KARYA ILHAM PUBLISHING
CONNECTING MINDS, BRIDGING IDEAS, INSPIRING READERS

Journal of Advanced Research in Business and Management Studies

Journal homepage:
https://karyailham.com.my/index.php/arbms/index
ISSN: 2462-1935

JOURNAL OF ADVANCED RESEARCH IN
BUSINESS AND MANAGEMENT STUDIES
ISSN: 2462-1935

Sailing into Cyber Awareness: Exploring Determinants of Security Behaviour Among Seafarers

Hasivini Manaoogaran[1], Noor Fadhiha Mokhtar[1,*]

[1] Faculty of Business, Economics and Social Development, Universiti Malaysia Terengganu, 21030 Kuala Nerus, Terengganu, Malaysia

ARTICLE INFO

Article history:
Received 1 December 2025
Received in revised form 1 January 2026
Accepted 2 February 2026
Available online 6 March 2026

Keywords:
Maritime cybersecurity; cybersecurity awareness; Health Belief Model; maritime digitalization

ABSTRACT

The maritime industry is increasingly vulnerable to cyber threats, as demonstrated by the 2017 Maersk cyber-attack, which exposed the fragility of global shipping operations. With the growing integration of digital technologies into shipboard systems, ensuring robust cybersecurity awareness among maritime personnel is more crucial than ever. However, empirical research on the human and behavioural factors influencing cybersecurity awareness in maritime contexts remains limited. Thus, this study aims to identify the determinants of cybersecurity awareness (self-efficacy, perceived benefits, cues to action, and perceived susceptibility) among Malaysian seafarers. Grounded in the Health Belief Model—a well-established framework from preventive healthcare adapted in this study to understand users' computer security behaviour. This study employs a quantitative approach to examine hypothesised relationships among these variables. Data were collected through structured questionnaires administered to shipboard personnel who regularly operate computer systems. Findings reveal that self-efficacy, perceived benefits and cues to action significantly contribute to improving cybersecurity awareness. In contrast, perceived susceptibility emerged as a weaker predictor. This is likely due to seafarers' limited experience with actual cyber incidents and the common belief that such threats mainly affect shore-based systems. Incident-based training and realistic simulations are recommended to clearly demonstrate the operational impact of cyber-attacks on shipboard environments. This study contributes to the growing body of literature on maritime cybersecurity by addressing a gap concerning human factors in information security behaviour. It offers practical implications for maritime organisations, shipping companies, and policymakers seeking to strengthen cyber resilience. Promoting continuous training and awareness initiatives can help foster a proactive cybersecurity culture among seafarers and mitigate risks associated with human error in digital maritime operations.

[*] *Corresponding author.*
E-mail address: noorfadhiha@umt.edu.my

https://doi.org/10.37934/arbms.42.1.6673

1. Introduction

The shipping industry is undergoing a digital transformation, becoming increasingly dependent on digital network systems and data. The driving force behind this transformation is the improvement of operational efficiency, sustainability and competitiveness of the global shipping supply chain [1]. Digitalisation and automation are leading the shipping industry towards a more profitable and carbon-free future [2]. As a result, shipping companies are actively using digital technologies to optimize their operations [3]. Unfortunately, as technology becomes more prevalent in the shipping industry, cybercriminals are increasingly exploiting these vulnerabilities [4].

As maritime operations become increasingly digital, limited attention has been paid in academic circles to cybersecurity issues on board ships, particularly those related to ship operation technologies, crew awareness, and incident response preparedness [5,6]. Addressing these issues is critical to creating a more resilient maritime ecosystem [7]. Thus, as the global shipping industry becomes increasingly reliant on advanced technology, the companies must pay greater attention to and understand the scale and impact of cyber-attacks [8]. Much of the world's shipping depends on maritime trade, so cyber-attacks on maritime infrastructure (a prime target for hackers) can have far-reaching consequences [9].

