Received: 13 June 2019 *Accepted: 21 November 2019* *DOI ID: 10.5505/jems.2019.85057*

Journal of ETA Maritime Science

JEMS JOURNAL

Corresponding Author: Gizem KAYİŞOĞLU

Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector

Pelin BOLAT, Gizem KAYİŞOĞLU

Istanbul Technical University, Maritime Faculty, Turkey
yilmazp@itu.edu.tr; ORCID ID: https://orcid.org/0000-0003-4262-3612
gizem6793@hotmail.com; ORCID ID: https://orcid.org/0000-0003-2730-9780

Abstract

Cybersecurity awareness has become an important issue in maritime transportation as well as in other sectors. In this paper, after analyzing maritime cybersecurity literature, it is aimed to understand the factors of antecedents and consequences of cybersecurity awareness in maritime domain by taking Turkish Maritime Sector as a case study. Structural Equation Modeling is used for understanding the factors by validating a questionnaire data from 211 maritime employees who graduated from the Department of Marine Transportation Management Engineering and Marine Engineering in Turkey. It is found that (a) education is a significant factor in enhancing the maritime cybersecurity awareness of employee's and their attitudes towards cybersecurity; (b) cybersecurity incidents or experiences significantly influence employee's cybersecurity awareness and their behavior; (c) maritime cybersecurity awareness significantly affects secure user behavior. In addition, results showed that rules and policies with information sharing do not have any significant effect on cybersecurity awareness and on the development of secure employee behavior.

Keywords: *Cybersecurity awareness, Maritime sector, Secure behavior, Factor analyzing.*

Deniz Siber Güvenlik Bilincinin Öncülleri ve Sonuçları: Türkiye Denizcilik Sektörü İçin Bir Vaka Çalışması

Öz

Siber güvenlik farkındalığı, deniz taşımacılığında ve diğer sektörlerde önemli bir sorun olarak ortaya çıkmaktadır. Bu çalışmada, deniz alanında siber güvenlik ile ilgili çalışmalar analiz edildikten sonra, Türk Denizcilik Sektörü bir örnek olay incelemesi olarak alınarak denizcilik alanındaki siber güvenlik farkındalığının öncül faktörlerinin ve sonuçlarının anlaşılması amaçlanmıştır. Yapısal Eşitlik Modellemesi, Türkiye'nin Deniz Ulaştırma İşletme Mühendisliği ile Gemi Makineleri İşletme Mühendisliği bölümlerinden mezun 211 denizcilik çalışanından elde edilen anket verilerini analiz ederek hipotezleri doğrulamak için kullanılmıştır. Yapısal Eşitlik Modelinin sonuçlarına göre; (a) eğitimin, deniz çalışanlarının siber güvenliğe yönelik doğru davranış geliştirebilmesi için siber güvenlik farkındalığını etkileyen önemli bir faktör olduğu; (b) siber güvenlik olaylarının veya deneyimlerinin, çalışanın siber güvenlik farkındalığını ve davranışlarını önemli ölçüde etkilediği; (c) deniz siber güvenlik farkındalığının, güvenli kullanıcı davranışını önemli ölçüde etkilediği sonuçları ortaya çıkmıştır. Ek olarak, bilgi paylaşımı ve kural ile politikaların diğer sektörlerde olduğunun tersine denizcilik sektöründe çalışanların siber güvenlik farkındalığı ve güvenli davranış geliştirmesi üzerinde önemli bir etkisi olmadığı sonucuna varılmıştır.

Anahtar Kelimeler: *Siber güvenlik farkındalığı, Denizcilik sektörü, Güvenli davranış, Faktör analizi.*

To cite this article: 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.
To link to this article: https://dx.doi.org/10.5505/jems.2019.85057

1. Introduction

The prefix "cyber" is a common term that is used for defining information technologies including computer and internet. The International Telecommunication Union describes "cybersecurity" as all technologies and procedures that include hardware, software, policies, security concepts, protection measures, guidelines, risk management approaches, precautions, education and applications for cyber space and related individuals and organizations. In the literature, there are also several definitions for cybersecurity. For example, National Initiative for Cybersecurity Careers and Studies [1] explains the term of cybersecurity as the state, capability, process which information and communications systems are protected from unauthorized modification and defended against damage. The National Institute of Standards and Technology [2] defines cybersecurity as the process of protecting information by frustrating, specifying, and replying to attacks. Cyber Strategy for Norway (ENISA) defines cybersecurity as the protection of data and systems connected to the Internet [3]. In addition, it is seen that multiple cybersecurity definitions have been given in national security policy agendas of the countries [4]. The common point of these definitions is that an end user is the essential agent in cybersecurity due to his/her role in preventing, detecting and responding to a cyber-attack. Accordingly, it can be concluded that cybersecurity is a user-centered concept which needs adoption of secure behavior against cyber vulnerabilities and attacks. For instance, VMWARE report [5] indicated that an average of 100 cyber-attacks per year had been experienced by the companies whose IT security teams could not diagnose 98% of them. Global Risks Report [6] also stated that a big number of cyber-crimes were not discovered every year because it was difficult for end users to realize the existence of an illicit access to cyber systems. Cybersecurity Intelligence Index [7] presented that 95% of all security events were caused due to human factor based errors. In this point of view, cybersecurity awareness has become an important challenge for sustainable information transaction in the digital world for end users both at home and at work.

