https://doi.org/10.7251/EMC2603962R
UDK: 351.824.11:368.2.026.4(4-672EU)
Datum prijema rada: 12. mart 2026.
Submission Date: March 12, 2026
Datum prihvatanja rada: 7. septembar 2026.
Acceptance Date: September 7, 2026
Časopis za ekonomiju i tržišne komunikacije
Economy and Market Communication Review
Godina/Vol. **XVI** • Br./No. **III**
str./pp. 962-978

ORIGINALNI NAUČNI RAD / ORIGINAL SCIENTIFIC PAPER

CYBERSECURITY IN THE MARITIME INDUSTRY: CREW PREPAREDNESS, ORGANISATIONAL COMMUNICATION, AND ECONOMIC IMPLICATIONS

Maja Račić | PhD, Faculty of Maritime Studies, University of Split, Split, Croatia, maja.racic@pfst.hr; ORCID ID: 0009-0009-2771-2853
Mira Pavlinović | Associate Professor, Faculty of Maritime Studies, University of Split, Split, Croatia, mira.pavlinovic@pfst.hr; ORCID ID 0000-0002-3613-9675
Jerko Glavaš | Full Professor, Faculty of Economics and Business in Osijek, J. J. Strossmayer University of Osijek, Osijek, Croatia, jerko.glavas@efos.hr; ORCID ID 0000-0001-9227-1227

***Abstract**: The maritime industry is increasingly exposed to cyber threats due to its strong reliance on information and communication technologies and automated systems. While digitalisation enhances the efficiency of maritime operations, it simultaneously creates new security challenges related to information management, the exchange of security-related data, and coordination within shipboard systems. In this context, cybersecurity is not solely a technical issue but an organisational and managerial one in which the crew plays a central role.*

This preliminary exploratory and descriptive study examines respondents' reported experiences and perceptions of maritime crew awareness, preparedness, and communication concerning cyber threats. The analysis addresses crew training, respondents' familiarity with security protocols, threat information sharing, perceived communication effectiveness among crew members, access control to information systems, and awareness of recovery plans and business continuity procedures in the event of a cyber incident.

The results indicate that respondents frequently reported basic technical security measures on board, while training was often reported as a one-time experience, participation in regular simulations was limited, and awareness of information-sharing practices and protocols was inconsistent. Respondents also frequently perceived cyber incidents as potentially having operational and economic consequences, including disruptions and negative effects on the financial stability and competitiveness of shipping companies. Based on these findings, this paper proposes preliminary recommendations for improving crew cyber preparedness, considering their potential operational and economic implications for maritime operations and shipping companies. This paper builds upon previous research on cyber challenges in the Croatian maritime industry published in 2022 by Springer.

The findings are based on a convenience sample of 77 male seafarers attending a Special Education Programme at a single Croatian institution. They represent respondents' self-reported perceptions rather than verified onboard practices or demonstrated economic effects and should not be generalised to the maritime industry as a whole.

***Keywords**: cybersecurity, maritime industry, cyber risk management, organisational communication, economic implications*

***JEL classification**: M15, D81, L92, J24*

INTRODUCTION

The contemporary maritime industry is facing increasingly complex cybersecurity challenges, primarily due to its growing reliance on digital technologies and automated systems. The integration of information and operational technologies into shipboard operations—including navigation, communication, cargo handling, and engine room management—significantly contributes to operational efficiency, while simultaneously introducing a range of new vulnerabilities to cyber threats (Car et al., 2014; Standard Club, 2020). Cyber-attacks in the maritime domain no longer represent solely a technical challenge but entail potential consequences for human safety, environmental protection, and the economic sustainability of the entire logistics system.

One of the key challenges lies in the quantification of the economic consequences of cyber incidents, including operational disruptions, revenue losses, increased insurance premiums, system recovery costs, and reputational damage. Industry examples, such as the attack on Maersk in 2017, have demonstrated that costs may reach hundreds of millions of dollars, while even smaller incidents can result in substantial losses if they interrupt vessel operations or compromise the integrity of supply chains. Cybersecurity management is therefore increasingly viewed as an integral component of financial planning and strategic decision-making, with investments in security measures and crew training more frequently justified through return-on-security-investment (ROSI) models.

Cyber risk management has evolved from traditional information security, with a key transition towards an integrated approach emerging in the early 2000s, when security began to be perceived as a business risk rather than exclusively a technical problem (Blakley et al., 2001; Gordon et al., 2003; Eling et al., 2021). This shift in perspective created space for the incorporation of organisational, managerial, and human factors into cybersecurity systems, which was soon reflected in industrial practice through standards such as ISO/IEC 27005:2008 and frameworks developed by national agencies such as NIST (NIST, 2024).

In the maritime sector, these concepts began to be applied more systematically only after 2014, when the International Maritime Organization (IMO) initiated the development of guidelines for cyber risk management (IMO, 2017a; IMO, 2017b). Industry stakeholders, led by BIMCO and partner organisations, developed *The guidelines on cyber security onboard ships*, which were subsequently integrated into safety management requirements through IMO Resolution MSC.428(98) (DNV, 2020). In this way, cybersecurity was formally embedded into existing Safety Management Sys-

tems (SMS); however, its operational implementation has remained largely dependent on the human factor.

