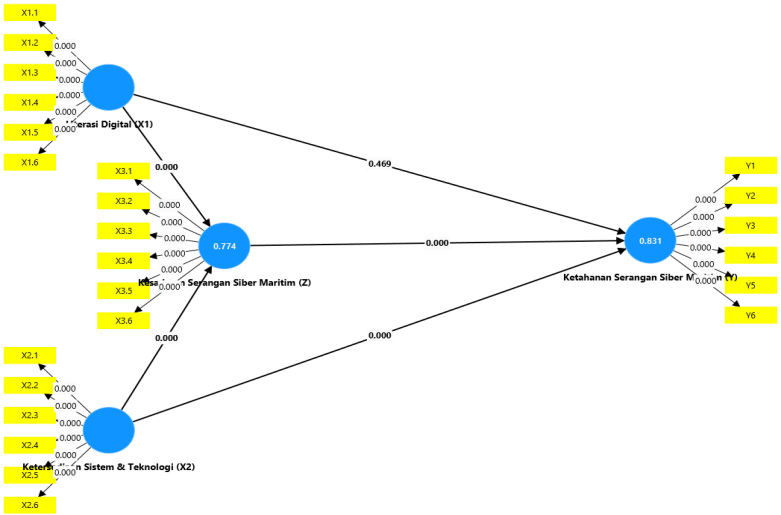


Figure 2. PLS Algorithm Output Results
Source: Calculated and Created by the Author (2024)

Based on the results of the PLS Algorithm output, as shown in Figure 1, a validity test is conducted for each variable utilized in this study. The validity testing is explained in more detail as follows:

Validity Testing Digital Literacy (X1)

Digital Literacy in this study is measured using three (6) indicators. The calculation results for the validity test of Digital Literacy are as follows:

Table 1. Results of Digital Literacy Validity Test

Variable /Dimension / Indicator	Loading Factor	Remarks
I am proficient in using digital tools such as PCs, maritime software, and digital navigation devices.	**0.844**	**Valid**
I have a solid understanding of the digital systems or technologies used onboard ships.	**0.886**	**Valid**
I am aware of potential cybersecurity threats that may occur while sailing.	**0.789**	**Valid**
I understand and apply safe practices when using digital technology.	**0.905**	**Valid**
I have a strong desire to continually learn about new technologies	**0.893**	**Valid**
I have a strong desire to continually learn about new technologies.	**0.883**	**Valid**

Source: Calculated and Created by the Author (2024)

Validity Testing of System & Technology Availability Variables (X2)

The System & Technology Availability variable is measured using three (6) statement indicators. The calculation results for the validity test of System & Technology Availability are as follows:

Table 2. Results of the Validity Testing for System & Technology Availability

Variable /Dimension / Indicator	Loading Factor	Remarks
Backup systems are always available when needed or during a cyberattack.	**0.867**	**Valid**
The ship has alternative communication methods in emergency situations or during a cyberattack.	**0.858**	**Valid**
The system recovery time in the event of a cyberattack is not prolonged.	**0.840**	**Valid**
The ship's crew is capable of handling cyber incidents quickly and effectively.	**0.906**	**Valid**
The onboard systems are capable of detecting cyber threats promptly.	**0.880**	**Valid**
The process of reporting incidents or indications of a cyberattack is promptly communicated to the ship's crew.	**0.887**	**Valid**

Source: Calculated and Created by the Author (2024)

Validity Testing for the Maritime Cybersecurity Awareness Variable (Z)

The Maritime Cybersecurity Awareness variable is measured using three (6) statement indicators. The calculation results for the validity test of Maritime Cybersecurity Awareness are as follows:

Table 3. Results of the Validity Testing for Maritime Cybersecurity Awareness

Variable /Dimension / Indicator	Loading Factor	Remarks
I understand the vulnerabilities of ships to potential cyberattacks.	**0.874**	**Valid**
I am aware of the potential impacts of cyberattacks on ship operations.	**0.868**	**Valid**
I am confident that the ship's digital systems or technologies can withstand cyberattacks effectively.	**0.876**	**Valid**
I believe the training provided is sufficient to address cyber threats.	**0.869**	**Valid**
I feel concerned about the possibility of cyberattacks occurring.	**0.758**	**Valid**
I feel prepared and know what to do in the event of a cyber incident.	**0.823**	**Valid**