Regarding cybersecurity awareness at workplace, since end users are employees themselves, they are important agents for ensuring the security of cyber physical system and protecting the information they process. Human-based vulnerabilities such as using weak passwords, opening unknown e-mail attachments, ignoring risks resulted by wireless systems and mobile devices at work can end up with cyber-attack [8]. Accordingly, cybersecurity incidents are resulted by the acts of employees that originate from inadvertency and not being aware of cybersecurity policies and procedures. Hansche [9] stated that threats to equipment, stored information, open network environments during cybersecurity incidents should be comprehended by the employees. Rezgui and Marks [10] found that conscientiousness, cultural beliefs and social conditions had impact on staff behavior and attitude toward information security awareness. Consequently, cybersecurity awareness programs should be established as tailor-made since organizational dynamics and employees' approaches can be different for each work environment. Accordingly, understanding the antecedents for cybersecurity awareness and investigating the consequences of cybersecurity awareness are empirically important from a managerial point of view to ensure cybersecurity in workplace.

In the foregoing circumstances, determinants of cybersecurity awareness and its mediating effect on end users' behavior should be investigated for the maritime sector. The literature shows us that researches about cybersecurity awareness have mostly been studied for finance [11], education [12] and aviation, [13] while it is seen that there is a lack of studies for the maritime sector.

The maritime transportation sector includes navigation, communication and execution systems that fall under the internal network of the vessel, and the information, communication and technology systems used in the communications of the vessel with the company [14]. The studies indicate that cybersecurity has been a new subject matter recently taken into consideration by large organizations such as IMO, BIMCO, DNV-GL. A limited number of researches done in cybersecurity awareness for the maritime sector shows that the maritime sector has a high level of cyber risk and low level of cybersecurity awareness profile [15,16,17,18].

Consequently, the main aim of this study is to investigate the antecedents and consequences of cybersecurity awareness in the maritime sector to provide a behavioral model for cybersecurity management processes in maritime sectorial companies.

2. Background

Providing cybersecurity by overcoming the risks enables effective operations in organizations. Realizing vulnerabilities and developing pre or post actions are socio-technological functions which require interactive coordination of the personnel and cyberspace interfaces. Thus personnel as end users in companies are of vital importance although they can be also defined as the weakest members of security measures. For example, Vroom and Solms argue that the number of the security events related to the individuals inside the institution surpasses the number of security violations related to the individuals outside, and this shows that the employees pose an enormous threat for the wellbeing of the company [19]. Since human factor has arisen as an important issue for ensuring cybersecurity, the industries which are directly related to human element can be under much more risks than the other sectors. In this context, from the perspective of cybersecurity, maritime transportation industry becomes a hot spot as %90 of the maritime accidents have occurred due to human-related errors.

When incidents and the penetration test related with cybersecurity in the maritime sector is evaluated, it has been seen that lack of awareness and lack of capability to develop secure behavior are important factors for the occurrence of cybersecurity breaches. When looking at responsible persons who are active in related cyber space, it is understood that they are not aware of the protection measures directed against the system [15,17, 20, 21]. Accordingly, we can conclude that maritime transportation is a sector which has high level risk and low level awareness in terms of cybersecurity. This fact was also supported by European Network and Information Security Agency as they presented seven major deficits in term of maritime cybersecurity, as follows [20]:

- Low awareness and focus
- Complex structure of Maritime systems
- Absence of holistic management approach in national and international context in the maritime field
- Inadequacies' related to security of cyber space in maritime regulations
- No holistic understanding of cybersecurity
- Lack of economic incentives and initiatives for work to increase the cybersecurity in the maritime sector
- Lack of incentives to motivate work

On the other hand, some other researches have dealt with understanding the cybersecurity awareness level in organizations. For example, Share Your

Smart Shipping Insights' survey was conducted by SAFETY4SEA [17] and it was assessed that whether stakeholders of maritime sector have been aware of the current and future smart shipping difficulties and have installed the Autonomous Shipping and Future Trends, nature of ECDIS & e-Navigation and Cyber Safety/ Cybersecurity in shipping. Bolat et al. has also done a cyber-security awareness perception survey to 256 participants in Turkish Maritime Sector and they found that the lack of regulations brings low cybersecurity awareness and cybersecurity awareness training would be an important action for maritime transportation industry [15]. Netherland Maritime Technology also emphasized that education and awareness were important for the protection and presentation process of maritime network systems against cyber threats [21]. They also presented that maritime employees should be aware of both cyber risks and secure behavior.

3. Hypothesis Development

3.1 Antecedents

Some studies have dealt with cybersecurity through analyzing situational awareness which includes cognitive studies [22, 23, 24, 25] while some others have studied behavioral aspects to understand general cybersecurity awareness in organizations [26, 27, 28]. In this paper, we also aimed to understand the antecedents and consequents of general cybersecurity awareness among maritime employees, which are shown in Figure 1 and Table 1.

From behavioral aspect, antecedents of cybersecurity awareness can be distinguished as impact of education and training, sharing information, rules and

Table 1. Hypothesis

HYPOTHESIS
H1: Education and Training on cybersecurity positively impacts level of cybersecurity awareness (CSA) of individuals in maritime sector.
H2: Rules and policy developed for cybersecurity positively impacts level of CSA of individuals in maritime sector.
H3: Information sharing about cybersecurity has positive effects on level of CSA of individuals in maritime sector.
H4: Experienced cybersecurity incidents positively impact the level of CSA of individuals in maritime sector.
H5: Cybersecurity awareness positively impacts adoption of secure behavior in maritime sector.