Effective cybersecurity management requires a comprehensive approach that includes threat identification, vulnerability assessment, the definition of preventive measures, and the development of response and recovery plans. Within this framework, the human factor represents the central link between technical systems and organisational procedures, with the ship's crew often constituting the first line of defence against cyber threats. Nevertheless, existing research indicates a low level of crew awareness and preparedness, accompanied by a lack of formal education and simulation-based exercises (Safety4Sea, 2017; Chupkemi & Mersinas, 2024).

Multicultural and technically heterogeneous crews, frequent crew rotation, and limited shipboard connectivity further complicate the implementation of unified and effective training programmes (Chupkemi & Mersinas, 2024). Under such conditions, communication regarding cyber threats gains particular importance as an organisational mechanism for coordination and the transfer of security-relevant information.

For these reasons, more recent guidelines, as well as classification recommendations such as DNVGL-RP-0496 (DNV, 2016), increasingly emphasise the need to develop so-called *cyber hygiene*, regular training, and the implementation of simulations in order to strengthen the resilience of the human factor. In this paper, communication regarding cyber threats is viewed as an organisational function of safety management, as it directly affects crew coordination, the implementation of security procedures, and the effectiveness of responses to cyber incidents.

Accordingly, this study adopts a preliminary exploratory and descriptive approach to examine the reported experiences and perceptions of seafarers concerning onboard cybersecurity. It focuses on the security measures and procedures encountered by respondents, their participation in training and simulations, their perceptions of crew preparedness and communication, and their views regarding the potential operational and economic consequences of cyber incidents.

The study addresses the following research questions: RQ1: What cybersecurity measures, procedures, and training practices do respondents report encountering on board their vessels? RQ2: How do respondents perceive crew preparedness, communication, and information-sharing practices concerning cyber threats? RQ3: How do respondents perceive the potential operational and economic consequences of cyber incidents, and what improvements do they recommend? The research questions are descriptive rather than hypothesis-testing. Accordingly, no hypotheses were formulated, and the study does not test causal relationships.

Data were collected through a structured questionnaire containing closed-ended items and one optional open-ended item. The questionnaire enabled a descriptive examination of respondents' reported experiences and perceptions, the identification of perceived challenges, and the formulation of preliminary recommendations. This research builds upon a previous analysis of seafarers' awareness of cyber threats (Pavlinović et al., 2022) and extends the focus to security protocols, cyber risk management procedures, crew operational preparedness, and the financial implications for shipping companies and the wider supply chain.

The structure of the paper is as follows. The next section reviews relevant literature on maritime cybersecurity, focusing on cyber risk management, the human fac-

tor, and organisational communication in the maritime environment. The methodology section outlines the research design and data collection conducted among seafarers. This is followed by the presentation and discussion of empirical findings related to crew preparedness, training, communication practices, and the economic implications of cyber incidents. The final section summarises the main conclusions and provides recommendations for improving cybersecurity preparedness and resilience in the maritime industry.

LITERATURE REVIEW

Cyber risk management has evolved from traditional information security, with a key transition towards an integrated approach emerging in the early 2000s, when security began to be perceived as a business risk rather than exclusively a technical problem (Blakley et al., 2001; Gordon et al., 2003). This concept was soon recognised in industry through standards such as ISO/IEC 27005:2008 and national frameworks such as the NIST Risk Management Framework, thereby establishing the foundations for systematic cyber risk management across various sectors, including maritime transport (NIST, 2024). This paradigm shift enabled a stronger integration of security considerations into strategic and financial planning processes. Today, cybersecurity is increasingly viewed as an integral component of overall business resilience, with losses caused by cyber-attacks—such as operational disruptions, contract losses, reputational damage, and increased insurance premiums—being quantified and incorporated into risk assessments (Eling et al., 2021; ENISA, 2022; Woods & Wolff, 2025).

The maritime industry recognised the seriousness of cyber threats relatively late; however, the past decade has seen accelerated development of regulatory and industry frameworks. A significant regulatory milestone occurred in 2017, when the International Maritime Organization (IMO) issued the *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3), emphasising the need to integrate cybersecurity into existing safety management systems (IMO, 2017a; IMO, 2017b), including clearly defined communication protocols and information exchange between shipboard crews and organisations. At the same time, industry guidelines jointly developed by BIMCO, ICS, INTERCARGO, and other organisations established the foundations for the operational implementation of protective measures at the ship level (BIMCO et al., 2020). In the context of technological transformation, organisational investments in digital technologies represent a key prerequisite for sustainable development, while the lack of such investments may limit a system's ability to respond to emerging security challenges (Spasojević & Đukić, 2025). These documents, incorporated into IMO Resolution MSC.428(98), require shipping companies to implement cyber risk management within their safety management systems by 2021 (DNV, 2020).

