Evaluation of Montenegrin Seafarers' Awareness of Cyber Security

Ivan Mraković, Ranko Vojinović

Topics on maritime cyber security have undoubtedly been attracting great public attention in recent days. The reasons are rapidly evolving computing technologies and digitalization in maritime sector. A successful cyber-attack may have catastrophic consequences and a harmful impact on people, properties or marine environment. In addition to numerous factors that pave the way for a successful cyber-attack on ships, human errors are also in the limelight as they are notorious sources of cyber-attacks today. In this research paper, the authors examine Montenegrin seafarers' level of familiarisation with current cyber-security risks by conducting a structured survey questionnaire. After thoroughly analysing the collected answers, the authors realise that the respondents have an insufficient level of cyber-security knowledge and awareness. Lastly, using the quantitative risk assessment method, the authors propose the best practices for maritime cyber security in the form of implementation of mandatory training course.

KEY WORDS
~ Cyber security
~ Maritime
~ Risk assessment
~ Seafarer
~ Education
~ Cyber-security awareness

Mediterranean University, Faculty of Information Technologies, Podgorica, Montenegro
e-mail: iwanmrak@gmail.com

doi: 10.7225/toms.v09n02.005

This work is licensed under CC BY

1. INTRODUCTION

A successful cyber-attack may be an important issue from the safety, environmental, and commercial standpoints. Cyber security at sea is largely related to critical infrastructures and, therefore, there is an urgent need to do the revaluation of the current awareness and preparedness of crews to adequately respond to maritime cyber risks.

"Maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety, or security failures as a consequence of information or systems being corrupted, lost or compromised" (International Maritime Organization, 2017a). As a matter of fact, modern vessels rely heavily on remote monitoring and automation that can provide porous holes to hackers and cybercriminals, resulting in a compromise of vessel's key components such as ECDIS, VDR, RADAR/ARPA, GNSS, ballast/cargo/engine control systems, which are operated and controlled by the crew. Skills of a crew define how efficiently the systems will work (Yousefi and Seyedjavadin, 2012).

In order to mitigate cyber-security risks and reduce the level of their human dependency, several leading maritime organizations such as e.g. IMO, BIMCO, International Chamber of Shipping developed a set of guidelines. Their purpose is to assist shipowners and vessel operators in reducing the chance of a successful cyber incident, and to recover from it.

BIMCO Guidelines on Cyber Security On board Ships (BIMCO, 2017), EU Regulation 2016/679 (The European parliament and the Council of the European Union, 2016), IMO MSC-FAL.1/Circ.3 (International Maritime Organization, 2017a), ISO 27032:2012, which will be soon replaced by ISO/IEC WD 27032 (ISO, no date),

USCG Policy Letter No. 08-16 (USCG, 2016), TMSA Cyber security guidelines for vessels (TMSA, 2019), UK Department of Transport Code of Practice Cyber Security for Ships (Boyes and Isbell, 2017), USCG Cyber Security Strategy (USCG, 2015) are the most important sources for raising cybersecurity awareness at sea.

Various internationally required training courses, such as Security Awareness Training for all Seafarers or the Marine Environmental Awareness, have already been established. IMO "encourages Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021" (International Maritime Organization, 2017b: 1) which is a great step forward towards achieving global shipping goals.

This research paper sheds a light on why the cyber risks at sea are still not adequately treated from the seafarer-education point of view, even after some very significant events such as hacking of Maersk's assets.

In fact, the hacking of Maersk occurred back in June 2017. At that time, due to successful NotPetya malware attack, the giant company lost between USD 250-300 million, and was forced to reinstall more than 4,000 servers and 45,000 PCs (A.P. Moller - Maersk, 2017; Cimpanu, 2018). Up to date, this has been the most serious attack of its kind, once again confirming that shipping companies are not prepared to respond to cyber risks adequately.

The largest number of safety incidents at sea occur due to human error (Yousefi and Seyedjavadin, 2012). It is no different in cyber security either. Overall situational awareness of the navigator while performing his duties on the navigation bridge consists of spatial, task, and system awareness, including cyber security awareness as well (Hareide et al., 2018). Research (Svilicic, Rudan, et al., 2019) explores cyber-security threatening Integrated Navigational System, stating that cyber-security awareness of crew is satisfying. However, another study (Svilicic, Kamahara, et al., 2019: 10) states that "crew is not familiar with cybersecurity policies, procedures and agreements, and practice insufficient cyber hygiene". More articles assess the IT infrastructure and on-board policies related to cyber-security protection, but only few of them are aimed at defining seafarers' level of awareness and knowledge of cyber threats (Bolat, Yüksel and Yüksel, 2016).