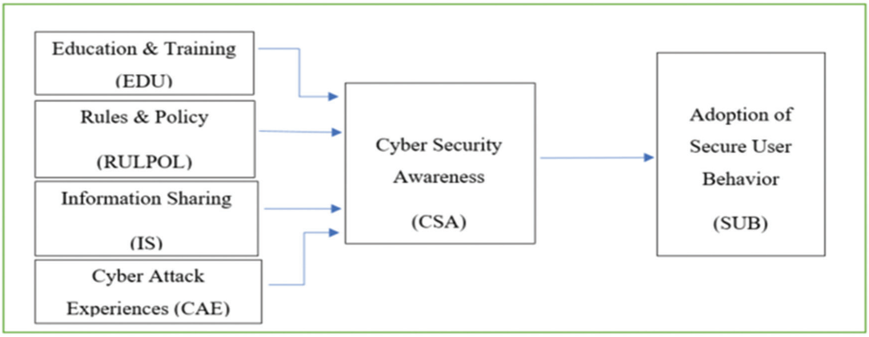

Education & Training (EDU)
Rules & Policy (RULPOL)
Information Sharing (IS)
Cyber Attack Experiences (CAE)
Cyber Security Awareness (CSA)
Adoption of Secure User Behavior (SUB)

Figure 1. Hypothesis Scheme

policies and experienced cyber-attacks while cybersecurity awareness mediates developing secure behavior [12, 29, 30, 31, 28].

Haeussinger and Kranz found that education and training programs about cybersecurity have mediated by cybersecurity awareness to maintain intention to develop secure behavior [12]. Bada and Sasse also emphasized that cybersecurity awareness education should be targeted, actionable, doable as awareness should be integrated with attention and knowledge and has to be properly organized [26]. There are also multifarious studies in the literature on the measures to be taken to affect successfully the behaviors and awareness of the users in this respect. For instance, Lund and Aarø argued that programs that combined with various measures such as information campaigns, trainings, rewards, technological / physical precautions, regulations and implementation, had the most positive effect on risk behaviors [32]. Dodge et al. evaluated the responses of the users for an e-mail phishing attack with an uninformed test [33]. They found that the effectiveness of cybersecurity awareness raising programs affected the security awareness of the participants and provided a promising feedback.

Regarding the maritime transportation industry, education and training has already been used to meet the minimum requirements of STCW and maritime safety and security awareness. In this context, we can obtain following hypothesis;

H1: Education and Training on cybersecurity positively impacts level of cybersecurity awareness (CSA) of individuals in the maritime sector.

Rules and Policy can be other antecedent of cybersecurity awareness. Herath and Rao stated that information security policies could be dependent on organizational, environmental and behavioral factors [29]. Clutch has reported that although companies have adopted cybersecurity policies, a significant number of employees are not aware of these policies and associated threats [34]. They also noted that cybersecurity policies would enhance cyber awareness and cybersecurity measures of the company. In the maritime domain, the fact “policies and rules drive awareness” is also a valid statement. Codes and conventions for maritime transportation which has been put into force by International Maritime Organization (IMO) aim to increase awareness on a specific maritime subject such as safety and security issues by focusing on standardizations and taking precautions. Therefore:

H2: Rules and policy developed for cybersecurity positively impacts the level of CSA of individuals in the maritime sector.

It has been known for some time that the most important factor in increasing information security is to gather, analyze and share information about actual or unsuccessful attempts in computer security violations. In this respect, the federal government of the USA promoted the establishment of sector based Information Sharing and Analysis Centers (ISACs) [35]. The ISACs facilitate the sharing of information of their members about their efforts to increase and maintain the security of their cyber-infrastructures [30]. Safa and Solm introduced that information sharing plays an important role due to its positive effects on the information-security awareness of the employees [36]. Regarding the maritime sector, information sharing and cooperation is also becoming an important implementation way for maritime safety and security solutions

[37]. Enterprises Shipping Trade emphasized that information sharing has been a continuous effort for enhancing the value between the maritime companies, the ships and the other stake holders. Information sharing is a triggering factor for high level effectiveness of dynamic environment of maritime infrastructures [38]. Therefore, we hypostatize that:

H3: Information sharing about cybersecurity has positive effects on the level of CSA of individuals in the maritime sector.

Vaneechoutte stated that awareness itself is also an experience which results from the filtering and processing of the several possible experiences going on in our bodies and brains [31]. According to Kapatker for learning about awareness, it is required to understand experiences [39]. He launched its industrial cybersecurity program with a philosophy awareness by experience. Therefore,

H4: Experienced cybersecurity incidents positively impacts the level of CSA of individuals in the maritime sector.

Development of secure behavior is the consequence of gaining cybersecurity awareness. D'Arcy and Hovav claimed that awareness of end users is a determinant for obtaining secure systems as the behavior of end users have been required for implementing the security countermeasures [40]. Safa et al. found that information security awareness and attitude towards information security have direct effects on the user's behavior [41]. Accordingly,

H5: Cybersecurity awareness positively impacts adoption of secure behavior in maritime sector.

4. Research Method

The research method is examined in three parts which are data collection method, sampling group and analysis and findings.

4.1. Data Collection Tool

"Five Point Likert Type Survey" method was used to understand antecedents and consequences of cybersecurity awareness amongst maritime employees in Turkey from the perspective of organizational management. Antecedents and consequences of cybersecurity in the maritime sector were assessed by a questionnaire which were formed from similar questions in various sources of literature [47, 48, 49, 50, 51,52] and based on our own expertise and experience, shown in Appendix, with 37 statements on a 5-point Likert scale compose from strongly disagree (1) to strongly agree (5). The survey consists of six sections as The Awareness of Cybersecurity – CSA, Developing Secure User Behavior – SUB, The Education related with Cybersecurity – EDU, Company Rules and Policies about Cybersecurity – RULPOL, Sharing of Cybersecurity Information – IS, The Influence of the Cyber Attack Experiences – CAE.

The proposed research model was empirically tested using the survey methodology. Analysis of questionnaire responses involve identifying the effectiveness of model structure, determining which items of the questionnaire should be involved or not, and evaluating the validity and reliability of the data. Likert-type questions include an expression with an attitude or opinion on the topic being searched, and options indicating the level of participation in that statement [42].

4.2. Sampling Group

The questionnaire survey was implemented to the participants via internet [43] and hardcopy.