Although the regulatory and institutional framework has been significantly strengthened over the past decade, numerous studies indicate that the human factor remains one of the weakest links in maritime cybersecurity systems. A survey conducted among seafarers in 2017 revealed that as many as 84% of respondents had received no or only minimal cybersecurity training, while 64% believed they were responsible for the security of IT systems but did not know how to act in practice (Safety4Sea, 2017). These findings point to a substantial gap between technical expectations and the actual level of crew awareness and preparedness.

Contemporary approaches to cyber risk management increasingly emphasise the development of so-called *cyber hygiene*—a set of basic security habits and behaviours that every crew member must understand and apply in daily operations. In its recommendations on ship resilience to cyber threats, DNV (2016) highlights the importance of conducting simulation exercises, regular training, and developing simple and comprehensible incident response procedures. However, the implementation of such activities in practice encounters numerous obstacles, including limited shipboard internet connectivity, frequent crew rotation, language barriers, and differences in digital literacy levels (Chupkemi & Mersinas, 2024). Under conditions of limited onboard internet connectivity, the effective implementation of cyber measures requires a secure data-processing environment, with local processing of sensitive information representing a practical solution that supports both protection and analytical processing (Milojković et al., 2025). This suggests that individual crew awareness and motivation are not sufficient without systematic organisational support and an adequate regulatory and educational framework, highlighting the importance of closing the gap between individual preparedness and institutional support (Grujić & Novaković, 2025).

Recent research by Chupkemi and Mersinas (2024) identified 17 specific challenges in the implementation of cyber training in the maritime sector, with particular emphasis on the lack of time available for training during voyages, resistance to change, and the absence of standardised curricula. The authors also highlight the need to introduce a risk-based approach to training, whereby crew members are trained primarily to address threats that are most likely within their operational environment, including phishing attacks, the use of unauthorised USB devices, and responses to suspicious system changes.

Industry recommendations further stress the importance of continuous awareness enhancement through campaigns such as *Be Cyber Aware at Sea*, as well as the integration of cybersecurity elements into formal maritime education programmes (Safety4Sea, 2017). Some shipping companies have already introduced roles such as the Cyber Security Officer (CySO), both onboard and ashore, whose responsibilities include coordinating training activities, conducting preparedness assessments, and facilitating functional communication between technical staff and crew members (Moen et al., 2024).

In addition to international organisations such as the IMO and industry associations, the European Union Agency for Cybersecurity (ENISA) plays a significant role in shaping approaches to cyber risk management within the European context. In its *Guidelines for Cybersecurity in the Maritime Sector*, ENISA (2022) emphasises the importance of involving all stakeholders—from shipping companies and port authorities to IT service providers—in a comprehensive risk management process. Particular emphasis is placed on cyber risk management in ports, which represent critical nodes within the maritime logistics chain and are often interconnected with numerous vulnerable systems. ENISA recommends the establishment of unified security policies, the regular conduct of risk assessments, and the development of coordinated incident response mechanisms, in line with European regulatory frameworks such as the NIS Directive.

Despite these challenges, recent trends indicate a gradual institutionalisation of security culture within the maritime sector, whereby the crew is no longer viewed sole-

ly as a risk but rather as a key line of defence. Systematic investment in training and the raising of seafarers' awareness is increasingly recognised as a fundamental prerequisite for effective cyber risk management and for ensuring the resilience of maritime operations in the digital era.

Nevertheless, despite the development of regulatory and industry frameworks, the literature review reveals that a relatively small number of empirical studies focus on the operational preparedness of shipboard crews, particularly in the context of communication practices and perceptions of the economic consequences of cyber incidents. Most existing studies primarily address technical security aspects or regulatory requirements, while organisational and human factors are often examined in a fragmented manner. This paper seeks to contribute to closing this research gap through an empirical analysis of crew awareness, training, communication, and perceptions of the economic implications of cyber threats in the maritime sector.

METHODOLOGY

The study employed a cross-sectional, exploratory and descriptive survey design. Its purpose was to describe respondents' reported experiences and perceptions rather than to test hypotheses or causal relationships. Accordingly, the quantitative analysis was limited to descriptive statistics, including frequencies and percentages. Complete response distributions are reported for all closed-ended items as frequencies (n) and percentages (%), calculated using N = 77 as the denominator and presented to two decimal places. No inferential statistical tests were conducted. The units of analysis were the individual respondents and their self-reported answers. Questions concerning crew preparedness, communication effectiveness, company procedures, and onboard security measures were therefore interpreted as respondents' perceptions or reported experiences. They were not treated as objective verification of crew competence, company-level practices, or the actual implementation and effectiveness of cybersecurity controls on board.

The sampling frame consisted of active seafarers attending the Special Education Programme (SEP) at the Faculty of Maritime Studies, University of Split, during the 2023/24 and 2024/25 academic years. Convenience sampling was used, and all SEP attendees present when the questionnaire was administered were invited to participate voluntarily. Questionnaires were distributed and collected in paper form during the programme sessions. A total of 86 questionnaires were returned. Nine questionnaires were excluded because they contained incomplete responses that prevented their consistent inclusion in the analysis, resulting in a final analytical sample of 77 respondents. Thus, 89.5% of the returned questionnaires were retained for analysis. The number of attendees present and invited was not recorded separately from the number of returned questionnaires; consequently, a formal response rate cannot be calculated.