To achieve its digital transformation goals, Malaysia has begun to actively invest in intelligent port infrastructure, maritime ICT systems, and the development of a national cybersecurity policy [10]. However, the country's efforts in maritime cybersecurity have focused mainly on technological innovation and organisational management, with little consideration given to the behaviour of seafarers [11]. While ports and shipping companies are increasingly implementing digital systems, many seafarers still do not receive adequate cybersecurity training, and knowledge of best practices varies between operators [12]. The lack of standardised and continuous training has led to significant gaps in seafarers' cybersecurity preparedness.

Therefore, the objective of this study is to identify the determinants of cybersecurity awareness among Malaysian seafarers to develop sustainable and human-oriented cybersecurity behaviour in the maritime industry.

2. Research Methodology

This study used a quantitative cross-sectional research method to examine the factors influencing Malaysian seafarers' awareness of cybersecurity. Based on the Health Belief Model (HBM), the influence of four psychological constructs, namely self-efficacy, perceived benefits, behavioural motivation, and perceived vulnerability, on seafarers' awareness of cybersecurity was examined. The primary data was collected through a survey designed to statistically test the presumed relationships between variables. The target respondents for this study were Malaysian seafarers, mainly engaged in the operation of or interaction with ship systems. The sample consisted of two groups: officers and ratings (general crews). These two groups were selected because it represents different responsibilities in performing their duties on board a ship and may be affected by cybersecurity measures.

Purposive sampling technique was used to collect 114 valid questionnaires to ensure that participants had relevant experience with digital systems or held positions that could lead to cyber risks. This sample size met the minimum standards for Structural Equation Modelling (SEM) using Partial Least Squares (PLS-SEM), especially when the model contained fewer than five predictor variables [13]. Data collection was conducted using a self-administered structured questionnaire consisting of two main parts. The first part collected demographic data such as gender, age, job title, and years of experience. The second part assessed research constructs using validated items (adapted from previous studies on cybersecurity behaviour and health psychology). Each construct was assessed using several items and a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). A pilot test involving 15 seafarers was conducted to assess clarity, content relevance, and linguistic appropriateness. Feedback from the pilot led to minor refinements in wording. Content validity was also reviewed by maritime cybersecurity experts and researchers in behavioural science.

Data collection was conducted over two months using both online forms and printed questionnaires to facilitate completion by respondents. The questionnaires were distributed by maritime companies, shipping companies, and professional maritime networks. All respondents participated in the survey voluntarily and with informed consent. Confidentiality and privacy were strictly guaranteed throughout the research process. Data analysis was performed using partial least squares structural equation modelling (PLS-SEM) with SmartPLS 4.0 software.

3. Results and Discussions

3.1 Demographic Profile

A total of 114 valid responses were collected from Malaysian seafarers working in the engine and deck departments. The gender distribution indicated a majority of male respondents (90.4%), while female seafarers represented 9.6% (n = 11). This gender distribution is consistent with the broader trend in the maritime industry, where female participation remains low but is gradually increasing due to gender inclusion initiatives. In terms of age, the largest proportion of respondents were aged 28–32 years (28.1%), followed by 33–37 years (18.4%) and 23–27 years (12.3%), reflecting a relatively young and active workforce. Notably, 13.2% of respondents were between 18–22 years, indicating new entrants into the industry, while only 7.9% were aged over 48 years, representing a small segment of senior personnel.

Regarding department affiliation, 61.4% (n = 70) of respondents were from the engine department, while 38.6% (n = 44) were from the deck department, providing perspectives from both operational and navigational domains. In terms of rank, officers made up the majority of the sample (70.2%, n = 80), with ratings (general crew) comprising the remaining 29.8% (n = 34). This distinction is important, as officers are often more involved in shipboard decision-making and digital system management. The data also revealed that most respondents had 6–10 years of experience in the maritime sector (38.6%), followed by those with 11–15 years (26.3%) and 1–5 years (21.1%). A smaller group (14.0%) had over 16 years of service. This spread allows for a comprehensive view of cybersecurity awareness across seafarers with different levels of experience. Table 1 presents the demographic characteristics of the respondents.