The target group of this study consists of maritime transportation engineers and marine engineers, for about a 15000 population size [55], in Turkish Maritime

Industry who are working either on sea side or shore side with minimum 1-year sea experience.

In this study, the questionnaire was done by 212 participants. One of them has been omitted because of dual answers for the questions. Hence, 211 engineers have constituted the sample group of the study.

In the literature, it can be seen that some research claimed that simple SEM models could be meaningfully tested even if sample size is quite small [58, 59, 60], but usually, N = 100–150 is considered the minimum sample size for conducting SEM [61;64]. Some researchers consider an even larger sample size for SEM, for example, N = 200 [65, 66, 67]. Simulation studies show that with normally distributed indicator variables and no missing data, a reasonable sample size for a simple CFA model is about N = 150 [68]. In this context, the sample size of this study (211) is adequate number for SEM.

Besides, in the literature, it is found that an "acceptable" margin of error used by survey researchers falls between 4% and 8% at the 95% confidence level [56]. The sample size of the study (211) is higher than 105 and 149 which were obtained for 8% margin of error with 90% and 95% confidence level respectively [57]. Consequently, the sample size 211 is convenient for a population size of 15000 for 6.70% margin of error with 95% confidence level.

The majority of total participants (%89) were male. Approximately %38 of participants aged between 35 and over. Besides, %24 of the participants had experience in the maritime sector for more than 16 years.

4.3. Analysis and Findings

Structural equation modeling (SEM) method was implemented to discover the relationships among the structure in the proposed model. SEM is used to prove the structural model. Particularly, proposed model was examined and the overall fit was evaluated by use of the maximum likelihood method in Amos.

In the proposed model, six potential structures and their observed variables were measured. To evaluate the reflective structure in the measurement model, structure validity, reliability and discriminant validity were examined. First, principal component analysis was performed to define and to affirm the different factors under each structure in the model. Especially, exploratory factor analysis (EFA) was carried out by using the IBM SPSS Statistics version 24.0. To analyze the factor out among the six factors in the model, EFA using principal-component factor analysis with Varimax rotation was conducted. The results showed that the six factors have eigenvalues greater than 1. After that, CFA was performed to prove the factors under each veiled variable with SEM via AMOS.

Table 2. *Descriptive Characteristics of Cybersecurity Perceptions*

Cybersecurity Perception	Items	Mean (SD)	Median	Min	Max	Cronbach's Alpha
Cybersecurity Awareness	6	2.91 (.62)	3	1.98	3.83	.71
Secure User Behavior	7	2.92 (.62)	3	2.56	3.27	.91
Education	9	2.27 (.23)	2	2	2.50	.96
Rules and Policies	7	2.62 (.02)	2.71	2.36	2.74	.95
Information Sharing	3	2.39 (.02)	2.33	2.28	2.56	.89
Cyber Attack Experiences	5	3.30 (.03)	3.60	3.08	3.45	.95

Cronbach's Coefficient Alphas of six dimensions (cybersecurity awareness, secure user behavior, education, rules and policies, sharing information, cyber-attack experiences) were in the desired range (.7–.9), presented in Table 2. As a result of this, it is claimed that both the structure validity and the structure reliability of our model are desirable.

Correlation matrix, presented in Table 3, showed reliability of the items, reflective measures and correlation of 6 variables. The dimension "cybersecurity awareness" was moderately associated with "sharing information". The dimension "secure user behavior" was moderately related to "education" and "rules & policies". The dimension "education" was significantly related to "rules & policies" and "sharing information". And dimension "rules and policies" was essentially associated with "sharing information". All relationship between dimensions were positive hence they were being directly proportionate to each other.

EFA results with principal-component factor analysis by Varimax rotation presented in Table 4. As Kaiser-Meyer-Olkin (KMO value) is ,919 and Bartlett's Test of Sphericity significance value ,000, EFA is valid. All estimated factor loadings are important at the significant level of p < 0.001 with acceptable accent (>0.50, optimum level is >0.70) except CSA2 and CSA5 for our model. The results showed that the convergent validity of measurement is good for our model.

When CFA with structural equation model was established according to EFA results, it was found that information sharing factor is not needed as items of information sharing (IS) factor have been matched with the rules and policy (RUL&POL) factor due to the same factor loading categories. On the other hand, two items, CSA 2 and CSA 5, have been removed from SEM as they have very low factor loadings (,071 - ,172). The fit statistics of the constructional model is reported in Table 5. Criteria of Indicators which shows acceptable values for CFA are presented in Table 6.

Calculating the path coefficients which show the strength of the relationships between the independent and dependent variables takes part in the test of the constructural model. The path coefficients are regression coefficients. The coefficients between the variables in Figure 2 show the relationship between those variables. The coefficients between the main variables are shown as estimate values in Table 7. In Figure 2 and Table 7, the aggregation of relationship for the structural model is supplied.

Table 3. *Inter-dimensional Spearman's Correlation*

	Awareness	Safe User Behavior	Education	Rules and Policies	Sharing Information
Cybersecurity Awareness	1,000				
Secure User Behavior	,405**				
Education	,298**	,413**			
Rules and Policies	,313**	,366**	,630**		
Sharing Information	,369**	,342**	,598**	,749**	
Cyber Attack Experiences	,235**	0,152	0,110	,233**	,324**

***Table 4.** Results of EFA*

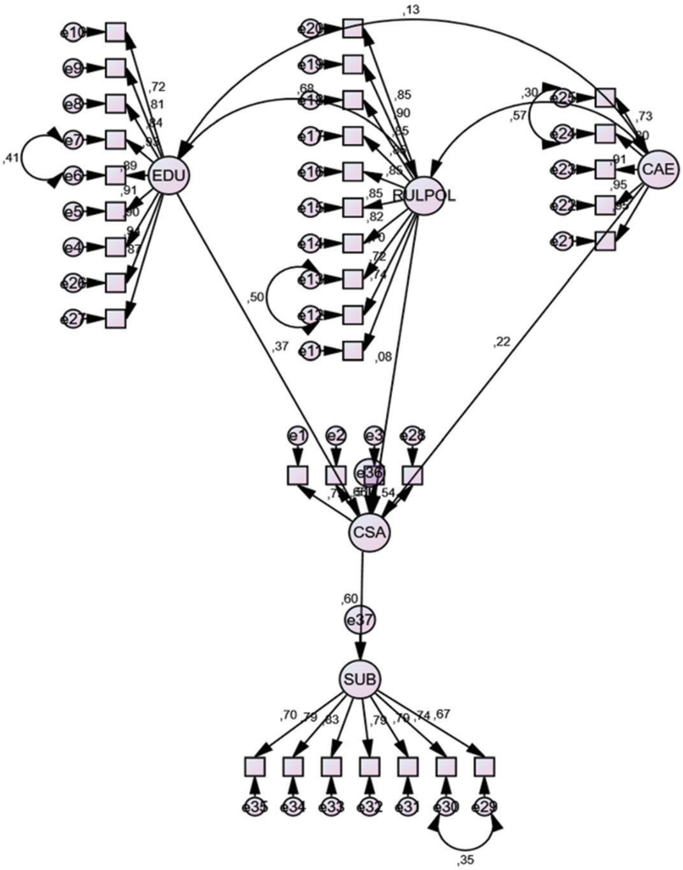
Indicator		Component					
		1	2	3	4	5	6
Cybersecurity Awareness (CSA)	CSA1					,552	
	CSA2					,071	
	CSA3					,789	
	CSA4					,653	
	CSA5					,172	
	CSA6					,706	
Secure User Behavior	SUB1			,758			
	SUB2			,747			
	SUB3			,754			
	SUB4			,809			
	SUB5			,794			
	SUB6			,758			
	SUB7			,709			
Education	EDU1	,743					
	EDU2	,771					
	EDU3	,814					
	EDU4	,863					
	EDU5	,808					
	EDU6	,838					
	EDU7	,833					
	EDU8	,849					
	EDU9	,772					
Rules &Policy	RUL&POL1		,800				
	RUL&POL2		,840				
	RUL&POL3		,804				
	RUL&POL4		,790				
	RUL&POL5		,809				
	RUL&POL6		,807				
	RUL&POL7		,726				
Information Sharing	IS1		,626				
	IS2		,655				
	IS3		,668				
Cybersecurity Experiences	CSE1				,825		
	CSE2				,856		
	CSE3				,915		
	CSE4				,918		
	CSE5				,912		

Table 5. *CFA Indices Results*

Indices	CMIN /Df	RMSEA	CFI	GFI	NFI
Results	1.852	0.064	0.930	0.786	0.861
Acceptable-Inacceptable Situation	Acceptable	Acceptable	Acceptable	Reasonable	Reasonable

Table 6. *Criteria of Indices*

Indices	Criteria of Indices (Acceptable Values)	Source
Chi square / Degrees of Freedom (CMIN /Df)	< 2.00 or 3.00	[46]
Root means square error of approximation (RMSEA)	< 0.08	[44]
Comparative fit index (CFI)	> 0.90	[44]
Goodness of fit index (GFI)	> 0.90 (Acceptable) 0.80–0.89 (Reasonable)	[45]
Normed fit index (NFI)	> 0.90	[46]



(Notes: EDU; Education, RULPOL; Rules and Policy, CAE; Cyber Attack Experiences, CSA; Cybersecurity Awareness, SUB; Secure User Behavior)

Figure 2. *SEM with Standard Estimates*

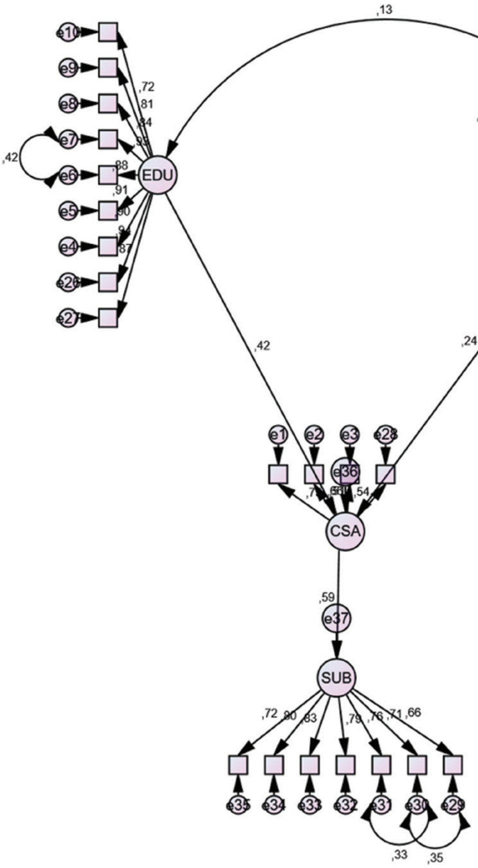
Table 7. *Test Results of Structural Equation Model*

			Estimate	S.E.	C.R.	P
CSA	<---	EDU	,310	,088	3,539	***
CSA	<---	RULPOL	,084	,106	,796	,426
CSA	<---	CAE	,171	,061	2,799	,005
SUB	<---	CSA	,453	,073	6,176	***

5. Discussion

The results confirm that (a) education is a significant factor in enhancing the maritime cybersecurity awareness for employee's behavior towards cybersecurity; (b) cybersecurity incidents or experiences significantly influence employee's cybersecurity awareness and their behavior; (c) maritime cybersecurity awareness significantly affect secure user behavior. On the other hand, rules and policy items were combined with information sharing items and hypothesis related with them (H2 – H3) were rejected, shown in Table 8.