Source: Calculated and Created by the Author (2024)

Validity Testing for Maritime Cybersecurity Resilience Variable (Y)

Maritime Cybersecurity Resiliencevariable is measured using three (6) statement indicators. The calculation results for the validity test of Maritime Cybersecurity Resilienceare as follows:

Table 4. Results of the Validity Testing for Maritime Cybersecurity Resilience

Variable /Dimension / Indicator	Loading Factor	Remarks
The operational system can recover quickly after experiencing disruptions.	**0.865**	**Valid**
Backup systems are always ready for use when needed.	**0.934**	**Valid**
Regular training is conducted periodically to enhance preparedness for cyber threats	**0.904**	**Valid**
In the event of a cyberattack, the ship's crew will immediately know the appropriate actions to address the disruption on board.	**0.918**	**Valid**
If a cyberattack occurs, the ship's crew will respond with exceptional speed.	**0.915**	**Valid**
Every day, the ship's crew adheres to security procedures diligently to ensure smooth operational continuity.	**0.873**	**Valid**

Source: Calculated and Created by the Author (2024)

Table 5. Results of the Discriminant Validity Testing

	(Z)	(Y)	(X2)	(X1)
(Z)				
(Y)	0,923			
(X2)	0,919	0,938		
(X2)	0,863	0,809	0,849	

Source: Calculated and Created by the Author (2024)

Based on the validity test results shown in Table above, the cross-loading values for each indicator used in this study indicate higher values for their respective constructs. This suggests that the latent constructs can effectively predict the indicators within their blocks better than the indicators from other blocks. Therefore, it can be concluded that all indicators used in this study have met the criteria for discriminant validity.

Reliability Testing

The Cronbach's Coefficient Alpha and Composite Reliability values for Digital Literacy, System & Technology Availability, Maritime Cybersecurity Awareness, and Maritime Cybersecurity Resilienceare as follows:

Table 6. Results of the Composite Reliability Testing

	Cronbach's alpha	Composite reliability (rho_c)	Average variance extracted (AVE)
(Z)	0.920	0.938	0.715
(Y)	0.954	0.963	0.813
(X2)	0.938	0.951	0.763
(X2)	0.935	0.949	0.755

Source: Calculated and Created by the Author (2024)

Based on the reliability test results shown in Table 6 above, the composite reliability values for the four variables (24 indicators) used in this study are greater than 0.70. Therefore, it can be concluded that the instruments used in this research are reliable.

Coefficient of Determination

The coefficient of determination (R^2) can be regarded as a percentage and varies from 0.0 to 1.0. The closer the value is to 1.0, the better the model is considered to be.

Table 7. Result Coefficient of Determination (R2)

	R-square	R-square adjusted
(Z)	0.774	0.773
(Y)	0.831	0.829

Source: Calculated and Created by the Author (2024)

Based on Table 7 above, Maritime Cybersecurity Resilience model yields a value of 0.831, or 83.1%, which falls into the strong category. Meanwhile, the Adjusted R-Square value for the Maritime Cybersecurity Awareness variable is 0.774, or 77.4%, also categorizing it as strong. Thus, it can be stated that the model is quite good, indicating that the predictive accuracy is satisfactory.

Hypothesis Testing

In this hypothesis testing section, the researcher conducts tests on the hypotheses proposed in Chapter II. The testing aims to examine whether the independent variables—Digital Literacy, System & Technology Availability—and the mediating variable—Maritime Cybersecurity Awareness—can influence Maritime Cybersecurity Resilience, both directly and indirectly. The results of this testing are based on the data analysis using Partial Least Square (PLS) with the SmartPLS 4.1.0.0 software.

Figure 2 presents the path diagram of the hypothesis testing results based on the Partial Least Square (PLS) analysis using SmartPLS version 4.1.0.0.