To reduce the possibility of repeated participation, the questionnaire was administered once within each programme group, and participants were instructed to complete it only once. However, because no personal identifiers were collected, possible participation by the same individual in both academic years could not be independently verified. Nationality, employer, vessel name, and exact collection dates were not recorded, as these variables were not required for the planned descriptive analysis. The respondents reported their professional position, work experience, and general vessel

type. The absence of nationality and employer information limits the possibility of assessing the organisational and national diversity of the sample.

SEP attendees were considered a relevant accessible group because they were active or professionally experienced seafarers undertaking continuing education aligned with the STCW Convention and could report on their recent shipboard experiences. Nevertheless, SEP attendees represent a specific subgroup of seafarers with access to continuing education and should not be considered representative of the maritime industry as a whole.

In line with the research goal and the themes identified in the literature review, the questionnaire consisted of a total of 25 questions, grouped into five thematic sections corresponding to the phases of risk management in the maritime environment:

- Demographic data (Q1–Q5): gender, age, work experience, position, type of vessel
- Technical and procedural measures (Q6–Q12): security measures, frequency of checks, recovery plans, threat detection
- Communication and awareness (Q13–Q17): training, simulations, information sharing, communication effectiveness, preparedness
- Monitoring, evaluation, and accountability (Q18–Q22): monitoring of measures, plan updates, incident analysis, recommendations
- Economic implications (Q23–Q25): perception of financial losses and operational disruptions, cost-effectiveness of investments in training, and assessment of the impact of cyber incidents on the financial stability and competitiveness of shipping companies.

The questionnaire primarily consisted of closed-ended questions with categorical response options. Selected attitude and perception items used Likert-type response scales, while Q22 was an open-ended question that allowed respondents to provide recommendations in their own words. The questionnaire was designed in the Croatian language. The English-language version presented in the paper was prepared by the authors for publication. The questionnaire assessed respondents' self-reported experiences, awareness, and perceptions of onboard cybersecurity. Q13 and Q16 assessed individual participation in simulations and training. Q15 and Q17 assessed perceived communication effectiveness and crew preparedness. Q6–Q12 and Q18–Q21 assessed respondents' awareness and perceptions of vessel- or company-level cybersecurity practices. Q23–Q25 assessed perceptions of potential operational and economic consequences. Accordingly, the questionnaire assessed how respondents experienced and understood cybersecurity practices rather than objectively testing their cybersecurity knowledge or independently verifying onboard controls and company-level practices.

The questionnaire consisted of standalone items addressing different topics and using different response formats. The items were analysed separately and were not combined into composite scores. A comparable literature-informed questionnaire containing different question formats and addressing several dimensions of maritime cybersecurity awareness was used by Moen et al. (2024). Questions Q1–Q5 were author-developed items used to collect respondents' demographic and professional characteristics. Questions Q6–Q12 were informed by the IMO Guidelines on Maritime Cyber Risk Management (IMO, 2017b), *The Guidelines on Cyber Security Onboard Ships* (BIMCO et al., 2020), and DNVGL-RP-0496 (DNV, 2016). Questions Q13–

Q17 were informed by BIMCO et al. (2020) and DNV (2016), while Q15 and Q17 were author-developed items measuring respondents' perceptions of communication effectiveness and crew preparedness, respectively. Questions Q18–Q21 were informed by IMO Resolution MSC.428(98) (IMO, 2017a), the IMO Guidelines on Maritime Cyber Risk Management (IMO, 2017b), BIMCO et al. (2020), and DNV (2016). Q22 was an optional open-ended item that allowed respondents to provide supplementary recommendations. The responses were used only to contextualise the descriptive findings and were not subjected to formal thematic coding, following a comparable treatment of supplementary open-text responses in maritime cybersecurity research (see Kurt et al., 2026). Questions Q23–Q25 were author-developed perception items informed by BIMCO et al. (2020), Gordon et al. (2003), and ENISA (2022).

Before administration, the draft questionnaire was informally reviewed by academic colleagues familiar with maritime education and cybersecurity-related topics. They considered the relevance, clarity, and comprehensibility of the questions. The questionnaire and response options were also informally checked with individuals comparable to the intended respondents, who confirmed that they were understandable. This informal review was used to improve the clarity and content relevance of the questionnaire.

Participation in the survey was voluntary and anonymous, and no personal identifying data were collected. The study adhered to the ethical principles of academic research.