The structural equity model was established again with the hypotheses supported in Figure 3, and their compliance levels and estimate values are shown below.



(Notes: CMIN/DF; 1.659, RMSEA; 0.056, CFI; 0.961, GFI; 0.860, NFI; 0.908)

Figure 3. *Final Model*

Table 8. *Summary of Hypothesis*

Hypothesis	Estimate	S.E	C.R	P	Result
H1	**,310**	**,088**	**3,539**	***	**Supported**
H2 & H3	,084	,106	,796	,426	Not supported
H4	**,171**	**,061**	**2,799**	**,005**	**Supported**
H5	**,453**	**,073**	**6,176**	***	**Supported**

6. Conclusion

Recently, an increasing number of studies are being conducted, as cybersecurity has emerged as a new topic in maritime sector. This naturally reveals that there are numerous aspects of the issue yet to be addressed. The analysis of the factors that affect the cybersecurity awareness in the maritime sector has not been conducted until now. Accordingly, the results obtained in this study are believed to yield both academic and industrial benefits.

Considering that the IMO has granted a time of respite to the ship managers and ship owners until 2021 to become ready for the cybersecurity risks in the vessels, we believe that this study would serve as a guideline for the ship managers and ship owners both industrially and administratively. They would know that they should start with raising awareness on cybersecurity in their personnel. In addition, they would see that education and experience are important topics in providing cybersecurity awareness in their personnel, and they would evaluate how to invest for this issue. Ship managers and ship owners, who perceive that cybersecurity awareness results in secure user behavior, would successfully deal with cybersecurity issues, which are new to the maritime sector with many gaps to fill.

References

[1] URL 1 < https://niccs.us-cert.gov/formal-education/cyber-competitions > (Access: 10.02.2018).

[2] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1, National Institute of Standards and Technology, January, 2017.

[3] ENISA, Analysis of Cybersecurity Aspects in The Maritime Sector, Cybersecurity Strategy for Norway, 2012.<file:///C:/Users/user/Downloads/ENISA%20Guidebook%20on%20National%20Cyber%20Security%20Strategies_Final.pdf>

[4] Rajnovic, D., Cyberspace, What is it?, Cisco Blog, 2012. (Access: 18.06.2017).

[5] Vmware, The Cyber-Chasm: How The Disconnect Between The C-Suite and Security Endangers The Enterprise, The Economist Intelligence Unit, 2016.

[6] Baller, S., Dutta, S., Lanvin, B., The Global Information Technology Report 2016, Innovating in the Digital Economy, 2016.

[7] IBM, Analysis of Cyber Attack and Incident Data from IBM's Worldwide S9ecurity Operations, IBM Security Services 2014 Cybersecurity Intelligence Index, 2014.

[8] NSI, A Brief User's Guide to Getting the Most from Your Employee Security Connection Subscription, Employee Security Connection, National Security Institute, (Access: 22.11.2017).

[9] Hansche, S., Designing A Security Awareness Program: Part 1 Information Systems Security, 9(6), 1-9, 2001.

[10] Rezgui, Y., Marks, A., Information Security Awareness in Higher Education: An Exploratory Study, Computers & Security, 27(7), 241-253, 2008.

[11] Ashford, W., Cybersecurity Awareness Top Priority in Financial Sector, ComputerWeekly.com, February, 2018.

[12] Haeussinger, F., Kranz, J., Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior, AIS Electronic Library, 2013

[13] Mogford, R., Mental Models and Situation Awareness in Air Traffic Control, The International Journal of Aviation Psychology, 7(4), 1997.

[14] Roumboutsos, A., Nikitakos, N., Gritzalis, S., Information Technology Network Security Risk Assessment and Management Framework for Shipping Companies, Maritime Policy & Management, Vol 32, Issue 4, pp. 421-432, 2005

[15] Bolat, P., Yüksel, G., Uygur, S., A Study For Understanding Cybersecurity Awareness Among Turkish Seafarers. The Second Global Maritime Conference on Innovation in Maritime Technology and the Future of Maritime Transportation, Muğla-Bodrum, Turkey, pp. 278 ,24-25 Oct 2016

[16] Kramek, J., The Critical Infrastructure Gap: US Port Facilities and Cyber Vulnerabilities, Center for 21st Century Security and Intelligence, Foreign Policy at Brookings, July, 2013.

[17] Apostolos, B., Smart Shipping Survey Findings, Safety4Sea, February, 2017.

[18] MI News Network, Safety4Sea Survey Reveals Industry's Smart Side, Marine Insight, January, 2017.

[19] Vroom, C., Von Solms, R., Towards Information Security Behavioural Compliance, Computers & Security, 23, pp 191 – 198, 2004.

[20] ENISA, Analysıs of Cybersecurity Aspects in The Marıtıme Sector, P.O. Box 1309, 71001 Heraklion, Greece, 2011.<file:///C:/Users/user/Downloads/2011_ENISA_Analysis_of_cyber_security_aspects_in_the_maritime_sector_1%200%20(4).pdf>

[21] Vleeschhouwer, S. D., Safety of Data, The Risks of Cybersecurity in The Maritime Sector, Netherlands Maritime Technology, MIIP018, 2017.