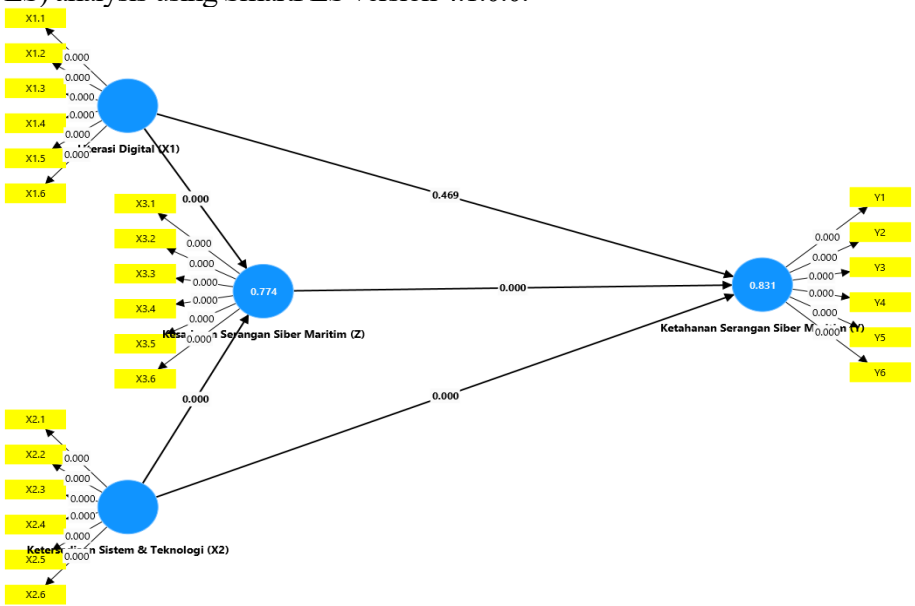


Figure 2. Path Diagram of Hypothesis Testing Output Results

Source: Calculated and Created by the Author (2024)

Based on the data processing results using SmartPLS version 4.1.0.0, as shown in the bootstrapping output in Figure 2 above, and as illustrated in Table 8, which presents the results of the direct effect testing, along with Table 9, which displays the results of the indirect effect testing, a more detailed explanation will be provided as follows:

Table 8. Testing the Direct Effects Output from Partial Least Square

	Original Sample	Standard Deviation	T Statistics	P values (1 Tail)	Conclusion
The Influence of *Digital Literacy* on *Maritime Cybersecurity Awareness* **(H1)**	0.324	0.06	5.43	0.000	H1 is accepted/supported
The Influence of *System & Technology Availability* on *Maritime Cybersecurity Awareness* **(H2)**	0.601	0.059	10.266	0.000	H2 is accepted/supported
The Influence of *Digital Literacy* on *Maritime Cybersecurity Resilience* **(H3)**	0.042	0.058	0.724	0.469	H0 is accepted/supported
The Influence of *System & Technology Availability* on *Maritime Cybersecurity Resilience* **(H4)**	0.535	0.093	5.751	0.000	H4 is accepted/supported
The Influence of *Maritime Cybersecurity Awareness* on *Maritime Cybersecurity Resilience***(H5)**	0.373	0.065	5.705	0.000	H5 is accepted/supported

Source: Calculated and Created by the Author (2024)

Hypothesis 1

The test results indicate a P-value of 0.000 < 0.05 (alpha 5%), thus H1 is accepted. It can be statistically concluded that, at a 95% confidence level, there is a positive influence of Digital Literacy on Maritime Cybersecurity Awareness among Indonesia active seafarer (Raut et al., 2022) . Based on this, it can be stated that Digital Literacy enhances Maritime Cybersecurity Awareness. individuals with better digital literacy tend to be more aware of cybersecurity threats

Hypothesis 2

The test results indicate a P-value of 0.000 < 0.05 (alpha 5%), thus H2 is accepted. It can be statistically concluded that, at a 95% confidence level, there is a positive influence of System & Technology Availability on Maritime Cybersecurity Awareness among Indonesia active seafarer (Kargin et al., 2020). Based on this, it can be stated that System & Technology Availability enhances Maritime Cybersecurity Awareness. A robust System & Technology Availability, equipped with automated monitoring and layered security systems, can increase awareness of potential cyber threats in real-time.