Is the awareness of Montenegrin seafarers of cyber-security high enough to make them a reliable part of the defensive shield to prevent malicious attacks on board vessel? To that end, this research paper carries out the analysis of seafarers' awareness and their knowledge of basic cyber-security aspects, and further weights the findings on a risk scale.

This paper is organised as follows: Section 2 provides an overview of common cyber-security threats at sea and users' best practices. Section 3 deals with current education process of seafarers in Montenegro. Section 4 explains the method of obtaining survey responses, which are assessed in Section 5. Section 6 elaborates the problem solutions. The findings are discussed in Section 7.

2. COMMON CYBER-SECURITY THREATS TO SHIPS AND USER BEST PRACTICES

There is a difference between general maritime security and maritime cyber security. While the topic of the former has been widely explored since the implementation of ISPS Code in 2003, the latter requires further attention.

Various studies have been done to clarify and explore cyber-security risks and threats on vessels. The most important ones are: Witherby Publishing Group, BIMCO, and the International Chamber of Shipping (ICS), 2019.

a. Malware – a malicious piece of code that is utilised by cyber pests to carry out a cyber-attack. The example of malware incorporates viruses, worms, Trojan horses, ransomware, spyware, bots, etc. The malware can steal, delete, encrypt or damage sensitive data without knowledge of the victim. "Malware often infects ship's computers through the crew's use of memory sticks". (Riviera, 2020);

b. Social engineering - technique that manipulates human psychology to get sensitive data. The victim makes mistakes that lead to data breaches. According to the Korean Register of Shipping, "social engineering means to secure access rights to systems, data, and buildings by exploiting human psychology instead of a technical hacking technique to steal into the system". There are different types of social engineering such as:

   a. *Phishing* - combines social engineering and technical methods to trick victims into divulging sensitive information such as identity and financial-related data or anything else that attackers perceive to have value (Furnell, Millet and Papadaki, 2019). Successful phishing attack can create extreme harm, e.g. in case of steeling sensitive information about the ship or itinerary details;

   b. *Spear phishing* - yet another form of phishing. Clicking on the link may cause installation of malicious software, trackers, loss of credentials, personal data or valuable shipping details. Spear phishing is sophisticated and difficult to detect;

   c. The so-called *e-mail spoofing*, still a surprisingly easy technique used for distribution of forged electronic documents that attempt to mislead the recipient about the origin of the message (Hu, Peng and Wang, 2018). Following of e-mail instructions or requests may lead to the loss of sensitive information, e.g. ship's schedule, data on nationality of the crew, etc.;

c. *Distributed denial of service* (DDoS) attack is a kind of cooperative attack model where attackers use many machines to simultaneously launch DoS attacks causing the target's resources

or network band-width to become exhausted or to collapse (Li et al., 2018). On board ship, it can lead to failure of navigational, engineering, and other system.

By conducting a literature research, two main types of best practices for reducing cyber-threat at sea are identified. The first is related to the network arrangement and implementation of various software and hardware solutions, while the second is focused on asset management and user best practices. For the purpose of this research, the authors have identified widely accepted cyber-security best practices whose level of success depends on user behaviour:

a. Use a strong password - Using a strong password can create the main barrier against cybercriminals. A weak password can be guessed within hours. Hackers compromise seafarers' passwords using various techniques such as a Brute-force attack, dictionary attack, and phishing attack. This type of attack can have devastating consequences;

b. Stay vigilant against phishing emails – The seafarer should avoid clicking on any attachment or link from suspicious emails, especially when working on a ship's system or a network;

c. Avoid using removable media - Removable media such as flash drive or smartphone memory card are vulnerable devices and can pose a serious challenge to ship's systems or/and network. Therefore, a seafarer must avoid using flash drives. They should save essential ship-related documents into the cloud drive or a soft copy into a secure personal computer or a laptop;