[22] D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., Roth, E., Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts, Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol 49, Issue 3, pp. 229 – 233, 2005

[23] Kokar, M. M., Endsley, M. R., Situation Awareness and Cognitive Modeling, IEEE Intelligent Systems, Vol 27, Issue 3, pp. 91-96, 2012

[24] Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., Farry, M., A Cognitive Task Analysis for Cyber Situational Awareness, Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol 54, Issue 4, pp. 279 – 283, 2010

[25] McNeese, M., Cooke, N. J., D'Amico, A., Endsley, M. R., Gonzalez, C., Roth, E., Salas, E., Perspectives on the Role of Cognition in Cybersecurity, Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol 56, Issue 1, pp. 268 – 271, 2016

[26] Bada, M., Sasse, A., Cybersecurity Awareness Campaigns: Why Do They Fail to Change Behavior, Global Cybersecurity Capacity Centre: Draft Working Paper, July, 2014

[27] Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, M. H., Information Security Awareness and Behavior: A Theory-Based Literature Review, Management Research Review, Vol. 37, Issue 12, pp.1049-1092, 2014

[28] Pfleeger, S. L., Caputo, D. D., Leveraging Behavioral Science to Mitigate Cybersecurity Risk, Computers & Security, Volume 31, Issue 4, pp. 597-611, 2012

[29] Herath, T., Rao, H. R., Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness, Decision Support Systems, Volume 47, Issue 2, pp. 154-165, 2009

[30] Gal-Or, E., Ghose, A., The Economic Incentives for Sharing Security Information, Information Systems Research, Vol 16, Issue 2, pp. 186-208, 2005

[31] Vaneechoutte, M., Experience, Awareness and Consciousness: Suggestions for Definitions as Offered by an Evolutionary Approach, Foundations of Science, Volume 5, Issue 4, pp 429–456, 2000

[32] Lund, J., Aarø, L. E., Accident Prevention, Presentation of A Model Placing Emphasis on Human, Structural and Cultural Factors, Safety Science, Volume 42, Issue 4, pp. 271-324, 2004

[33] Dodge, R. C., Carver, C., Ferguson, A. J., Phishing for user security awareness, Computers & Security, Volume 26, Issue 1, pp. 73-80, 2007

[34] Clutch., < https://clutch.co/it-services/resources/employee-awareness-it-security-threats > (Access: 25.06.2018)

[35] National Council of ISACs., < https://www.nationalisacs.org/single-post/NCI-Anniversary > (Access: 26.06.2018)

[36] Safa, N. S., Solms, R. V., An Information Security Knowledge Sharing Model in Organizations, Computers in Human Behavior, Volume 57, pp. 442-451, 2016

[37] EU., < https://ec.europa.eu/isa2/actions/sharing-information-maritime-surveillance_en > (Access: 01.06.2018)

[38] Olesen, P. B., Hvolby, H. H., Popovska, I. D., Enabling Information Sharing in a Port, IFIP International Conference on Advances in Production Management Systems, Vol 393, pp. 152-159, 2012

[39] Kapatker., < https://www.scienceandnonduality.com/time-t-0-is-pure-awareness/ >, (Access: 04.06.2018)

[40] D'Arcy, J., Hovav, A., Deterring Internal Information Systems Misuse, Communications of the ACM, Vol 50, Issue 10, pp. 113-117, 2007

[41] Safa, N. S., Sookhak, M., Solms, R. V., Furnell, S., Ghani, N. A., Herawan, T., Information Security Conscious Care Behaviour Formation in Organizations, Computers & Security, Vol 53, pp. 65-78, 2015

[42] Turan, İ., Şimşek, Ü., & Aslan, H., Eğitim Araştırmalarında Likert Ölçeği ve Likert-Tipi Soruların Kullanımı ve Analizi, Sakarya Üniversitesi Eğitim Fakültesi Dergisi, Vol 30, pp. 186-203, 2015

[43] GoogleDrive.,< https:/ /docs.google.com/forms/d/1CX0sq_tXHuAV47KsMHUDjBsLJOVJKcVhr9WmjEOkKac/edit.>(Access: 06.07.2017)

[44] Atkinson, T. M., Rosenfeld, B. D., Sit, L., Mendoza, T. R., Fruscione, M., Lavene, D., . . . Basch, E., Using Confirmatory Factor Analysis to Evaluate Construct Validity of the Brief Pain Inventory (BPI), Journal of Pain and Symptom Management, 41(3), 558-565, 2011

[45] Santor, D. A., Haggerty, J. L., Lévesque, J.-F., Burge, F., Beaulieu, M.-D., Gass, D., & Pineault, R., An Overview of Confirmatory Factor Analysis and Item Response Analysis Applied to Instruments to Evaluate Primary Healthcare, Healthcare Policy, 7(Spec Issue), 79, 2011

[46] Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J., Reporting Structural Equation Modeling and Confirmatory Factor Analysis Results: A Review, The Journal of Educational Research, 99(6), 323-338, 2006

[47] Rheea, H. S., Kimb, C., Ryuc, Y. U., Self-Efficacy in Information Security: Its Influence On End Users' Information Security Practice Behavior, Computers & Security, 1 – 1 1, 2009

[48] URL 2 < https://www.itgovernance.asia/cyber-security-risk-assessments-10-steps-to-cyber-security > (Access: 16.06.2017)

[49] HM Government., 2015 Information Security Breaches Survey, Technical Report, Conducted by PWC and Info Security Europe, 2015

[50] Bulley, A., Moulder, C., Cyber Resilience Capabilities Questionnaire, Bank of England Prudential Regulation Authority, 2015

[51] Chan, H., Mubarak, S., Significance of Information Security Awareness in the Higher Education Sector, International Journal of Computer Applications (0975 – 8887) Volume 60– No.10, December 2012

[52] Future Reserach Nautics., Crew Connectivity 2015 Survey Report, 2015

[53] Richardson, R., 2008 CSI Computer Crime & Security Survey, CSI, 2008

[54] Egan, D., Roberts, F., Report on Cybersecurity Education Project, Command, Control and Interoperability Center for Advanced Data Analysis, June 4, 2014

[55] Gönel, O., Gemi Adami Arz-Talebinin İncelenerek Gelecekteki İstihdam Ve Eğitimin Planlanmasi, İstanbul Teknik Üniversitesi, Yüksek Lisans Tezi, 2013

[56] URL 3, <http://www.surveystar.com/startips/oct2008.pdf>, (Access: 31.10.2019)

[57] URL 4, < aves.akdeniz.edu.tr › ImageOfByte > (Access: 31.10.2019)

[58] Hoyle, R. H., Statistical Strategies For Small Sample Research, Sage, 1999

[59] Hoyle, R. H., Kenny, D. A., Sample Size, Reliability, And Tests of Statistical Mediation, Statistical Strategies for Small Sample Research, Volume 1, pp 195-222, 1999.