Table 1
Demographic profile

Demographic Variable	Category	Frequency (n)	Percentage (%)
Gender	Male	103	90.4
	Female	11	9.6
Age	18–22 years	15	13.2
	23–27 years	14	12.3
	28–32 years	32	28.1
	33–37 years	21	18.4
	38–42 years	13	11.4
	43–47 years	10	8.8
	>48 years	9	7.9
Department	Engine	70	61.4

Demographic Variable	Category	Frequency (n)	Percentage (%)
	Deck	44	38.6
Rank	Officer	80	70.2
	Rating (Crew)	34	29.8
Years of Service in Maritime Industry	1–5 years	24	21.1
	6–10 years	44	38.6
	11–15 years	30	26.3
	16–20 years	16	14.0

3.2 Measurement Model Assessment

The measurement model assessment confirmed that all constructs in the study demonstrated acceptable levels of reliability and validity. Internal consistency reliability was established as all Cronbach's Alpha and Composite Reliability (CR) values exceeded the recommended threshold of 0.70, indicating that the items consistently measured their respective constructs [13]. Convergent validity was achieved, with all constructs recording Average Variance Extracted (AVE) values above 0.50, confirming that each construct explained more than half of the variance in its indicators [14]. Discriminant validity was supported using both the Fornell-Larcker criterion and the Heterotrait-Monotrait (HTMT) ratio, ensuring that each construct was empirically distinct from others [15]. These results confirm that the measurement model is statistically robust and suitable for structural model evaluation using PLS-SEM.

3.3 Hypotheses Testing

The structural model was evaluated to test the hypothesized relationships between the independent variables—self-efficacy, perceived benefits, cues to action, and perceived susceptibility—and the dependent variable, cybersecurity awareness. The bootstrapping procedure with 5,000 resamples in SmartPLS 4.0 was used to estimate path coefficients (β), t-values, and p-values. The results are presented in Table 2.

Table 2
Hypothesis testing results

Hypothesis	Relationship	Path Coefficient (β)	t-value	p-value	Result
H1	Self-Efficacy → Cybersecurity Awareness	0.364	5.027	0.000	Supported
H2	Perceived Benefits → Cybersecurity Awareness	0.301	4.218	0.000	Supported
H3	Cues to Action → Cybersecurity Awareness	0.278	3.987	0.000	Supported
H4	Perceived Susceptibility → Cybersecurity Awareness	0.067	1.229	0.220	Not Supported

The hypothesis testing results in Table 2 provide valuable insights into the behavioural drivers of cybersecurity awareness among Malaysian seafarers. Four hypothesized relationships were tested using PLS-SEM, and the results reflect both statistical significance and practical implications.

According to Table 2, self-efficacy shows the strongest positive influence on cybersecurity awareness, indicating that seafarers who believe in their ability to detect and manage cyber threats are significantly more aware of cybersecurity practices. The path coefficient (β = 0.364) suggests a moderate-to-strong effect size, and the high t-value confirms its statistical significance. This finding supports Bandura's [16] that social cognitive theory, which posits that self-efficacy is a key determinant of behaviour, especially in high-risk, skill-dependent environments. In the context of maritime operations is where cyber threats may compromise navigation, communication, and operational control, the seafarers with greater self-efficacy interpret risks as manageable and take appropriate precautions [17]. Furthermore, this result reinforces the importance of competency-based training, where technical skills are enhanced alongside confidence through real-time simulations, practical drills, and incident response exercises [18].

Besides, the relationship between perceived benefits and cybersecurity awareness is also statistically significant, with a path coefficient of 0.301, indicating a moderate positive effect. This means that when seafarers understand the advantages and usefulness of adopting cybersecurity practices such as protecting ship operations or reducing downtime which are more likely to be aware and responsive. This outcome aligns with earlier studies in information security, which found that users are more willing to comply with security measures when they perceive direct personal or organizational benefits [19]. Similarly, Ifinedo [20] emphasized that highlighting the beneficial outcomes of compliance—such as system reliability and organizational efficiency—increases the likelihood of employees engaging in secure information behaviour. It implies that shipping companies should clearly communicate the real-world benefits of cyber hygiene to strengthen adoption [21].