d. Stay vigilant against SMS attacks - Seafarers often prefer using SIM cards that offer cheap rates and data plans. Today's hackers better understand human psychology and know how to manipulate it. To this end, they send a phishing SMS with a link that involves the cheapest offers on calling and data plans. As soon as the seafarer opens the link, malware is installed on his/her phone. To avoid this nightmare, the seafarer must disregard such SMS or avoid opening unknown links inside it;

e. Avoid using free Wi-Fi - Free offers and gifts often grab everyone's attention, but they can prove detrimental to Seafarer's digital property. Threat actors often cleverly provide free Wi-Fi at ports or its suburbs. The seafarer must not access a free public Wi-Fi hotspot and must avoid putting sensitive credentials;

f. Patching - All the ship's systems should be regularly patched and updated. A patch can fix a security vulnerability and bugs in the software application as well as improve its performance. For example, if an ECDIS is not stable upon installation of new charts, a new patch can resolve the issue.

3. CURRENT EDUCATION PROCESS RELATED TO CYBER SECURITY AT SEA

How does the current educational process in Montenegro look like and is it good enough to suit the needs of today's market?

The education of seafarers in Montenegro is organised in two levels. The first is secondary education, which lasts for 4 years. Upon completion of Maritime High School, a person can choose between two paths - joining a vessel and starting a professional career or enrolling one of the accredited Maritime Faculties in order to get a higher education degree. Enrolment to a university study programme is allowed to anyone who has completed secondary education, even if it is not through Maritime High School. Upon completion of 3-year studies, students get the Bachelor's degree and are allowed to start their seafarer career.

In 2010, Maritime High School in Kotor started carrying out re-qualification courses for all those who had previously obtained a non-maritime high school diploma. Their purpose is to offer an alternative to people who are not interested in higher education and at the same time have no will to study the complete maritime-high-school programme for another 4 years. The re-qualification course plan has been done in accordance

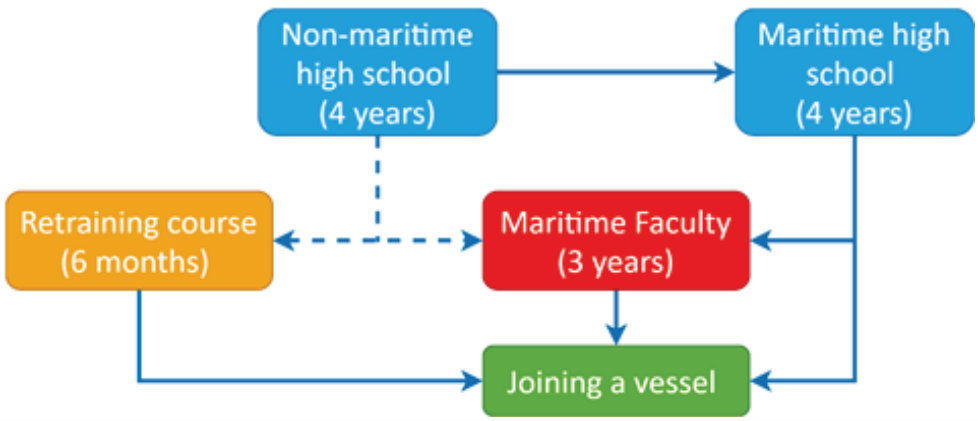

Figure 1.
Education road-map for becoming a seafarer in Montenegro.

with IMO model courses 7.03 - Officer in Charge of Navigational Watch and 7.04 - Officer in Charge of Engineering Watch, and are popular among elder population.

To better demonstrate the official educational path of seafarers in Montenegro, the following scheme has been created (Figure 1). Of course, seafarer education process does not end on finishing Maritime Faculty studies, Maritime High School or a re-qualification course, or on joining a vessel for the first time.

"The Standards of Training, Certification and Watch keeping (STCW) regulations developed by the International Maritime Organization (IMO) lists down the competencies and skills the seafarer should possess"(Sharma et al., 2019: 4). According to legislation in the Republic of Montenegro (The government of Montenegro, 2013, 2017; Ministry of Transport and Maritime Affairs, 2015, 2018), anyone who wants to be a seafarer is required to continue the education process by attending and completing various courses and passing related examinations in front of the Harbour Master's Commission. That is the case in all other countries that ratified the STCW convention.