[60] Marsh, H. W., Hau, K. T., Confirmatory factor analysis: Strategies for small sample sizes, Statistical strategies for small sample research, Volume 1, pp 251-284, 1999

[61] Tinsley, H. E., Tinsley, D. J., Uses of factor analysis in counseling psychology research, Journal of counseling psychology, Volume 34-4 pp 414, 1987

[62] Anderson, J. C., Gerbing, D. W., Structural equation modeling in practice: A review and recommended two-step approach, Psychological bulletin, Volume 103-3, pp 411, 1988

[63] Ding, L. V., Wayne, F., Harlow, L. L., Effects of Estimation Methods, Number of Indicators Per Factor, and Improper Solutions on Structural Equation Modeling Fit Indices, Structural Equation Modeling: A Multidisciplinary Journal, Volume 2-2, pp 119-143, 1995

[64] Tabachnick, B. G., Fidell, L. S., Principal Components and Factor Analysis, Using Multivariate Statistics, Volume 4,pp 582-633,2001

[65] Hoogland, J. J., Boomsma, A., Robustness Studies in Covariance Structure Modeling: An Overview and a Meta-Analysis, Sociological Methods & Research, 26(3), 329–367, 1998

[66] Boomsma, A., Hoogland, J. J., The Robustness of LISREL Modeling Revisited, Structural Equation Models: Present and Future. A Festschrift in Honor of Karl J{\"o}reskog, VVVolume 2-3, pp 139-168, 2001

[67] Kline, R. B., Methodology in the Social Sciences, Principles and Practice of Structural Equation Modeling (2nd ed.), New York, 2005

[68] Muthen, B. O., Asparouhov, T., Modeling of Heteroscedastic Measurement Errors, Los Angeles, CA: Muthen & Muthen, 2002

Appendix

Survey Items

The Awareness of Cybersecurity – CSA (whether I am aware that…)	
CSA1	I have responsibilities in the security measures taken for the information systems using in the maritime sector
CSA2	There are cybersecurity vulnerabilities in the information systems used in the maritime industry
CSA3	I need to devote some time to solving cybersecurity problems in the information systems using in the maritime sector
CSA4	There are the recommended solutions for security problems of information systems used in the maritime sector
CSA5	There may be cyber-attacks on the information systems used in the maritime industry
CSA6	I may have encountered cyber-attacks on information systems using in the maritime industry
Developing Secure User Behavior – SUB (whether I am willing to…)	
SUB1	To understand terms related to information systems used in maritime industry
SUB2	To follow the rules and regulations on the information systems used in the maritime industry
SUB3	To manage firewalls for the information systems used in the maritime industry
SUB4	To implement strong security policies for the information systems used in the maritime industry (difficult to solve passwords, antivirus systems ... etc)
SUB5	To understand the ways in which cyber-attacks can be done for the information systems used in the maritime industry
SUB6	To detect and prevent cyber-attacks against information systems used in the maritime sector
SUB7	To take security measures of computer-based systems, removable devices, e-mail systems, and the Internet / satellite network of the ship used in the maritime industry
The Education related with Cybersecurity – EDU (Whether it is enough to / for…)	
EDU1	To teach information technology in vocational education
EDU2	For the seafarers working at maritime company to be given information about the results of their access to unauthorized computer systems
EDU3	For seafarers working at maritime company to be educated about the cybersecurity vulnerabilities that can occur during the use of the internet network
EDU4	For seafarers working at maritime company to be informed about the ways to attack the ship against the ship information and communication system
EDU5	To provide training for seafarers in maritime company about their responsibilities for security of information technology.
EDU6	For the seafarers to be trained in order to determine the incidents of cybercrime that might occur in the company
EDU7	To provide training on how to report actual cyber events to computer systems on board
EDU8	To provide training on security measures and technologies related to the computer systems used in maritime company's vessels
EDU9	To provide training to evaluate the security technologies that work with computer systems used in maritime company's ships

Company Rules and Policies about Cybersecurity – RULPOL (whether it is sufficient to…)	
RULPOL1	To conduct a security assessment against the cyber-attack against the information and communication technology systems on board
RULPOL2	To carry out a security plan against the cyber-attack against the information and communication technology systems on board
RULPOL3	To implement the information and communication technology policies for the vessel
RULPOL4	To apply the password creation policy which is hard to break, to predict the usage of information and communication technology on board
RULPOL5	To have experts check the deficiencies of the information and communication technology of vessels
RULPOL6	To have written procedures (guide, instruction, booklet ...) for the use of the information and communication technology of ships
RULPOL7	To apply penal sanctions to the seafarers who does not comply with the security rules of the ship
Sharing of Cybersecurity Information – IS (whether it is enough to / for…)	
IS1	To inform vessels about the cyber-attacks occurred in maritime sector
IS2	To share developments in information and communication technologies in the maritime area with vessels
IS3	For the seafarers to be informed of the action plan to be implemented in emergency situations related to the cybersecurity on a ship
The Influence of the Cyber Attack Experiences – CAE(whether cyber-attacks against ICT systems on vessels have an impact on…)	
CAE1	Habits about using these systems
CAE2	Frequency of security checks of these systems
CAE3	Desire to learn the necessary preventive measures for these systems
CAE4	Ability to use these technologies
CAE5	Ability to follow the developments in cybersecurity