Hypothesis 3

The test results show a P-value of 0.469 > 0.05 (alpha 5%), thus H3 isn't accepted. It can be statistically concluded that, at a 95% confidence level, there is no positive influence of Digital Literacy on Maritime Cybersecurity Resilience among Indonesia active seafarer. These results may indicate that efforts to improve digital literacy alone may not be enough to strengthen maritime cyber resilience. Therefore, a more comprehensive approach is needed, such as special cybersecurity training, improving technological infrastructure, or implementing stricter regulatory policies.

Hypothesis 4

The test results indicate a P-value of 0.000 < 0.05 (alpha 5%), thus H4 is accepted. It can be statistically concluded that, at a 95% confidence level, there is a positive influence of System & Technology Availability on Maritime Cybersecurity Resilience among Indonesia active seafarer (Karaca & Söner, 2023). Therefore, it can be stated that System & Technology Availability enhances Maritime Cybersecurity Resilience. A good backup system allows for quick recovery from cyber incidents, reducing the impact and potential losses.

Hypothesis 5

The test results show a P-value of 0.000 < 0.05 (alpha 5%), leading to the acceptance of H5. It can be concluded statistically, at a 95% confidence level, that there is a positive influence of Maritime Cybersecurity Awareness on Maritime Cybersecurity Resilience among Indonesia active seafarer (Svilicic, Kamahara, et al., 2019). Therefore, it can be stated that Maritime Cybersecurity Awareness enhances Maritime Cybersecurity Resilience, A strong and comprehensive maritime cyber security system is an important foundation in building maritime system resilience against various cyber threats.

Table 9. Testing the Influence of Indirect Output from Partial Least Square

	Original Sample	Standard Deviation	T Statistics	P values (1 Tail)	Conclusions
Digital Literacy indirectly influences Maritime Cybersecurity Resilience through Maritime Cybersecurity Awareness ***(H6)***	0.121	0.031	3.918	0.000	H6 is accepted/supported.
System & Technology Availability influences Maritime Cybersecurity Resilience through Maritime Cybersecurity Awareness **(H7)**	0.224	0.046	4.856	0.000	H7 is accepted/supported.

Source: Calculated and Created by the Author (2024)

Hypothesis 6

The results of the test indicate a P-value of 0.000, which is less than 0.05 (alpha 5%), thus supporting H6. It can be concluded statistically, at a 95% confidence level, that there is a positive influence of the theory of Digital Literacy indirectly through Maritime Cybersecurity Awareness on Maritime Cybersecurity Resilience. Based on this, it can be stated that Digital Literacy indirectly through Maritime Cybersecurity Awareness can enhance Maritime Cybersecurity Resilience (Svilicic et al., 2019)

Hypothesis 7

The results of the test indicate a P-value of 0.000, which is less than 0.05 (alpha 5%), thus supporting H7. It can be concluded statistically, at a 95% confidence level, that there is a positive influence of the theory of System & Technology Availability indirectly through Maritime Cybersecurity Awareness on Maritime Cybersecurity Resilience. Based on this, it can be stated that System & Technology Availability indirectly through Maritime Cybersecurity Awareness can enhance Reuse Intention (Androjna et al., 2020).

Conclusion

This study highlights the critical relationships between Digital Literacy, System & Technology Availability, Maritime Cybersecurity Awareness, and Maritime Cybersecurity Resilience among active seafarers in Indonesia. The findings demonstrate that Digital Literacy positively influences Maritime Cybersecurity Awareness, indicating that individuals with higher digital proficiency are better equipped to identify and address cybersecurity threats. Similarly, the availability of robust systems and technologies significantly enhances cybersecurity awareness by enabling real-time threat monitoring and prevention.