Cues to action also show a significant positive effect on cybersecurity awareness. The β value of 0.278 suggests that reminders, training, prompts, and policies play an important role in maintaining seafarers' awareness. While the effect is slightly lower than self-efficacy and perceived benefits, it remains meaningful. Research suggests that structured and frequent cues, like scenario-based training and cybersecurity simulations, enhance long-term cyber hygiene [22]. Furthermore, cues to action are particularly vital in settings like ships, where turnover is high, access to shore-based support is limited, and operational schedules are demanding. This reinforces the need for sustainable cybersecurity communication strategies onboard that go beyond one-off training sessions. Frequent, context-specific cues can increase not only awareness but also actual secure behaviour, reducing the risk of human error in digital maritime operations [23]. Embedding such measures into routine shipboard operations not only strengthens human defences but also supports IMO's Guidelines on Maritime Cyber Risk Management [24], ultimately contributing to a resilient maritime cybersecurity culture [25].

On the other hand, perceived susceptibility did not significantly predict cybersecurity awareness. The low path coefficient (0.067) and non-significant p-value ($p > 0.05$) suggest that seafarers do not strongly believe they are personally at risk of cyber-attacks. This may stem from a lack of firsthand experience with cyber incidents or the belief that ships are isolated from such threats [17]. This result aligns with past literature indicating that users often underestimate their own vulnerability to cyber threats [26]. The seafarers may hold a false sense of security due to the physical isolation of ships at sea, assuming that limited connectivity reduces the likelihood of cyber intrusions—a notion increasingly challenged by modern shipboard systems like ECDIS, AIS, and satellite communication, which are highly vulnerable to cyber exploitation [27]. Due to that shipping companies need to increase awareness of real maritime cyber incidents through case studies and threat simulations to enhance perceived risk and motivate precautionary behaviours.

4. Theoretical and Practical Contribution

This study contributes to the theoretical development of cybersecurity behaviour research by extending the application of the Health Belief Model (HBM) into the maritime domain—a context that remains underexplored in cybersecurity literature. While the HBM has been widely used in health and information systems research, its integration into maritime cybersecurity offers a novel lens to understand how individual cognitive perceptions—such as self-efficacy, perceived benefits, cues to action, and susceptibility—affect awareness levels among seafarers. The findings confirm that HBM constructs can be meaningfully applied to model cybersecurity behaviour in operational maritime environments, especially among shipboard personnel who interact with critical digital infrastructure. This provides a theoretical foundation for future behavioural studies in maritime risk management and offers a basis for cross-sectoral comparisons with aviation, healthcare, and other high-reliability industries.

From a practical perspective, the study provides valuable insights for shipping companies, maritime academies, and policymakers in designing more effective cybersecurity awareness programs. The significant influence of self-efficacy, perceived benefits, and cues to action underscores the need for tailored training programs that not only equip seafarers with technical skills but also clearly communicate the advantages of secure practices and reinforce them through continuous onboard engagement. The insignificant role of perceived susceptibility signals a need to raise risk perception through case-based simulations and exposure to real-world maritime cyber incidents. By addressing both capability and motivation, maritime organizations can foster a stronger cybersecurity culture and reduce the likelihood of human-related vulnerabilities in shipboard digital systems.

5. Conclusion

This study examined the psychological determinants influencing cybersecurity awareness among Malaysian seafarers by applying the Health Belief Model (HBM). The findings indicate that self-efficacy, perceived benefits, and cues to action significantly contribute to enhancing cybersecurity awareness onboard vessels, while perceived susceptibility showed no significant effect. These insights highlight that seafarers are more likely to adopt secure practices when they feel confident in their abilities, perceive real value in doing so, and are regularly reminded or prompted through organizational cues. However, a limited perception of personal risk may hinder the proactive adoption of cybersecurity measures.