Besides the previously mentioned IMO model courses 7.03 and 7.04, education plans and programmes of Maritime Faculties are also in line with the IMO model courses 7.01 - Master and Chief Mate and 7.02 - Chief Engineer Officer and Second Engineer Officer. On analysing these model courses, it is clear that the IMO does not require a seafarer to have any knowledge either about IT/OT topics or about cyber security. However, the world leading classification societies DNVGL and Lloyd's Register organise the *E-learning Maritime Cyber Security Course* (DNV GL, no date) and *Cyber and Data Protection Awareness Training* (Lloyd's Register, no date) respectively.

Exploring the current curricula of the above-mentioned educational institutions in Montenegro, one finds that each of them is exploring specific IT fields, most notably the application of software programmes from MS Office – Word and Excel. The use of the Internet and modern maritime technologies such as Radio Frequency Identification (RFID) is addressed to a lesser extent. The Faculty of Maritime Studies of Kotor goes a step further by providing students with an education in the basics of computer networks and network protocols. A deeper study of computer networks as well as their protection has not been addressed so far.

The following sections present a survey done among active seafarers in order to scale their level of awareness of cyber security.

4. SURVEY METHOD

Taking into consideration common cyber threats and best practices presented in Section 2 of this paper, the authors created a structured survey questionnaire. Its purpose is to find out the level of Montenegrin seafarers' awareness and their potential ability to adequately respond to cyber threats.

The total number of active seafarers licensed in Montenegro is 3,000 (official data not published). The research population consists of 429 participants sailing in the rank of deck/engine officer or Master on ocean-going vessels operated by various worldwide reputable companies, including Mediterranean Shipping Company – MSC, Mitsui Ocean Line – MOL, Eastern Mediterranean Maritime, Dabinović, Reederei Nord, Crnogorska Plovidba, Bernhard Schulte Ship Management, CMA CGM, Subsea 7, and others. Even though all the previously mentioned companies employ multinational crews, the conducted survey was limited to seafarers of Montenegrin nationality whose names are undisclosed due to privacy.

The survey questionnaire consists of a total of 18 questions which are presented in Table 3. They are structured in a comprehensive way to enable quantitative research as plausible and affordable method for gathering information from seafarers. The respondents were asked to choose only one answer for each question.

5. RISK ASSESSMENT AND SURVEY RESULTS

To carry out risk assessment, it is necessary to define the key terms at the very beginning: risk, hazard, harm (impact), likelihood, severity, and risk assessment.

There are several definitions of risk. A commonly-used glossary (Committee on Foundations of Risk Analysis, 2015) offers 7 definitions of risk while ISO (ISO, 2009) shortly defines it as the "effect of uncertainty on objectives". "Information security risk comprises the impacts on an organization and its stakeholders that could occur due to the threats and vulnerabilities associated with the operation and use of information systems and the environments in which those systems operate" (Gantz and Philpott, 2013).

"A hazard is a source of potential injury, harm or damage. It may come from many sources, e.g. situations, the environment or a human element."(Maritime and Coastguard Agency, 2019, p. 37)

Harm or impact can be defined as the degree of damage or harm caused to the organisation or an asset.

The likelihood of occurrence is the probability that a cybercriminal will initiate a threat or the probability that a threat could successfully exploit the given vulnerability (ISO, 2009).

Both likelihood and impact can be viewed in either objective or subjective terms. In an objective expression, likelihood and impact could be expressed in terms of numerical values. On the other hand, subjectively, both elements are termed qualitatively or utilizing a range of descriptions on a scale.

Severity is the amount of damage that a hazard could create. For example, the severity of harm can be slight, moderate or extreme.

Risk assessment is a systematic process of determining the number of hazards or threats that could occur in a given amount of time to your computer systems and networks (Prowse, 2017). "The purpose of risk assessment is primarily to support decision-making, including decisions on risk-reducing measures in the context of a structured, systematic and documented process" (Vinnem and Røed, 2020, p. 78). There are two types of risk assessment – i.e. "Quantitative Risk Assessment" and "Qualitative Risk Assessment."