However, Digital Literacy does not directly impact Maritime Cybersecurity Resilience, suggesting that digital proficiency alone is insufficient to strengthen resilience. In contrast, System & Technology Availability has a direct and significant influence on resilience, particularly through the implementation of effective backup systems and layered security measures. Maritime Cybersecurity Awareness plays a pivotal role in strengthening resilience, both directly and as a mediator between digital literacy and technology systems. Based on these findings, it is recommended to implement targeted digital literacy training programs, invest in advanced technological infrastructure, conduct specialized cybersecurity training, and establish strict regulatory policies. These efforts will collectively enhance maritime cybersecurity awareness and resilience, fostering a robust and adaptive cybersecurity ecosystem in Indonesia.

REFERENCES

Afenyo, M., & Caesar, L. D. (2023). *Maritime cybersecurity threats: Gaps and directions for future research*. https://doi.org/10.1016/j.ocecoaman.2023.106493

Agbo-ola, A. (2022). *Motivating Cybersecurity Awareness within an Organisation: An explorative study from an awareness practitioners perspective*.

Alotaibi, A. (2022). *Ransomware Attacks As a Cybercrime in the United States: an Exploratory Study*.

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, *8*(10), 1–21. https://doi.org/10.3390/jmse8100776

BIMCO. (2021). *BIMCO Seafarer Workforce Report 2021-1.pdf*.

Catarina, N. A. S. (2020). *Contingency Theory and The Role of Mediating Effect*. https://osf.io/zxfyt/download

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, *62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Karaca, İ., & Söner, Ö. (2023). an Evaluation of Students' Cybersecurity Awareness in the Maritime Industry. *International Journal of 3D Printing Technologies and Digital Industry*, *7*(1), 78–89. https://doi.org/10.46519/ij3dptdi.1236264

Karas, A. (2023). Maritime Industry Cybersecurity: A Review of Contemporary Threats. *European Research Studies Journal*, 921–930. https://doi.org/10.35808/ersj/3336

Kargin, A., Panchenko, A., Ivaniuk, O., & Muhitovs, R. (2020). Motion Control of Smart Autonomous Mobile System Based on the Perception Model. In *Lecture Notes in Intelligent Transportation and Infrastructure: Vol. Part F1382*.

https://doi.org/10.1007/978-3-030-39688-6_20
Mersinas, K., & Chana, C. D. (2022). Reducing the Cyber-Attack Surface in the Maritime Sector via Individual Behaviour Change CYBER 2022 : The Seventh International Conference on Cyber-Technologies and Cyber-Systems. *The Seventh International Conference on Cyber-Technologies and Cyber-Systems Reducing*, *7*(c), 93–99.
Putri, S. A., & Burhanuddin, A. (2024). Maritime Cybersecurity: Tantangan Dan Strategi Keamanan Maritim Indonesia. *MANDUB: Jurnal Politik, Sosial, Hukum, Dan Humaniora*, *2*(1), 378–386. https://doi.org/10.59059/mandub.v2i1.940
Raut, D. S. D., Shinde, D. A. R., & Patil, D. M. K. (2022). Cyber Security Awareness: A Movement of Digital Literacy Towards making of Digital India. *IBMRD's Journal of Management & Research*, *11*(2), 174. https://doi.org/10.17697/ibmrd/2022/v11i2/172617
Svilicic, B., Brčić, D., Žuškin, S., & Kalebić, D. (2019). Raising awareness on cyber security of ecdis. *TransNav*, *13*(1), 231–236. https://doi.org/10.12716/1001.13.01.24
Svilicic, B., Kamahara, J., Rooks, M., & Yano, Y. (2019). Maritime Cyber Risk Management: An Experimental Ship Assessment. *Journal of Navigation*, *72*(5), 1108–1120. https://doi.org/10.1017/S0373463318001157

Copyright holder:
Arizal Hendriawan, Idris Gautama, Denny Siahaan, Kurniawan (2025)

First publication right:
Syntax Literate: Jurnal Ilmiah Indonesia

This article is licensed under: