Journal of Naval Sciences and Engineering
2024, Vol. 20, No. 2, pp. 135-162 *DOI: 10.56850/jnse.1485985*
Electrical-Electronics Engineering/Elektrik-Elektronik Mühendisliği

RESEARCH ARTICLE

** This study was conducted in accordance with ethics committee procedures of human experiments. To apply the scale to maritime workers, Piri Reis University, Istanbul, Türkiye Ethics Committee approval was received with the code number 2023/9.*

DEVELOPING A MEASUREMENT SCALE TO ASSESS THE PERCEPTION OF CYBERSECURITY AMONG EMPLOYEES IN THE MARITIME INDUSTRY

Cihat AŞAN[1]

[1]Piri Reis University, Maritime Faculty, Department of Maritime Transportation and Management Engineering, İstanbul, Türkiye, casan@pirireis.edu.tr

Received: 17.05.2024 **Accepted: 16.09.2024**

ABSTRACT

The emergence of Industry 4.0, within the historical context of industrial revolutions shaped by human needs, signifies a rapid integration of technology into society. Despite societal concerns about technology displacing human labor, cybersecurity is a significant challenge associated with Industry 4.0. This study aims to create a "5-point Likert Scale" to assess the conceptual awareness of cybersecurity among maritime transportation sector employees. The "Cybersecurity Awareness Scale" consists of 43 queries and is subjected to rigorous validity and reliability analyses. Administered to 200 individuals in Istanbul, Türkiye, the scale revealed varying awareness levels, with information technology personnel showing high awareness and others exhibiting comparatively lower awareness, both organizationally and regarding individual security vulnerabilities. This scale contributes significantly to evaluating companies' cybersecurity awareness, aiding them in identifying strengths and weaknesses and implementing necessary measures. Future research can deepen theoretical discussions by utilizing the scale to uncover regional and sectoral differences in cybersecurity awareness. Recommendations include larger sample sizes for subsequent studies, enabling comprehensive comparisons and enriching the literature on this subject.

Keywords: *Maritime workers, Cyberattack, Survey, Security awareness.*

DENİZCİLİK SEKTÖRÜ ÇALIŞANLARI ARASINDA SİBER GÜVENLİK ALGISININ DEĞERLENDİRİLMESİ İÇİN BİR ÖLÇÜM ÖLÇEĞİ GELİŞTİRİLMESİ

ÖZ

Endüstri 4.0'ın ortaya çıkışı, insan ihtiyaçları tarafından şekillendirilen sanayi devrimlerinin tarihsel süreci içinde, teknolojinin topluma hızlı entegrasyonunu simgelemektedir. Teknolojinin insan işgücü istihdamını azaltacağı yönündeki endişelerle birlikte, siber güvenlik Endüstri 4.0'ın beraberinde getirdiği bir diğer sorun olarak karşımıza çıkmaktadır. Bu çalışma, denizcilik taşımacılığı sektörü çalışanlarının siber güvenlik farkındalığını ölçmek için bir ölçek oluşturmayı ve bunu İstanbul, Türkiye bölgesi örnek alınarak uygulamayı amaçlamaktadır. "Siber Güvenlik Farkındalık Ölçeği" 43 sorudan oluşmakta olup, kapsamlı geçerlilik ve güvenilirlik analizlerine tabi tutulmuştur. İstanbul, bölgesinde 200 denizcilik endüstrisi çalışanına uygulanan ölçek, bilgi teknolojisi personelinin yüksek farkındalığa sahip olduğunu, diğerlerinin ise hem kurumsal hem de bireysel güvenlik açısından nispeten daha düşük farkındalık sergilediğini ortaya çıkarmıştır. Bu ölçek, denizcilik şirketleri açısından çalışanlarının siber güvenlik farkındalığını değerlendirmede önemli bir katkı sağlayacak olup, güçlü ve zayıf yönlerini belirlemelerine ve gerekli önlemleri almalarına yardımcı olacaktır. Müteakiben yapılacak araştırmalarda bu ölçek kullanılarak farklı bölgeler ve sektörlerdeki siber güvenlik farkındalığı ölçülebilir ve karşılaştırma yapılarak farklılıklar ortaya çıkartılabilir.

Anahtar Kelimeler: *Denizcilik çalışanları, Siber saldırı, Anket tarama, Durumsal farkındalık.*

1. INTRODUCTION

Technological advancements in the maritime sector, while fostering growth opportunities, have also increased vulnerability to cyber-attacks (Fitton et al., 2015). The escalating cyber threats raise concerns about potential disruptions to critical infrastructure in the future (Bielawski and Lazarowska, 2021). Cybercrime poses a significant threat to maritime industries, with recent security breaches highlighting risks to human welfare, the environment, and financial losses for shipping companies. This compromise led to the unauthorized acquisition of sensitive information, causing the company's share value to immediately decline by 5%

(Nguyen, 2018; Kapalidis, 2020). In June 2017, A.P. Moller-Maersk experienced a cyber incident involving 'NotPetya' malware, causing global disruption and affecting the company's terminal in Ukraine (Parizo, 2019; Progoulakis et al., 2021). The virus affected up to 76 of the company's port facilities worldwide, including critical locations such as Rotterdam, Los Angeles, Mumbai, and Auckland (Mcquade, 2018; Nguyen, 2018). Thus, the maritime transport industry presents a significant cybersecurity risk, often with a low level of awareness in this area.

Human involvement in cybersecurity is crucial, especially in industries like maritime transportation, where accidents are common due to lack of knowledge and adherence to safe practices (Hasanspahić et al., 2021; S. de Vleeschhouwer, 2017). Increasing cybersecurity awareness is vital in the maritime industry, where human error is significant. This study aimed to measure cybersecurity awareness using a 5-point Likert-type scale developed from 500 questions, with input from experts. Validity and reliability were assessed, and the scale was used in Istanbul, Türkiye, with a large maritime workforce to gauge cybersecurity awareness. Suggestions were made based on the analysis to enhance awareness.

The literature on maritime transportation and cyber security highlights the critical role of the maritime sector in global trade and its increasing reliance on technology. When reviewing the literature focused on studies examining the role of the human factor in cybersecurity, Tuomala (2021) offers guidelines for maritime employees, focusing on cyber-attack awareness, role definitions, and cybersecurity understanding. The study addresses preventive measures for cybersecurity risks, including regulatory compliance, privacy attacks, vessel specifics, and operational technology security. Kanwal et al. (2022) studied factors affecting cybersecurity performance in the maritime sector, identifying six key dimensions: regulations, company procedures, shipboard systems readiness, training and awareness, human factors, and compliance monitoring. Perez (2019) created an online survey to explore how cyber curiosity and situational awareness relate to cyber risk in organizations. Data analysis aimed to find differences in Cyber Situational Awareness and Cyber Curiosity levels between maritime and shoreside IT users. Mraković and Vojinović (2019) address key cybersecurity challenges in the maritime industry and offer recommendations to tackle them. The study highlights the crucial role of awareness at all levels of the business. Larsen and Lund (2021) examined cyber risk perception in the maritime sector using psychological models. They studied key dimensions and cognitive biases, including the nine dimensions of the psychometric model, such as perceived benefit and optimistic bias, within maritime operations. Bolat and Kayışoğlu (2019) investigated cybersecurity awareness in the Turkish Maritime Sector using Structural Equation Modeling. Their study highlights education's role in enhancing cybersecurity awareness and links cybersecurity incidents to awareness and behavior. Tam and Jones (2019) propose a model-based risk assessment framework to tackle the increasing hacker awareness of cyber vulnerabilities in the maritime sector. Nwankpa and Datta (2023) investigate how working remotely may result in a moral hazard for employees regarding their understanding of cybersecurity and their behavior regarding security-based precautions. Hong et. al. (2023) introduced an expanded knowledge-attitude-behavior (KAB) model that suggests the education level of society as a whole acts as a moderator in the connection between knowledge and attitude. With an emphasis on small and medium-sized enterprises (SMEs), Chaudhary et al. (2023) carried out a thorough analysis of the literature on cybersecurity awareness. To guide future research and tailor cybersecurity awareness to SMEs' requirements, their study seeks to identify knowledge and research gaps in the sector for SMEs. Karaca and Söner (2023) used a questionnaire with three attitude scores to look at the cybersecurity awareness of maritime students. Their study offers recommendations for raising students’ cybersecurity knowledge in light of its findings. Tolossa (2023) emphasizes the importance of cybersecurity awareness training for businesses to protect their networks and maintain customer trust, highlighting the need for a comprehensive security plan incorporating policy and technology controls. Chaudhary (2024) identified seven attributes that can positively influence employees' cybersecurity behaviors, using a literature review and Delphi method with 22 experts, and subsequently employing a questionnaire design. Abrahams et.al. (2024)’s study explores cybersecurity awareness and education programs, focusing on employee engagement and accountability. It examines various methodologies, including interactive workshops, simulated phishing exercises, online modules, and gamified learning platforms. With an emphasis on psychological, behavioral, and sociocultural elements, Sangwan (2024) investigated the human side of cybersecurity awareness. The study looks at involvement, cost limitations, and cybersecurity awareness initiatives' benefits and drawbacks.

The literature emphasizes the importance of cybersecurity in maritime transportation, highlighting the human element's role in cyber risks. A study is needed to measure cybersecurity awareness among maritime employees.

This scale makes a substantial contribution to the evaluation of the cybersecurity awareness of firms, which assists these organizations in determining their strengths and weaknesses and in putting into action the necessary steps. Through the utilization of the scale, future research has the potential to delve deeper into theoretical discussions by revealing regional and sectoral variances in cybersecurity awareness. In the recommendations, higher sample sizes for forthcoming studies are suggested. This would make it possible to conduct extensive comparisons and would improve the existing body of literature on this topic.

2. METHODOLOGY

This study introduces a scale for measuring cybersecurity awareness in the maritime transportation sector, using a Likert-type scale for easy use and statistical analysis. Initially, a 43-item draft scale was prepared by experts brainstorming from a pool of items. Expert opinions were consulted for the draft scale with a 480-item pool to determine the content validity of the Cyber Security Awareness Scale. Based on the opinions of the experts on the scale items the application scale with 43 items was obtained. Data was collected via Google Forms from a population in the maritime domain in Istanbul, Türkiye, with a sample size of 200 participants. The scale, consisting of 43 items, is provided in the Annex. The research addresses the increasing threat of cyber-attacks to businesses, highlighting financial losses and reputation damage. The scale focuses on maritime industry employees, with 33 items measuring personal cybersecurity awareness and 10 items assessing Cyber Security Awareness of Information Technology (IT) and Management staff.

Initially, descriptive analysis used the Mann-Whitney U test for gender and the Kruskal Wallis-H test for age and education level. Kruskal Wallis H test is a technique used to test the significance of the difference between the means of three or more groups in groups that do not show normal distribution. Kruskal Wallis H test was used because the age groups and education level groups of the sample participants were 3 or more. Mann-Whitney U test is a non-parametric test that is an alternative to an independent sample test. This test is used to look at the mean difference between two independent groups from similar populations and to determine the difference or equality between the groups. Mann-Whitney U test was used because it was performed on 2 different gender groups, women and men. The scale's reliability and validity were then tested using Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) with SPSS (Version 26) and AMOS software. As the scale did not have predetermined factors, Principal Component Analysis (PCA) was conducted to extract dimensions, followed by CFA to model the scale. After confirming the scale's reliability and validity, it was administered to the 200 participants. Approval from the Piri Reis University Ethics Committee in Istanbul, Türkiye, was obtained under code number 2023/9 to use the scale in maritime workers.

The findings of this study enable guidance to maritime businesses in developing strategies against cyber threats and improving their overall cybersecurity practices.

3. RESULTS and DISCUSSION

In this section, statistical analyses and tests of the collected data were conducted, and the results were interpreted. Initially, the distribution of the 200 participants has been presented in Table 1 based on their genders, age range, and education level respectively.

Table 1. *Gender, Age Group, and Education Level Distribution of Participants.*

Gender	Age Group	Education Level	
21% Woman	%24 (20-30)	%6 Elementary School	%17 High School
79% Man	%52 (31-45)	%56 Graduate	%21 Post Graduate
	%25 (45+)		

3.1. Descriptive Statistics

For initial tests to evaluate the acquired data, as stated in Table 1, the Mann-Whitney U test is applied for the genders, and the Kruskal Wallis-H test is utilized regarding participants' age and education level as given in Figures 1, 2, and 3.

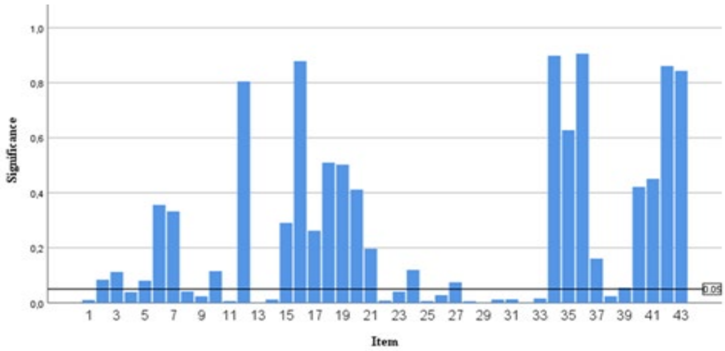

Figure 1. *Mann Whitney U Test Results for Gender.*

As per the Mann Whitney U test, there were notable differences ($p<0.05$) in items M1, M4, M8, M9, M11, M13, M14, M22, M23, M25, M26, M28, M29, M30, M31, M32, M33, and M38 between the two gender categories. However, the remaining 25 items did not exhibit significant differences. Out of the 18 items analyzed, responses varied between genders, while for the remaining items, both genders held similar perspectives on the concepts.

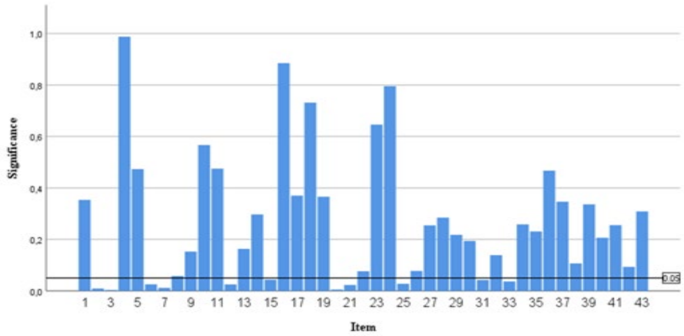

Figure 2. *Kruskal-Wallis Test Results for Education Level.*

According to the results of the Kruskal-Wallis Test regarding educational back-grounds, significant differences ($p<0.05$) were identified in items M2, M3, M6, M7, M12, M15, M20, M21, M25, M31, M33, and M38. However, the remaining 30 items did not show significant variations across the various educational levels. For the majority of items, educational backgrounds did not provide distinct insights.

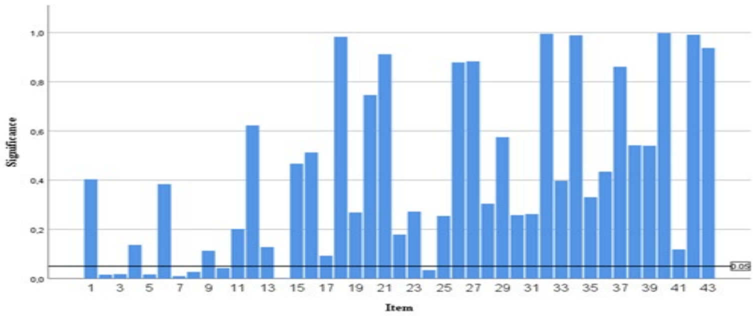

Figure 3. *Kruskal-Wallis Test Results for Age.*

According to the results of the Kruskal-Wallis Test across different age categories, significant differences (p<0.05) were noted in items M2, M3, M5, M7, M8, M10, M14, M24, and M38. Conversely, the remaining 34 items did not demonstrate notable distinctions within the specified age ranges. This implies that, when evaluated across various age groups, 34 items in the scale lack consistency.

3.2. Reliability and Validity Tests

The reliability of a scale is assessed through item analysis using item-total correlation, and Cronbach's Alpha (Cα) values are computed for each item, as detailed in the Annex. Within this framework, values within the 0.80 ≤ Cα < 1.00 range signify a notable degree of reliability for the scale (Nunnally, 1978), (Mehdiyev et al., 2017). For the proposed Cybersecurity Awareness Scale, the total Cα value is found as 0.921 among 43 items, as stated in Table 2.

Table 2. *Reliability Statistics.*

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	Number of Items
0,921	0,919	43

Table 3 presents the initial item-total statistics, providing Scale Mean, Scale Variance, Corrected Item-Total Correlation, and Cα values for each item to facilitate the initial reliability analysis. To comprehensively assess the reliability, it is essential to grasp the contribution of each item to the scale's reliability. Consequently, items with low item-total correlation values, falling below the threshold of 0.2, have been considered to be excluded to enhance the overall scale reliability.

Table 3. *Initial Item-Total Statistics.*

A: **Items, B: Initial Scale Mean, C: Initial Scale Variance, D: Initial Corrected Item-Total Correlation, E: Initial Cα**

A	B	C	D	E	A	B	C	D	E
M1	162,61	719,920	,634	,940	**M23**	162,86	741,480	,389	,942
M2	161,54	763,288	**,295**	,943	**M24**	163,40	744,495	,334	,943
M3	161,53	763,397	**,244**	,943	**M25**	162,79	718,883	,713	,940
M4	162,18	743,647	,431	,942	**M26**	162,67	726,369	,683	,940
M5	161,91	753,653	,452	,942	**M27**	162,49	719,076	,707	,940
M6	161,58	759,605	,319	,942	**M28**	162,54	709,253	,826	,939
M7	163,05	744,158	,316	,943	**M29**	162,54	711,467	,787	,939
M8	162,88	731,860	,508	,941	**M30**	162,58	710,891	,777	,939
M9	162,74	735,447	,461	,942	**M31**	162,58	711,605	,753	,939
M10	162,04	752,892	**,295**	,943	**M32**	162,51	718,219	,663	,940
M11	162,11	739,382	,528	,941	**M33**	162,56	723,715	,635	,940
M12	161,51	763,933	**,280**	,943	**M34**	161,75	744,760	,601	,941
M13	162,74	721,340	,650	,940	**M35**	162,68	737,256	,441	,942
M14	161,86	747,801	,471	,942	**M36**	161,96	742,106	,553	,941
M15	161,58	759,141	,434	,942	**M37**	162,49	735,504	,549	,941
M16	162,35	745,482	,438	,942	**M38**	162,61	730,884	,613	,941
M17	162,58	733,177	,632	,941	**M39**	161,82	736,540	,589	,941
M18	162,54	724,895	,647	,940	**M40**	163,04	735,784	,455	,942
M19	162,65	719,303	,700	,940	**M41**	162,28	738,027	,459	,942
M20	162,07	745,709	,402	,942	**M42**	162,56	760,501	**,119**	,945
M21	161,88	739,895	,597	,941	**M43**	162,77	762,393	**,115**	,944
M22	162,16	737,314	,497	,941					

Upon analyzing the adjusted item-total correlation values, it is observed that the values for M42 and M43 fell below the 0.20 threshold. Despite the potential inclination to exclude these items to enhance the scale's reliability, the author consciously chose to retain them. This decision was driven by the direct relevance of these items to the field of Information Technologies, encompassing technologies such as the Global Positioning System (GPS), Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS), particularly within the context of maritime operations and associated cybersecurity concerns. Additionally, items M2, M3, M10, and M12 exhibited correlation values ranging from 0.20 to 0.30. To enhance the scale's reliability, it was decided to eliminate only M3 from the scale. This choice was based on the rationale that the inquiry about whether participants had an antivirus program on their computers was adequately addressed by M2. Considering scale consistency, enhancements in reliability measures, and the fact that participants with antivirus programs typically receive automatic updates, M3 was excluded.

Regarding the other items, as they did not show low correlation values and remained relevant to the scale's subject matter, it was deemed appropriate to retain them within the scale. Following the removal of only Item M3, reliability analysis was conducted again, yielding the results presented in Table 4 and Table 5. Re-application of the tests revealed a new Cα value of 0.943, indicating no significant improvement overall but maintaining a high level of reliability of the scale. Despite the lack of significant improvement in correlation, items with low correlation values retained their status. In light of these results, it has been opted to keep all items other than M3, emphasizing their importance within the subject matter, given the sufficiently high Cα value. Item-wise, all items maintained their high-reliability status concerning Cα values on the updated scale, as depicted in Table 4.

Table 4. *Reliability Statistics After Item M3 Removal.*

Cronbach's Alpha After Item Removal	Cronbach's Alpha Based on Standardized Items After Item Removal	Number of Items
0,943	0,943	42

Table 5. *Initial Item-Total Statistics After Item M3 Removal.*

A: Items, **B:** Scale Mean After Item M3 Removal, **C:** Scale Variance After Item M3 Removal, **D:** Corrected Item-Total Correlation, **E:** Cronbach's Alpha After Item M3 Removal

A	B	C	D	E	A	B	C	D	E
M1	157.91	712.046	.631	.940	**M23**	158.16	733.314	.388	.942
M2	156.84	755.385	**.279**	.943	**M24**	158.70	736.463	.331	.943
M4	157.47	735.754	.426	.942	**M25**	158.09	710.546	.717	.940
M5	157.21	745.419	.450	.942	**M26**	157.96	718.213	.683	.940
M6	156.88	751.431	.315	.943	**M27**	157.79	710.848	.708	.940
M7	158.35	735.910	.316	.943	**M28**	157.84	701.100	.828	.939
M8	158.18	723.540	.510	.942	**M29**	157.84	703.242	.789	.939
M9	158.04	727.249	.461	.942	**M30**	157.88	702.681	.779	.939
M10	157.33	744.583	**.295**	.943	**M31**	157.88	703.395	.755	.939
M11	157.40	731.352	.525	.941	**M32**	157.81	709.980	.665	.940
M12	156.81	755.730	**.275**	.943	**M33**	157.86	715.409	.637	.940
M13	158.04	713.249	.649	.940	**M34**	157.05	736.551	.600	.941
M14	157.16	739.492	.472	.942	**M35**	157.98	728.910	.443	.942
M15	156.88	750.967	.429	.942	**M36**	157.26	733.912	.552	.941
M16	157.65	737.125	.440	.942	**M37**	157.79	727.169	.551	.941
M17	157.88	724.895	.633	.941	**M38**	157.91	722.760	.612	.941
M18	157.84	716.564	.650	.940	**M39**	157.12	728.395	.588	.941
M19	157.95	711.122	.701	.940	**M40**	158.33	727.476	.456	.942
M20	157.37	737.523	.401	.942	**M41**	157.58	729.712	.460	.942
M21	157.18	731.647	.597	.941	**M42**	157.86	752.587	**.113**	.945
M22	157.46	729.145	.496	.942	**M43**	158.07	753.924	**.117**	.944

Factor analysis was performed to gather the correlated variables among these 43 variables into one category, to obtain fewer factors, and to reduce the number of variables, that is, to provide ease of visualization and interpretation of the analysis by reducing the number of dimensions.

To determine if the data is suitable for factor analysis, the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's Test of Sphericity were carried out as given in Table 6 below.

Table 6. *KMO and Bartlett's test.*

Kaiser-Meyer-Olkin Test for Measure of Sampling Adequacy		Overall: 0.854
Bartlett's Test of Sphericity	Approx. Chi-Square	1981.547
	df	861
	p	<.001

KMO test value closer to 1 indicates that the patterns of correlation are tight and the sample size is sufficient for factor analysis. Since the obtained KMO value is 0.854, the result showed adequacy for factor analysis. The result of Bartlett's test is also significant since p=0.001< 0.05, which shows that the relationships between variables are present, and the obtained results as well as the data are adequate for factor analysis. According to both findings, the data is suitable for factor analysis. After proving adequacy for factor analysis, first an exploratory factor analysis was conducted by utilizing PCA to determine the factor structure of the refined scale, then it is followed by CFA.

For PCA, common factor variances (commonalities) were first calculated to show how much variance each variable shares with others, as shown in Table 7. Next, eigenvalues were calculated to indicate the variance explained by each factor, and the total explained variance was presented.

Table 7. *Commonalities.*

Items	Initial	Extraction	Items	Initial	Extraction	Items	Initial	Extraction
M1	.448	.406	**M16**	.373	.365	**M30**	.789	.767
M2	.452	.435	**M17**	.479	.460	**M31**	.821	.849
M4	.518	.585	**M18**	.518	.572	**M32**	.645	.628
M5	.527	.455	**M19**	.526	.554	**M33**	.575	.498
M6	.402	.400	**M20**	.488	.462	**M34**	.578	.562
M7	.413	.419	**M21**	.603	.619	**M35**	.532	.487
M8	.578	.539	**M22**	.535	.552	**M36**	.710	.795
M9	.546	.544	**M23**	.520	.490	**M37**	.732	.728
M10	.424	.451	**M24**	.317	.179	**M38**	.679	.616
M11	.611	.511	**M25**	.621	.503	**M39**	.732	.661
M12	.481	.454	**M26**	.676	.617	**M40**	.627	.719
M13	.542	.452	**M27**	.639	.642	**M41**	.501	.511
M14	.500	.470	**M28**	.766	.777	**M42**	.351	.369
M15	.470	.562	**M29**	.709	.717	**M43**	.386	.329

To reduce the number of variables by transforming them into related factors, and improve the visualization and interpretation of the analysis, factor analysis was used for 43 variables. Based on Kaiser's criterion, eigenvalues exceeding "1" were used to determine factors. After the transformation, 10 factors emerged as stated in Table 8.

Table 8. *Factor characteristics.*

		Unrotated Solution			Rotated Solution		
Factors	**Eigen values**	**Sum Sq. Loadings**	**Proportion Var.**	**Cumulative**	**Sum Sq. Loadings**	**Proportion Var.**	**Cumulative**
Factor 1	16.695	16.024	0.286	0.286	10.000	0.179	0.179
Factor 2	4.775	4.134	0.074	0.360	4.599	0.082	0.261
Factor 3	2.966	2.182	0.039	0.399	3.795	0.068	0.329
Factor 4	2.314	1.696	0.030	0.430	2.674	0.048	0.377
Factor 5	2.173	1.479	0.026	0.456	2.244	0.040	0.417
Factor 6	2.044	1.394	0.025	0.481	2.140	0.038	0.455
Factor 7	1.867	1.135	0.020	0.501	1.474	0.026	0.481
Factor 8	1.724	0.935	0.017	0.518	1.389	0.025	0.506
Factor 9	1.609	0.885	0.016	0.534	1.343	0.024	0.530
Factor 10	1.501	0.804	0.014	0.548	1.010	0.018	0.548

When Table 8 is analyzed, the first factor explains 28.6% of the total variance in the unrotated solution, which is the majority of the variance. In the rotated solution, the first factor explains 17.9% of the variance. The cumulative variance explained by the eigenvalues is 54.8% of the total variance for both solutions.

As a result of these tests, which variables are collected under which factor will be stated in the following paragraphs, and the final factor loadings will be presented in Table 11.

A scree plot was also used to visualize the point where the linearization occurs after eigenvalue 1. In the scree plot in Figure 4, the eigenvalue approach is in line with the plot "elbow" point, where 10 factors can be determined with $\lambda \geq 1$.

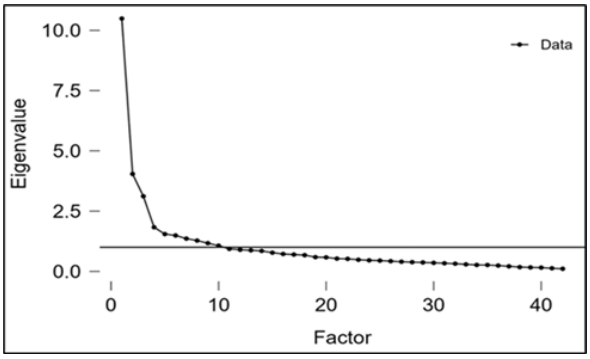

Figure 4*. Scree plot for Cybersecurity Awareness Scale dimensions***.

For further evaluation, the rotated component matrix has been calculated. For the rotated component matrix, Varimax with Kaiser Normalization was determined as the rotation method and was converged after 13 iterations.

The rotated factor loadings matrix in Table 9 shows the association of variables with each factor.

Table 9. *Factor loadings.*

Factor	1	2	3	4	5	6	7	8	9	10
M1									0.464	
M2					0.367				0.567	
M4									0.772	
M5					0.569				0.308	
M6					0.511					
M7										0.708
M8				0.588						0.381
M9				0.734						
M10			0.303	0.538	0.368					
M11			0.594						0.348	
M12					0.433					
M13		0.393				0.341			0.351	
M14			0.356		0.500					
M15					0.715					
M16					0.371					0.421
M17		0.366								0.464
M18						0.969				
M19						0.544				0.458

M20			0.743							
M21			0.690							
M22			0.521	0.386			0.335			
M24	0.409									
M23							1.018			
M25	0.417						0.344			
M26		0.468					0.337			
M27		1.003								
M28	0.731	0.422								
M29	0.896									
M30	1.126									
M31	1.190									
M32	0.816									
M33	0.674									
M34										
M35								0.486		
M36								0.332		
M37								0.569		
M38								0.485		
M39								0.410		
M40								0.646		
M41								0.413		
M42										
M43										

Exploratory Factor Analysis showed that there are 9 factors or dimensions of the scale based on the data. From Table 9, some of the items have high cross-loadings, which means they are represented strongly by more than one factor. On the other hand, Factor 7 only has one member, which is M23. Hence, it is not suitable for CFA and is left out.

As the observed values are satisfactory, the model can be stated to satisfy structural validity, and CFA can be performed.

3.2. Confirmatory factor analysis

CFA was performed using AMOS software. To provide a satisfactory CFA model, model fitness indicators were evaluated. The criteria for model fitness indicators are given in Table 10 below (Fornell & Larcker, 1981), (Hu & Bentler, 1998), (Hair Jr. et al., 2014), (Köseoğlu et al., 2022).

***Table 10.** Model fit criterion.*

Model Fit Indices	**Model Fit Criterion**	**Results**
X^2	-	924.030
df	-	619
X^2/df	X^2/df <3	1.493
RMSEA	0.00≤RMSEA≤0.1	0.050
CFI	0.9≤CFI	0.911
IFI	0.9≤IFI	0.913
TLI	0.9≤TLI	0.900
Goodness of Fit		0.971

According to model fit indices, the CFA model shows inconsistency with the criteria. Chi-Square fitness statistic values show a good fit with (X^2) = 1597,42, (df) = 764, and (X^2/df) = 2.091. Among other fit indicators, the root mean square error of approximation (RMSEA) was observed as 0.050, which indicates a good and close fit, while the comparative fit index value (CFI = 0.911), Incremental Fit Index (IFI = 0.913), and Tucker-Lewis Index (TLI = 0.900) are above 0.9, which means the model shows potential to be a good fit, as given in Table 9. The finalized factor loadings are given in Table 11.

***Table 11.** Finalized factor loadings.*

						95% Confidence Interval	
Factor	**Indicator**	**Estimate**	**Std. Error**	**z-value**	**p**	**Lower**	**Upper**
Factor 1	M24	0.355	0.096	3.714	< .001	0.168	0.543
	M28	1.095	0.076	14.450	< .001	0.947	1.244
	M29	1.063	0.079	13.497	< .001	0.909	1.218
	M30	1.107	0.079	13.944	< .001	0.951	1.262
	M31	1.122	0.079	14.267	< .001	0.968	1.276
	M25	0.623	0.192	3.238	0.001	0.246	1.000
	M32	1.054	0.084	12.599	< .001	0.890	1.218
	M33	0.899	0.086	10.455	< .001	0.731	1.068
Factor 2	M13	0.121	0.155	0.779	0.436	-0.183	0.425
	M26	0.952	0.085	11.162	< .001	0.784	1.119
	M27	1.097	0.088	12.454	< .001	0.925	1.270
	M25	0.179	0.205	0.870	0.384	-0.224	0.581
Factor 3	M11	0.973	0.087	11.204	< .001	0.803	1.143

	M20	0.443	0.093	4.754	< .001	0.260	0.625
	M14	0.370	0.098	3.793	< .001	0.179	0.561
	M10	0.949	0.189	5.010	< .001	0.578	1.320
	M21	0.605	0.078	7.757	< .001	0.452	0.758
	M22	0.817	0.094	8.705	< .001	0.633	1.001
Factor 4	M8	0.979	0.099	9.852	< .001	0.784	1.173
	M9	0.964	0.092	10.475	< .001	0.784	1.144
	M2	-1.021	0.375	-2.725	0.006	-1.755	-0.287
	M10	-0.294	0.190	-1.546	0.122	-0.667	0.079
Factor 5	M5	0.415	0.103	4.039	< .001	0.213	0.616
	M6	0.599	0.073	8.194	< .001	0.456	0.742
	M14	0.436	0.101	4.305	< .001	0.238	0.635
	M15	0.718	0.075	9.599	< .001	0.571	0.865
	M12	0.605	0.073	8.317	< .001	0.462	0.747
Factor 6	M18	0.917	0.093	9.830	< .001	0.734	1.100
	M19	0.943	0.097	9.689	< .001	0.753	1.134
Factor 8	M35	0.477	0.048	10.039	< .001	0.384	0.570
	M36	0.308	0.034	8.961	< .001	0.241	0.375
	M37	0.532	0.037	14.407	< .001	0.460	0.604
	M38	0.496	0.039	12.693	< .001	0.419	0.572
	M39	0.379	0.037	10.239	< .001	0.306	0.452
	M40	0.559	0.046	12.134	< .001	0.469	0.649
	M41	0.389	0.047	8.342	< .001	0.297	0.480
Factor 9	M1	0.811	0.097	8.336	< .001	0.620	1.001
	M2	1.557	0.367	4.244	< .001	0.838	2.275
	M5	0.477	0.099	4.830	< .001	0.284	0.671
	M4	0.836	0.086	9.689	< .001	0.667	1.005
Factor 10	M7	0.680	0.106	6.404	< .001	0.472	0.888
	M16	0.483	0.089	5.403	< .001	0.308	0.658
	M13	0.841	0.147	5.741	< .001	0.554	1.129
	M17	0.858	0.088	9.709	< .001	0.685	1.031

The items listed were adjusted to exhibit correlated residual covariances, reflecting their shared variances, as detailed in Table 12. Additionally, modifications to the model are reflected in Table 13, where factor covariances are presented. This method not only enhanced the model fit but also incorporated cross-loadings to contribute to overall model fitness.

Table 12. *Residual covariance modifications.*

							95% Confidence Interval	
			Estimate	**Std. Error**	**z-value**	**p**	**Lower**	**Upper**
M36	↔	M39	0.088	0.015	5.807	< .001	0.058	0.118
M20	↔	M21	0.487	0.087	5.585	< .001	0.316	0.658
M30	↔	M31	0.238	0.057	4.150	< .001	0.126	0.350
M25	↔	M26	0.376	0.083	4.537	< .001	0.214	0.538

Table 13. *Factor covariance modifications.*

							95% Confidence Interval	
Factors			**Estimate**	**Std. Error**	**z-value**	**p**	**Lower**	**Upper**
Factor 1	↔	Factor 2	0.842	0.041	20.628	< .001	0.762	0.921
Factor 1	↔	Factor 3	0.442	0.073	6.054	< .001	0.299	0.585
Factor 1	↔	Factor 4	0.707	0.057	12.319	< .001	0.595	0.820
Factor 1	↔	Factor 5	0.205	0.085	2.400	0.016	0.038	0.372
Factor 1	↔	Factor 6	0.581	0.070	8.285	< .001	0.444	0.719
Factor 1	↔	Factor 8	0.307	0.072	4.249	< .001	0.165	0.449
Factor 1	↔	Factor 9	0.590	0.066	8.933	< .001	0.461	0.720
Factor 1	↔	Factor 10	0.565	0.076	7.414	< .001	0.416	0.715
Factor 2	↔	Factor 3	0.434	0.082	5.259	< .001	0.272	0.595
Factor 2	↔	Factor 4	0.633	0.074	8.540	< .001	0.488	0.779
Factor 2	↔	Factor 5	0.341	0.089	3.808	< .001	0.165	0.516
Factor 2	↔	Factor 6	0.632	0.077	8.151	< .001	0.480	0.783
Factor 2	↔	Factor 8	0.315	0.080	3.952	< .001	0.159	0.471
Factor 2	↔	Factor 9	0.608	0.069	8.796	< .001	0.472	0.743
Factor 2	↔	Factor 10	0.689	0.080	8.576	< .001	0.532	0.847
Factor 3	↔	Factor 4	0.720	0.077	9.347	< .001	0.569	0.871
Factor 3	↔	Factor 5	0.560	0.078	7.148	< .001	0.407	0.714
Factor 3	↔	Factor 6	0.501	0.087	5.787	< .001	0.332	0.671
Factor 3	↔	Factor 8	0.202	0.083	2.431	0.015	0.039	0.365
Factor 3	↔	Factor 9	0.748	0.058	12.944	< .001	0.635	0.862
Factor 3	↔	Factor 10	0.761	0.065	11.753	< .001	0.634	0.888

Factor 4	↔	Factor 5	0.199	0.101	1.975	0.048	0.001	0.396
Factor 4	↔	Factor 6	0.795	0.069	11.582	< .001	0.660	0.929
Factor 4	↔	Factor 8	0.252	0.086	2.940	0.003	0.084	0.420
Factor 4	↔	Factor 9	0.825	0.065	12.740	< .001	0.698	0.952
Factor 4	↔	Factor 10	0.847	0.067	12.642	< .001	0.716	0.979
Factor 5	↔	Factor 6	0.317	0.097	3.254	0.001	0.126	0.508
Factor 5	↔	Factor 8	0.047	0.088	0.530	0.596	-0.126	0.219
Factor 5	↔	Factor 9	0.478	0.089	5.390	< .001	0.304	0.652
Factor 5	↔	Factor 10	0.420	0.093	4.499	< .001	0.237	0.603
Factor 6	↔	Factor 8	0.337	0.085	3.961	< .001	0.170	0.504
Factor 6	↔	Factor 9	0.751	0.067	11.205	< .001	0.620	0.882
Factor 6	↔	Factor 10	0.857	0.069	12.445	< .001	0.722	0.992
Factor 8	↔	Factor 9	0.204	0.082	2.496	0.013	0.044	0.364
Factor 8	↔	Factor 10	0.359	0.083	4.310	< .001	0.196	0.522
Factor 9	↔	Factor 10	0.815	0.063	13.034	< .001	0.692	0.938

CFA model for the Cybersecurity Awareness Scale is presented in Figure 5 below. The proposed "Cybersecurity Awareness Scale" can be stated to be ensured with promising results after exploratory factor analysis and CFA.

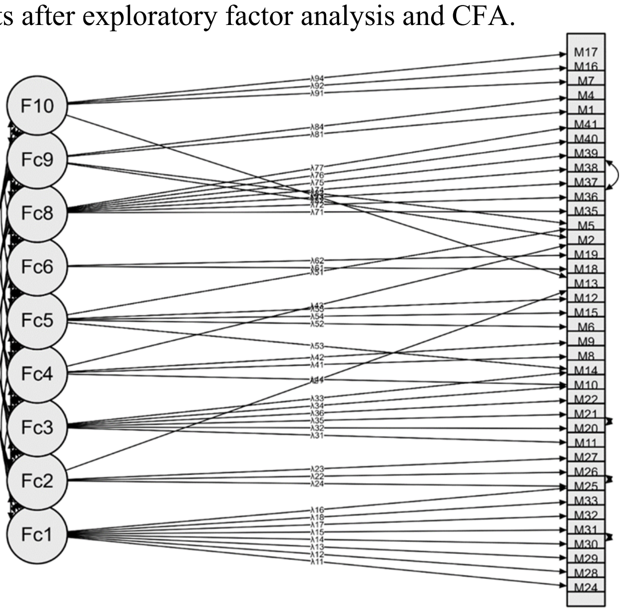

Figure 5. *Confirmatory factor analysis model for cybersecurity awareness scale.*

Current results indicate a good fit with the created model. The limitation of such a proposition for a scale comes from the sample size, meaning the participants. The industrial stakeholders do not have updated knowledge on cybersecurity as of today, which is why the Cybersecurity Awareness Scale is proposed. Although the acquired results showcase the reliability and validity of the proposed scale, the model has room to improve with an increased sample size.

3.3. Discussion

The cybersecurity scale has been applied to 200 participants in İstanbul, Türkiye. Initially, descriptive statistics have been applied to the collected data to look for the sensitivity of questions based on the demographics of the sample size. Accordingly, 18 items for gender, 13 items for education level, and 9 items for age demographics have been observed to have significant differences in statistical analysis and can be stated to be sensitive to these demographics.

The validity and reliability of the scale were assessed through EFA and CFA. The Cronbach alpha value was initially used to determine eligibility for EFA and CFA. The scale was refined based on Cronbach alpha scores, leading to the removal of item M3 and resulting in a 42-item scale. Adequacy for factor analysis was further confirmed through KMO and Barlett's tests. EFA using PCA revealed nine factors or dimensions of the scale. The distribution of items across factors was evaluated both theoretically and mathematically, with the authors confirming the distribution based on their theoretical relationship after obtaining the mathematical distribution from EFA.

EFA was followed by CFA to refine the scale. Initially, CFA results were unsatisfactory, prompting modifications to improve model fit and statistics scores. Once a satisfactory fit was achieved, CFA, along with reliability and validity analyses, was completed. The scale was then applied to participants, and the data collected was evaluated regarding cybersecurity awareness among maritime employees in Istanbul. An online survey involving 200 employees was conducted, with results analyzed based on 42 items and nine factors identified through factor analysis.

Training (M1): The results show that 48% of employees have received cybersecurity training. However, the analysis suggests these programs lack the depth needed to address evolving cyber threats, indicating a need for a more comprehensive approach to improve sector-wide cyber resilience.

Computer-Related Practices (M2, M4, M5): The results show that 37% of respondents, including the undecided, do not use passwords for important files. It is recommended to use encryption methods to enhance file security.

Mobile Phone Security (M6, M7): The data shows a security weakness in mobile phones, with 58% of employees, including undecided respondents, not using antivirus software. This leaves mobile devices highly vulnerable to attacks.

Online Behavior (M8-M14): The data reveals issues with online behavior: 56% of respondents do not check website security certificates, and 57% do not use a VPN in public, exposing them to potential attacks. While 88% are suspicious of unfamiliar emails, indicating phishing awareness, broader cybersecurity practices need attention.

Password Management (M16-M19): While 76% of respondents use strong passwords, 60%, including undecided respondents, do not use multi-factor authentication, underscoring the need for additional security measures beyond passwords.

Social Media Practices (M20-M22): Positive trends in social media practices are evident, with 75% of respondents avoiding adding unknown people as friends. However, 54% lack awareness of social engineering, indicating a need for comprehensive training to recognize and mitigate these threats.

Cybersecurity Term Awareness (M24-M33): Approximately 71% of employees have not experienced a cyberattack, indicating good current cybersecurity preparedness. However, constant vigilance is required due to ongoing cyber threats.

Senior Management and IT Employee Awareness (M34-M42): Questions for senior management and IT staff reveal their crucial role in shaping an organization's cybersecurity. Survey results show high cybersecurity awareness among these individuals, who have more knowledge than other employees. As organizations prioritize cybersecurity awareness, these survey items can help assess organizational preparedness.

Specific Inquiry for Ship Employees (M43): Question M43, which is specific to shipboard personnel, reveals that about 80% of respondents in this group ensure the cybersecurity of IT equipment on board. However, considering removing this question to make the survey more applicable to other sectors highlights the need to balance specificity and generalizability.

4. CONCLUSION

From the perspective of the historical setting of industrial revolutions that were molded by human demands, the rise of Industry 4.0 represents a fast integration of technology into society. Cybersecurity is a serious problem that is related with Industry 4.0, despite the fact that modern society is concerned about the possibility of technology replacing human labor. The purpose of this research is to develop a "5-point Likert Scale" in order to evaluate the level of conceptual knowledge regarding cybersecurity among personnel working in the maritime sector. The "Cybersecurity Awareness Scale" is comprised of 43 questions and is submitted to rigorous procedures for determining its validity and reliability. The scale, which was administered to two hundred maritime employees in Istanbul, Türkiye, indicated various levels of awareness. Information technology workers shown a high level of awareness, while other individuals had a somewhat lower level of knowledge, both in terms of organizational security risks and individual security vulnerabilities. The survey provides valuable insights into cybersecurity awareness, highlighting the need for comprehensive training and increased vigilance. While maritime respondents showed caution in clicking survey links, indicating a positive security mindset, it's important to recognize that cyber-attacks extend beyond phishing. A broader cyber-defense strategy, including integrating cybersecurity training into accredited institutions' curricula, is needed to equip professionals to deal with cyber threats effectively.

A substantial contribution is made by this scale to the evaluation of the cybersecurity awareness of firms, which assists these organizations in determining their strengths and weaknesses and in putting into action the required steps. Through the utilization of the scale, future research has the potential to delve deeper into theoretical discussions by revealing regional and sectoral variances in cybersecurity awareness. Higher sample sizes for forthcoming research are suggested and this would make it possible to conduct extensive comparisons and would improve the existing body of knowledge on this topic. Not only in maritime domain but also for other industries, future research could use this general scale to compare results from different regions and sectors, contributing to theoretical discussions.

DECLARATION OF COMPETING INTEREST

The author declares that there is not any competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ACKNOWLEDGMENT

The author declares that this study was conducted in accordance with ethics committee procedures of human experiments. To apply the scale to maritime workers, Piri Reis University, Istanbul, Türkiye Ethics Committee approval was received with the code number 2023/9.

REFERENCES

Abrahams, T. O., Farayola O. A., Kaggwa S., Uwaoma P. U., Hassan A. O., & Dawodu S. O. (2024). Cybersecurity Awareness and Education Programs: A Review of Employee Engagement and Accountability. Computer Science & IT Research Journal, 5(1), 100-119. https://doi.org/10.51594/csitrj.v5i1.708

Bielawski, A., & Lazarowska, A. (2021). Discussing cybersecurity in maritime transportation. *Maritime Technology and Research*, *4*(1), 252151. https://doi.org/10.33175/mtr.2022.252151

Bolat, P., & Kayişoğlu, G. (2019). Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector. *Journal of ETA Maritime Science*, *7*(4), 344–360. https://doi.org/10.5505/jems.2019.85057

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. Computers & Security, 142, 103858. https://doi.org/10.1016/j.cose.2024.103858

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review, 50, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Clark, J. (2018). Cybercrime in the shipping industry. *A Presentation by Shipping Hill Dickinson LLP*. https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf

Fitton, M. O., Prince, D., & Lacy, M. (2015). *The Future of Maritime Cyber Security., Lancaster University's Faculty of Science and Technology*. https://eprints.lancs.ac.uk/id/eprint/72696/

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39. https://doi.org/10.2307/3151312

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629–3654. https://doi.org/10.1007/s00521-016-2275-y

Hair Jr., J. F., Gabriel, M. L. D. da S., & Patel, V. K. (2014). AMOS Covariance-

Based Structural Equation Modeling (CB-SEM): Guidelines on Its Application as a Marketing Research Tool. *Brazilian Journal of Marketing*, *13*(2), 44–55. https://doi.org/10.5585/remark.v13i2.2718

Hasanspahić, N., Vujičić, S., Frančić, V., & Čampara, L. (2021). The Role of the Human Factor in Marine Accidents. *Journal of Marine Science and Engineering*, *9*(3), 261. https://doi.org/10.3390/jmse9030261

Hong W. C. H., Chun Y. C., Liu J., Zhang Y. F., Lin Lei V. N., & Xu X. S. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. Educ Inf Technol 28, 439–470 (2023). https://doi.org/10.1007/s10639-022-11121-5

Hu, L., & Bentler, P. M. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological Methods*, *3*(4), 424–453. https://doi.org/10.1037/1082-989X.3.4.424

Jensen, L. (2015). Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*, *5*(4), 35–39. https://doi.org/10.22215/timreview/889

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C.-H. (2022). Maritime cybersecurity: are onboard systems ready? *Maritime Policy & Management*, 1–19. https://doi.org/10.1080/03088839.2022.2124464

Kapalidis, P. (2020). Cybersecurity at Sea. In L. Otto (Ed.), *Global Challenges in Maritime Security. Advanced Sciences and Technologies for Security Applications.* (pp. 127–143). https://doi.org/10.1007/978-3-030-34630-0_8

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

Köseoğlu, M. C., Çetin, O., & Yıldırım, F. A. (2022). Maritime Psychology: A Study on Evaluation of Seafarers Aggression Tendencies. *Dokuz Eylül University Maritime Faculty Journal*, *14*(1), 26–50. https://doi.org/DOI: 10.18613/deudfd.1130265

Larsen, M. H., & Lund, M. S. (2021). Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. *IEEE Access*, *9*, 144895–144905. https://doi.org/10.1109/ACCESS.2021.3122433

Mcquade, M. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Mehdiyev, E., Uğurlu, C. T., & Usta, H. G. (2017). The Validity and Reliability Study of English Language Learning Difficulties Scale. *Journal of Theory and Practice in Education*, *13*(3), 411–429. https://dergipark.org.tr/tr/download/article-file/330368

Mraković, I., & Vojinović, R. (2019). Maritime Cyber Security Analysis – How to Reduce Threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Nguyen, L. (2018, February). *e-paper: Collaboration in the Shipping Industry: Innovation and Technology*. KNect365. https://informaconnect.com/epaper-collaboration-in-the-shipping-industry-innovation-and-technology/

Nunnally, J. C. (1978). An Overview of Psychological Measurement. In *Clinical Diagnosis of Mental Disorders* (pp. 97–146). Springer US. https://doi.org/10.1007/978-1-4684-2490-4_4

Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. Computers & Security, 130, 103266. https://doi.org/10.1016/j.cose.2023.103266

Parizo, E. (2019). *Maersk CISO Says NotPeyta Devastated Several Unnamed US firms*. https://www.darkreading.com/omdia/maersk-ciso-says-notpeyta-devastated-several-unnamed-us-firms

Perez, G. F. (2019). *Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry* [Florida, Nova Southeastern University]. https://nsuworks.nova.edu/gscis_etd

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. *Journal of Marine Science and Engineering*, *9*(12), 1384. https://doi.org/10.3390/jmse9121384

Sangwan, A. (2024). Human Factors in Cybersecurity Awareness. 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS), 1–7. https://doi.org/10.1109/ISCS61804.2024.10581139

S. de Vleeschhouwer. (2017). *Safety of data. The risks of cyber security in the maritime sector*. https://maritimetechnology.nl/media/NMT_Safety-of-data-The-risks-of-cyber-security-in-the-maritime-sector.pdf

Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*(1), 129–163. https://doi.org/10.1007/s13437-019-00162-2

Tolossa, D. (2023). Importance of Cybersecurity Awareness Training for Employees in Business. Vidya - A Journal of Gujarat University, 2(2), 104–107. https://doi.org/10.47413/vidya.v2i2.206

Tuomala, V. (2021). *Maritime Cybersecurity. Before the risks turn into attacks*. South-Eastern Finland University of Applied Sciences, Kotka. https://www.theseus.fi/bitstream/handle/10024/504156/URNISBN9789523443600.pdf;jsessionid=3A77CE1482EE9FA27DCFD59FED7562FB?sequence=2

ANNEX - SCALE

CHAPTER 1: SOCIO-DEMOGRAPHIC INFORMATION

a: Your gender:, b: Your age:, c: Your educational status:, d: Type of the company:, e: Your position in the company:, f: Your length of service with the company:

CHAPTER 2: PERSONAL CYBERSECURITY AWARENESS

1: I have been trained in cybersecurity before. [M1]
2: I use antivirus software on my computer. [M2]
3: I update my operating system and the programs I use. [M3] (Item M3 was removed)
4: I put a password on important files on my computer. [M4]
5: I regularly back up files on my computer [M5]
6: I have a screen lock on my cell phone. [M6]
7: I have antivirus software on my mobile phone. [M7]
8: I change my wireless modem password periodically. [M8]
9: I check the security certificates of the websites I visit. [M9]
10: I prevent my web browser from automatically filling in my password and credit card information. [M10]

11: I regularly delete my internet history to prevent cookie theft. [M11]
12: I use a 3D secure method in my online shopping. [M12]
13: I use a VPN when connected to public wireless networks. [M13]
14: I do not share my contact information/personal information on the internet. [M14]
15: I am suspicious of emails from people I don't know. [M15]
16: I use upper/lower case letters, numbers, punctuation, and special symbols to create passwords with at least 16 characters. [M16]
17: I renew my passwords at least once every 3 months. [M17]
18: I use multi-factor authentication when logging into my accounts. [M18]
19: I do not use the same username and password for more than one account. [M19]
20: I don't add people I don't know to my social network. [M20]
21: I adjust the privacy settings of my social media accounts. [M21]
22: I log out of my social network accounts when I am done. [M22]
23: I back up my data encrypted in the cloud. [M23]
24: I've been subjected to a cyber-attack before. [M24]
25: I can tell when someone else is working on my computer in the background. [M25]
26: I know what to do if my computer is hit by a cyber-attack. [M26]
27: I have knowledge about phishing, Spear phishing, smishing, and voicing. [M27]
28: I know what a social engineering attack is. [M28]
29: I know what ransomware is. [M29]
30: I know the difference between Dos and DDOS. [M30]
31: I know what a zombie computer is. [M31]
32: I know what a key logger is. [M32] 33: I know reverse engineering. [M33]

CHAPTER 3: CYBER SECURITY AWARENESS OF THE COMPANY'S IT AND MANAGEMENT STAFF

34: Our company considers that there may be possible risks in terms of cyber security and takes measures against them. [M34]
35: ISO 27001 Information Security Management Standards are applied in our company. [M35]
36: Measures related to KVKK are taken in our company. [M36]
37: Regular cybersecurity training and drills are implemented in our company. [M37]
38: Our company has an alarm system for physical attacks. [M38]
39: Our company has a UPS against possible power failures. [M39]
41: Our company uses a paper shredding machine. [M41]
42: Our company uses a cloud backup service. [M42]
43: We ensure the cybersecurity of our equipment such as GPS, AIS, ECDIS, RADAR.