RESULTS

The results are presented in accordance with the three descriptive research questions. All findings refer exclusively to the answers provided by the respondents included in the study. References to onboard measures, procedures, communication, preparedness, and economic consequences therefore describe respondents' reported experiences and perceptions and should not be interpreted as independently verified conditions. There were no missing responses to the closed-ended items in the final analytical sample. According to the gender structure, all respondents (100%) were male. The sample included an almost equal proportion of respondents aged 31–40 years (31.17%) and 18–30 years (38.96%), while respondents aged 41–50 years accounted for 29.87% of the sample. With regard to maritime work experience, the largest proportion of respondents had up to 5 years of experience (38.96%), followed by those with 6–10 years (31.17%) and 11–20 years of experience (29.87%).

The most frequently reported position on board was deck officer (44.16%), followed by engine officer (33.77%) and crew member (20.78%), while only one respondent indicated that they currently held the position of captain. In terms of the type of vessel on which respondents were currently employed, the largest proportion worked on tankers (38.96%), followed by cargo ships (31.17%) and passenger vessels (28.57%), while one respondent reported another type of vessel.

Table 1. Demographic characteristics of respondents (N = 77)

Demographic characteristics	Category	Frequency	%
Gender	Male	77	100.00
	Female	0	0.00
Age	18–30	30	38.96
	31–40	24	31.17
	41–50	23	29.87
Experience	0–5	30	38.96
	6–10	24	31.17
	11–20	23	29.87
Position	Deck officer	34	44.16
	Engine officer	26	33.77
	Crew member	16	20.78
	Captain	1	1.30
Type of vessel	Cargo ship	24	31.17
	Passenger ship	22	28.57
	Tanker	30	38.96
	Other:_____	1	1.30

Source: Authors

After examining the demographic characteristics of the sample, Table 2 presents respondents' reports of technical and procedural cybersecurity measures on the vessels to which their answers referred. Antivirus protection was the most frequently reported measure, while respondents most commonly reported that system security checks were conducted every few months. Forty-four respondents (57.14%) reported that incident-reporting procedures were available to all crew members, whereas 33 respondents (42.86%) reported that threat-detection systems were not used. Furthermore, 43 respondents (55.84%) reported that the most recent cyber-risk assessment had been conducted within the previous six months. However, 53 respondents (68.83%) did not know whether a cyber-incident recovery plan existed. This indicates uncertainty or limited respondent awareness and should not be interpreted as evidence that recovery plans were absent.

Table 2. Technical and procedural cybersecurity measures (Q6-Q12; N = 77)

Question (code)	Short question	Response category	n	%
Q6	Implemented security measures	Antivirus	75	97.40
		Firewall	48	62.34
		Access control	37	48.05
		Data backup	29	37.66
		Encryption	18	23.38
		Other security measures	5	6.49
		None	1	1.30

Q7	Frequency of system security checks	Weekly or more frequently	9	11.69
		Monthly	18	23.38
		Every few months	41	53.25
		Once a year or less frequently	6	7.79
		Never	3	3.90
Q8	Existence of incident-reporting procedures	Yes, for all crew members	44	57.14
		Yes, but only for designated personnel	18	23.38
		No	9	11.69
		I do not know	6	7.79
Q9	Use of threat-detection systems	Yes	25	32.47
		No	33	42.86
		I do not know	19	24.68
Q10	Perceived level of cyberattack risk	Very high	8	10.39
		High	30	38.96
		Moderate	27	35.06
		Low	10	12.99
		Very low	2	2.60
Q11	Timing of the most recent cyber-risk assessment	Within the past six months	43	55.84
		Between six and twelve months ago	15	19.48
		More than one year ago	8	10.39
		No assessment has been conducted	4	5.19
		I do not know	7	9.09
Q12	Existence of a cyber-incident recovery plan	Yes	15	19.48
		No	9	11.69
		I do not know	53	68.83

Source: Authors (note: Q6 was a multiple-response item; therefore, its percentages may sum to more than 100%.)

As effective cybersecurity management does not rely solely on technical solutions, Table 3 presents respondents' reports related to crew communication and training, including simulations, information sharing, and perceived preparedness. Thirty-two respondents (41.56%) reported never having participated in cyber-incident recovery simulations; however, this finding should not by itself be interpreted as evidence of limited practical crew preparedness. Official notices were the most frequently reported method of sharing threat-related information (n = 32; 41.56%), while 42 respondents (54.55%) perceived threat-related communication as effective. A total of 61 respondents (79.22%) reported having participated in formal cybersecurity training at least once. Furthermore, 46 respondents (59.74%) perceived the crew as only partially prepared to address cyber threats.

Table 3. Communication practices and cybersecurity training (Q13-Q17; N = 77)

Question (code)	Short question	Response category	n	%
Q13	Participation in recovery simulations	No, never	32	41.56
		Yes, once	27	35.06
		Yes, more than once	18	23.38
Q14	Method of sharing threat-related information	Through official notices	32	41.56
		During organised meetings or briefings	18	23.38
		By email or another digital platform	15	19.48
		Through informal communication	8	10.39
		Information is not regularly shared	4	5.19
Q15	Effectiveness of threat-related communication	Very effective	12	15.58
		Effective	42	54.55
		Neither effective nor ineffective	13	16.88
		Ineffective	8	10.39
		Very ineffective	2	2.60
Q16	Participation in formal cybersecurity training	Yes, once	40	51.95
		Yes, more than once	21	27.27
		No, never	16	20.78
Q17	Perceived crew preparedness for cyber threats	Fully prepared	15	19.48
		Partially prepared	46	59.74
		Not prepared	13	16.88
		I do not know	3	3.90

Source: Authors

Table 4 presents respondents' reports concerning the monitoring of cybersecurity measures, incident analyses, security-plan updates, and responsibility for the security plan. Periodic checks were the most frequently reported method of monitoring security measures, while 30 respondents (38.96%) identified an IT specialist as the person responsible for the security plan.