Moving forward, this study provides a foundation for both theory-building and practical strategies in maritime cybersecurity. Future research could extend this framework by incorporating additional behavioural variables such as organizational support, prior incident experience, or cultural influences. Moreover, comparative studies across regions, vessel types, or company sizes could offer deeper insights into contextual differences in cybersecurity practices. Longitudinal studies would also be beneficial to capture changes in awareness and behaviour over time, especially following regulatory changes or major cyber incidents. As the maritime industry continues to digitize, understanding and improving human factors in cybersecurity remains a critical priority for achieving operational safety and resilience at sea.

References

[1] Kusumawati, Evyana Diah, and Budi Punomo. "Technological Transformation and Innovation Strategy as a Key Pillar in Improving Sustainability Efficiency In The Maritime Industry." *IITE Proceeding: International Inovation Technology Proceeding* 2, no. 1 (2024): 65-76.

[2] Alavi-Borazjani, Seyedeh Azadeh, Alberto Antonio Bengue, Valentina Chkoniya, and Muhammad Noman Shafique. "An overview of critical success factors for digital shipping corridors: A roadmap for maritime logistics modernization." *Sustainability* 17, no. 12 (2025): 5537. https://doi.org/10.3390/su17125537

[3] Gavalas, Dimitris, Theodoros Syriopoulos, and Efthimios Roumpis. "Digital doi: 10.1186/s41072-022-00111-y.adoption and efficiency in the maritime industry." *Journal of Shipping and Trade* 7, no. 1 (2022): 11. https://doi.org/10.1186/s41072-022-00111-y

[4] Akpan, Frank, Gueltoum Bendiab, Stavros Shiaeles, Stavros Karamperidis, and Michalis Michaloliakos. "Cybersecurity challenges in the maritime sector." *Network* 2, no. 1 (2022): 123-138.

https://doi.org/10.3390/network2010009

[5] Vaarandi, Risto, Leonidas Tsiopoulos, Gabor Visky, Muaan Ur Rehman, and Hayretdin Bahşi. "A Systematic Literature review of Cyber security monitoring in Maritime." *IEEE Access* (2025). https://doi.org/10.1109/ACCESS.2025.3567385

[6] Caprolu, Maurantonio, Roberto Di Pietro, Simone Raponi, Savio Sciancalepore, and Pietro Tedeschi. "Vessels cybersecurity: Issues, challenges, and the road ahead." *IEEE Communications Magazine* 58, no. 6 (2020): 90-96. https://doi.org/10.1109/MCOM.001.1900632

[7] Todorov, Yavor. "Navigating uncharted waters: tackling maritime cybersecurity challenges in the black sea region." *Information & Security* 55, no. 2 (2024): 113-132. https://doi.org/10.11610/isij.5509

[8] Clavijo Mesa, Maria Valentina, Carmen Elena Patino-Rodriguez, and Fernando Jesus Guevara Carazas. "Cybersecurity at sea: A literature review of cyber-attack impacts and defenses in maritime supply chains." *Information* 15, no. 11 (2024): 710. https://doi.org/10.3390/info15110710

[9] Polikarovskykh, Oleksiy, Mykola Malaksiano, Varvara Piterska, Yurii Daus, and Mariia Tkachenko. "Measures to counter cyber attacks on maritime transportation." In *Maritime Systems, Transport and Logistics I: Safety and Efficiency of Operation*, pp. 197-212. Cham: Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-82027-4_13

[10] Marine Department Malaysia, “Digital Strategic Plan: 2021-2025,” 2022.

[11] Mersinas, Konstantinos, and D. C. Chupkemi. "Reducing the Cyber-Attack Surface in the Maritime Sector via Individual Behaviour Change." *Proceedings of the CYBER* (2022).

[12] Heering, Dan. "Rethinking Seafarer Training for the Digital Age." In *Maritime Cybersecurity*, pp. 29-53. Cham: Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-87290-7_3

[13] Hair, Joseph F., Jeffrey J. Risher, Marko Sarstedt, and Christian M. Ringle. "When to use and how to report the results of PLS-SEM." *European business review* 31, no. 1 (2019): 2-24. https://doi.org/10.1108/EBR-11-2018-0203

[14] Fornell, Claes, and David F. Larcker. "Evaluating structural equation models with unobservable variables and measurement error." *Journal of marketing research* 18, no. 1 (1981): 39-50. https://doi.org/10.1177/002224378101800104

[15] Henseler, Jörg, Christian M. Ringle, and Marko Sarstedt. "Using partial least squares path modeling in advertising research: basic concepts and recent issues." In *Handbook of research on international advertising*. Edward Elgar Publishing, 2012. https://doi.org/10.4337/9781781001042.00023

[16] A. Bandura, W. H. Freeman, and R. Lightsey, “Self-Efficacy: The Exercise of Control,” *J. Cogn. Psychother.*, 1999. https://doi.org/10.1891/0889-8391.13.2.158

[17] Tam, Kimberly, and Kevin Jones. "Cyber-risk assessment for autonomous ships." In *2018 international conference on cyber security and protection of digital services (cyber security)*, pp. 1-8. IEEE, 2018. https://doi.org/10.1109/CyberSecPODS.2018.8560690

[18] Kanwal, Kamlesh, Wenming Shi, Christos Kontovas, Zaili Yang, and Chia-Hsun Chang. "Maritime cybersecurity: are onboard systems ready?." *Maritime Policy & Management* 51, no. 3 (2024): 484-502. https://doi.org/10.1080/03088839.2022.2124464

[19] Ng, Boon-Yuen, Atreyi Kankanhalli, and Yunjie Calvin Xu. "Studying users' computer security behavior: A health belief perspective." *Decision Support Systems* 46, no. 4 (2009): 815-825. https://doi.org/10.1016/j.dss.2008.11.010

[20] Ifinedo, Princely. "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory." *Computers & security* 31, no. 1 (2012): 83-95. https://doi.org/10.1016/j.cose.2011.10.007

[21] Odimarha, Agnes Clare, Sodrudeen Abolore Ayodeji, and Emmanuel Adeyemi Abaku. "Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies." *World Journal of Advanced Science and Technology* 5, no. 1 (2024): 026-030. https://doi.org/10.53346/wjast.2024.5.1.0030

[22] Parsons, Kathryn, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, and Tara Zwaans. "The human aspects of information security questionnaire (HAIS-Q): two further validation studies." *Computers & Security* 66 (2017): 40-51. https://doi.org/10.1016/j.cose.2017.01.004

[23] Parsons, Kathryn, Marcus Butavicius, Paul Delfabbro, and Meredith Lillie. "Predicting susceptibility to social influence in phishing emails." *International Journal of Human-Computer Studies* 128 (2019): 17-26. https://doi.org/10.1016/j.ijhcs.2019.02.007

[24] International Maritime Organization, “Guidelines on Maritime Cyber Risk Management MSC-FAL.1/Circ.3/Rev.2,” 2022. [Online]. Available: https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx

[25] Hopcraft, Rory, Kimberly Tam, Juan Dorje Palbar Misas, Kemedi Moara-Nkwe, and Kevin Jones. "Developing a maritime cyber safety culture: Improving safety of operations." *Maritime Technology and Research* 5, no. 1 (2023): 258750-258750. https://doi.org/10.33175/mtr.2023.258750

[26] Alnifie, Khaled M., and Charles Kim. "Appraising the manifestation of optimism bias and its impact on human perception of cyber security: A meta analysis." *Journal of Information Security* 14, no. 2 (2023): 93-110. https://doi.org/10.4236/jis.2023.142007

[27] Oruc, Aybars. "Cyber security of the integrated navigation system (INS)." PhD diss., Ph. D. dissertation, Dept. Inf. Secur. Commun. Technol., Norwegian Univ. Sci. Technol., Trondheim, Norway, 2024.