Table 4. Monitoring, updating, and accountability in cybersecurity implementation (Q18-Q21; N = 77)

Question (code)	Short question	Response category	n	%
Q18	Monitoring the effectiveness of security measures	Periodic checks	34	44.16
		Continuous monitoring	20	25.97
		Checks following an incident	13	16.88
		No monitoring	6	7.79
		I do not know	4	5.19
Q19	Frequency of incident analysis	After every incident	22	28.57
		Every three months	9	11.69

		Every six months	28	36.36
		Once a year	13	16.88
		Never/I do not know	5	6.49
Q20	Frequency of security-plan updates	After a cybersecurity incident	8	10.39
		Every three months	27	35.06
		Every six months	23	29.87
		Once a year	14	18.18
		Never/I do not know	5	6.49
Q21	Person responsible for the security plan	IT specialist	30	38.96
		Captain	18	23.38
		Company cybersecurity officer	14	18.18
		Designated crew member	9	11.69
		Shore-based manager	4	5.19
		I do not know	2	2.60

Source: Authors

Respondents were given an opportunity to provide additional recommendations in an optional open-text format (Q22). Their comments referred to clearer cybersecurity protocols, improved information sharing, more frequent security checks and incident simulations, additional crew training, and clearer allocation of responsibilities. For example, one respondent recommended clearer procedures, regular crew training, and more frequent onboard security checks. These comments are presented as supplementary contextual observations rather than formally coded qualitative findings, following the approach used by Kurt et al. (2026).

Table 5. Respondents' perceptions of the economic implications of cybersecurity (Q23-Q25; N = 77)

Question (code)	Short question	Response category	n	%
Q23	Financial losses and operational disruptions for the shipping company	Strongly agree	40	51.95
		Agree	24	31.17
		Neither agree nor disagree	8	10.39
		Disagree	4	5.19
		Strongly disagree	1	1.30
Q24	Cost-effectiveness of investments in crew training	Yes	65	84.42
		No	8	10.39
		I do not know	4	5.19
Q25	Long-term impact on financial stability and competitiveness	Poses a significant threat to financial stability and competitiveness	44	57.14
		Poses a moderate threat	22	28.57
		Poses a limited threat	7	9.09
		Has no significant impact	2	2.60
		I do not know	2	2.60

Source: Authors

Table 5 presents respondents' perceptions of the potential economic implications of cyber incidents. Forty respondents (51.95%) strongly agreed that insufficient crew preparedness and inadequate protective measures could result in financial losses and operational disruptions. Sixty-five respondents (84.42%) perceived investment in crew training as cost-effective, while 44 respondents (57.14%) perceived a cyber incident as a significant long-term threat to a company's financial stability and competitiveness. These findings describe respondents' perceptions and do not demonstrate actual financial losses or the cost-effectiveness of cybersecurity investments.

DISCUSSION

The responses obtained from 77 seafarers suggest possible gaps in respondents' awareness of and exposure to certain onboard cybersecurity procedures, despite the existence of formal IMO and industry guidelines (IMO, 2017a; IMO, 2017b; DNV, 2020). For example, 75 respondents (97.40%) reported that antivirus protection was used on the vessels to which their responses referred, indicating that this was the most commonly reported basic technical measure (Table 2). However, 53 respondents (68.83%) selected "I do not know" when asked whether a recovery plan existed (Q12), while 33 respondents (42.86%) reported that threat-detection systems were not used (Q9). The responses to Q12 indicate uncertainty or limited awareness and should not be interpreted as evidence that recovery plans were absent.

Similar findings have been reported in previous studies, which identify a gap between the existence of technical measures and their operational effectiveness, particularly with regard to crew awareness and training (Safety4Sea, 2017; Chupkemi & Mersinas, 2024). For instance, although 61 respondents (79.22%) reported having participated in formal cybersecurity training at least once (Q16), 46 respondents (59.74%) perceived the crew as only partially prepared (Q17). This is consistent with DNV's (2016) emphasis on continuous practical application, simulations, and exercises as important components of shipboard cyber resilience.

Thirty-two respondents (41.56%) reported never having participated in recovery simulations (Q13), which contrasts with industry recommendations that identify simulation-based exercises as an important component of cyber hygiene (DNV, 2016; BIMCO et al., 2020). Furthermore, 44 respondents (57.14%) reported that incident-reporting procedures were available to all crew members (Q8), while 28 respondents (36.36%) reported that incident analyses were conducted every six months (Q19). These responses may indicate uneven respondent awareness of and exposure to operational cybersecurity procedures but do not verify their actual implementation or effectiveness on board.

The supplementary comments to Q22 referred to clearer protocols, more frequent checks, improved communication, and additional training, which is consistent with ENISA's recommendations (2022). Because the responses were not formally coded, the prevalence of these recommendations within the sample cannot be established. At the same time, 30 respondents (38.96%) identified an IT specialist as the person responsible for the security plan, which may reflect a perceived emphasis on technical responsibility for cybersecurity.

An additional dimension concerns respondents' perceptions of the potential economic implications of insufficient cybersecurity preparedness. Forty respondents

(51.95%) strongly agreed that insufficient awareness and training could result in financial losses and operational disruptions. Sixty-five respondents (84.42%) perceived investments in crew training as economically justified, while 44 respondents (57.14%) perceived a successful cyberattack as a significant long-term threat to a shipping company's financial stability and competitiveness. These findings indicate that respondents perceived cybersecurity as both a technical concern and a potential business risk.

Recent research increasingly highlights the need to apply a risk-based approach to training, whereby education should be focused on the most likely scenarios, such as phishing attacks, unauthorised use of devices, or responses to suspicious system changes (Chupkemi & Mersinas, 2024). Within the present sample, 32 respondents (41.56%) reported official notices as the method of communicating information about cyber threats, while 42 respondents (54.55%) perceived threat-related communication as effective. These responses describe respondents' reported experiences and do not verify the consistency or effectiveness of company-level information-sharing practices.

Given that the study sample is entirely male, the findings do not capture potentially different experiences and perceptions among women seafarers, which provides scope for future research on the gender dimension of cybersecurity in the maritime sector. In addition, most respondents are between 18 and 40 years of age, while most reported less than 10 years of maritime experience (Table 1). This age and experience profile limits the applicability of the findings to older and more experienced seafarers. Previous research has identified professional experience and individual characteristics as potentially relevant to cybersecurity awareness and preparedness (Chupkemi & Mersinas, 2024; Moen et al., 2024), however, their relationship with respondents' answers was not tested in the present study.

When interpreting these findings, certain methodological limitations of the study should also be taken into account. The study used a convenience sample of SEP attendees recruited from a single Croatian institution. Participation in continuing education may be associated with motivation, career stage, certification requirements, employer support, or access to training, creating a risk of selection and self-selection bias. Nationality and employer information were not collected, a formal response rate could not be calculated, and possible repeated participation across the two academic years could not be independently verified because the questionnaires were anonymous. Consequently, the results provide preliminary insight into the reported experiences and perceptions of the surveyed respondents but should not be generalised to the Croatian or international maritime industry.

Overall, respondents frequently reported encountering basic elements of cybersecurity protection, while their answers suggest possible gaps in awareness of and exposure to training, operational procedures, and the allocation of cybersecurity responsibilities. These findings reflect the perceptions and reported experiences of the surveyed sample rather than verified conditions across the maritime sector. As emphasised by ENISA (2022), strengthening resilience requires not only technical measures but also the development of a security culture at all levels in which the crew is recognised as an important component of cybersecurity resilience.

CONCLUSION

This research highlights respondents' perceptions of the importance of the human factor as a key element of cybersecurity management systems in the maritime industry, particularly in the context of shipboard crew preparedness for cyber threats. Despite formal regulatory requirements and industry guidelines, the results suggest possible gaps in respondents' awareness of and exposure to their operational implementation at the ship level, particularly in the areas of continuous training, the conduct of simulations, and the practical application of security procedures. Empirical data obtained through the survey show that respondents frequently reported encountering basic technical security measures on-board, while their responses indicate less consistent awareness of or exposure to more advanced elements of cyber resilience, such as recovery plans, threat detection systems, and regular incident simulations. These findings suggest a perceived need for stronger institutional and organisational support in building a security culture, in which education and digital literacy should be integrated into everyday shipboard operations rather than limited to occasional or purely formal forms of training. The findings further suggest that respondents perceive cybersecurity as both a technical and an economic concern. The majority of respondents perceive an association between the level of cybersecurity protection, operational stability, and the financial health of shipping companies. Cyber incidents may lead to business disruptions, revenue losses, increased recovery costs, higher insurance premiums, and long-term deterioration of competitiveness, although these effects were not directly measured in this study. Respondents' answers indicate that they generally perceive investments in preventive measures and crew training as economically justified; however, the study does not establish their actual cost-effectiveness. Based on respondents' answers, the following preliminary, sample-specific recommendations can be proposed: (1) the introduction of more frequent cyber incident simulation exercises as an integral part of safety management, (2) the development of tailored digital training modules for continuous seafarer education, focused on the most common and high-risk attack scenarios, and (3) the improvement of accessibility to security-related information and incident response plans at the level of shipping companies, accompanied by a clear allocation of responsibilities between technical personnel and crew members. The potential operational and economic effects of these proposed measures were not tested in the present study and should be examined in future research. In this context, investments in crew training and cybersecurity capabilities were perceived by respondents as potentially valuable long-term investments. Given the exploratory design, convenience sampling, all-male sample, recruitment from a single institution, and reliance on self-reported data, the findings should be regarded as preliminary and should not be generalised to the maritime industry as a whole. Future research should further examine the economic effects of such investments, as well as the effectiveness of different training and communication approaches under real operational conditions.

Acknowledgement: *This research is the result of the project SIDRO- Stakeholder synergy for the development of a sustainable entrepreneurial society, funded by the European Union- NextGenerationEU. The views and opinions expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.*

LITERATURE

BIMCO, Chamber of Shipping of America, Digital Container Shipping Association, INTERCARGO, InterManager, INTERTANKO, International Chamber of Shipping, International Union of Marine Insurance, Oil Companies International Marine Forum, Superyacht Builders Association, & World Shipping Council. (2020). *The guidelines on cyber security onboard ships (Version 4).* https://www.bimco.org/media/oq0ft0gr/guidelines-on-cyber-security-onboard-ships-v4-1.pdf

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In: *Proceedings of the 2001 Workshop on New Security Paradigms*. ACM: 97–104. https://doi.org/10.1145/508171.508187

Car, T., Pilepić, Lj., & Šimunić, M. (2014). Mobile technologies and supply chain management – Lessons for the hospitality industry. *Tourism and Hospitality Management*, 20(2): 207–219. https://doi.org/10.20867/thm.20.2.5

Chupkemi, D. C., & Mersinas, K. (2024). Challenges in maritime cybersecurity training and compliance. *Journal of Marine Science and Engineering*, 12(10): 1844. https://doi.org/10.3390/jmse12101844

DNV. (2020). *ISM cyber security is coming soon – check your preparedness.* available at: https://www.dnv.com/news/2020/ism-cyber-security-is-coming-soon-check-your-preparedness-186252/

DNV GL. (2016). *Cyber security resilience management for ships and mobile offshore units in operation* (DNVGL-RP-0496).

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review, 24*(1), 93–125. https://doi.org/10.1111/rmir.12169

European Union Agency for Cybersecurity. (2022). *ENISA threat landscape 2022: July 2021 to July 2022*. https://doi.org/10.2824/764318

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3): 81–85. https://doi.org/10.1145/636772.636774

Grujić, M., & Novaković, V. (2025). The impact of artificial intelligence on the accounting profession in Bosnia and Herzegovina: Perceptions, readiness and regulatory gap. *Economy and Market Communication Review*, 15(2). DOI:10.7251/EMC2502296G

International Maritime Organization. (2017a). *Maritime cyber risk management in safety management systems* (Resolution MSC.428(98)). https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Documents/RESOLUTION%20MSC.428%20-98%20-.pdf

International Maritime Organization. (2017b). *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3). https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3.pdf

Kurt, Y. B., Black, H., Uflaz, E., Kurt, R. E., & Turan, O. (2026). A quantitative assessment of human factors in maritime cybersecurity: An investigation of seafarers' knowledge and practices. *Journal of Cybersecurity*, 12(1): 1-15. https://doi.org/10.1093/cybsec/tyag015

Milojković, S., Kljajić, Ž., & Dakić, P. (2025). Z score and Valido AI: An explainable AI framework for payroll analytics with statistical anomaly detection in Serbian small and medium enterprises. *Economy and Market Communication Review*, 15(2): 379–396. https://doi.org/ 10.7251/EMC2502379M

Moen, I., Oruc, A., Amro, A., Gkioulos, V., & Kavallieratos, G. (2024). Survey-based analysis of cybersecurity awareness of Turkish seafarers. *International Journal of Information Security*, 23(3): 3153–3178. https://doi.org/10.1007/s10207-024-00884-2

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework*

(CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Pavlinović, M., Račić, M., & Karin, I. (2022). Cyber risks in maritime industry – Case study of Croatian seafarers. In: *Human interaction, emerging technologies and future systems V*, Ahram, T., Taiar, R. (ur.). Lecture Notes in Networks and Systems, Vol. 319. Cham: Springer. DOI:10.1007/978-3-030-85540-6_14

Safety4Sea. (2017). *Survey finds lack of maritime cyber security training amongst crews*. SAFETY4SEA. https://safety4sea.com/survey-finds-lack-of-maritime-cyber-security-training-amongst-crews/

Spasojević, B., & Đukić, A. (2025). Investicije u umjetnu inteligenciju kao pokretač održivog razvoja malih i srednjih preduzeća u Bosni i Hercegovini. *Economy and Market Communication Review*, 15(2): 346–359. https://doi.org/10.7251/EMC2502346S

Standard Club. (2020). *Cyber risks – Smart guide.* London: Standard P&I Club.

Woods, D. W., & Wolff, J. (2025). A history of cyber risk transfer. *Journal of Cybersecurity, 11*(1), tyae028. https://doi.org/10.1093/cybsec/tyae028