Quantitative risk assessment is a systematic risk-analysis technique used to quantify the risks associated with the IT infrastructure of an organization. It helps in understanding the exposure to risk of the IT environment, employees (or seafarers), corporate assets and its reputation. As said before, this technique involves numerical values. Though Quantitative Risk Assessment is easier, cheaper, and quicker, it cannot give a total asset value for a potential monetary loss. For instance, using this approach we can assign the ranges from 1 to 50 or 1 to 100. If the number is high, the likelihood of occurrence is high. For example, the computer having no firewall or antivirus programme has a high probability of risk.

"Risk analysis methods that use intensive quantitative measures are not suitable for today's information security risk analysis" (Karabacak and Sogukpinar, 2005, p. 148). However, to measure cyber security awareness of Montenegrin seafarers, the authors implemented ISRAM (Karabacak and Sogukpinar, 2005) quantitative risk assessment method as the second most useful in comparison with *SANS, OA, Mehari*, *COBRA* and *FAIR* (Svensson, 2017).

The risk model of *ISRAM* is based on the following formula:

$$Risk = \left(\frac{\Sigma_m[T_1(\Sigma_i w_i p_i)]}{m}\right) x \left(\frac{\Sigma_m[T_2(\Sigma_j w_j p_j)]}{n}\right) \quad (1)$$

where:

i: the number of questions for the survey of probability of occurrence;

j: the number of questions for the survey of consequences of occurrence;

m: the number of participants who participated in the survey of probability of occurrence;

n: the number of participants who participated in the survey of consequences of occurrence;

w_i ; w_j: weight of the question i ; j;

p_i ; p_j: numerical value of the selected answer choice for question i / j;

T_1: the risk table for the survey of probability of occurrence;

T_2: the risk table for the survey of consequences of occurrence;

Risk: a single numeric value for representing the risk.

Note: All the survey participants answered all the questions from the questionnaire. Therefore, *m* is equal to *n*.

On completion of the questionnaire, but before conducting the survey, the authors "weighted" each question to scale their importance in assessing final risk. In other words, not all questions contribute equally to the conclusion of this research. Weight scale is shown in Table 1 for both probability and consequence of cyber-attack.

Table 1.
Weight (importance) of each question for final risk assessment,

Weight value	Probability of occurrence	Seriousness of consequence
3		Severe
2		Normal
1		Low

After designation of answer choices, they are converted into numerical values as shown in Table 2 in order to scale probability and/or consequence of potential cyber accident.

Table 2.
Numerical values of answer choices.

Weight value	Probability of occurrence	Seriousness of consequence
0	Answer has no effect on probability and/or consequence of cyber accident.	
1	Answer is slightly effective to probability and/or consequence of cyber accident.	
2	Answer is considerably effective to probability and/or consequence of cyber accident.	
3	Answer is highly effective to probability and/or consequence of cyber accident.	
4	Answer is extremely effective to probability and/or consequence of cyber accident.	

Further in-depth scaling of questionnaire with probability and consequence weights included is shown in Table 3.

Table 3.
Questions valued for probability and/or consequence, with their respective answer choice.

	Question Weight value of Probability (P); Consequence (C)	Answer choice / Numerical value of answer choice
Q1	Have you ever shared your personal passwords with a colleague? P=3 ; C=3	Yes / 4 No / 0
Q2	Did you know that emails containing attachments are the most common way of cyber-attack? P=3 ; C=3	Yes / 0 No / 4
Q3	Did you know that a displayed web address in an email could be different from the underlying link that it will direct to? P=2 ; C=3	Yes / 0 No / 4
Q4	Did you know that "From" field in an email can be manipulated to show any trusted email address? P=2 ; C=2	Yes / 0 No / 4
Q5	Did you know that NMEA 0183 protocol has no encryption? P=2 ; C=3	Yes / 0 No / 4
Q6	Is it safe to open any email while anti-virus is running? P=2 ; C=3	Yes / 4 No / 0
Q7	Do you know what DDoS attack is and how it can disrupt or slow down ship's IT systems or network services? P=2 ; C=3	Yes / 4 No / 0
Q8	In your opinion, are crew members an important factor in terms of cyber-security vulnerabilities of on-board systems? P=N/A ; C=2	Yes / 0 No / 4
Q9	Have you ever heard about the social engineering attacks on seafarers and about their ways of manipulation of seafarers to break the vessel's security procedures to gain access to critical systems or networks? P=2 ; C=3	Yes / 0 No / 4
Q10	How do threat actors use a Short Messaging Service (SMS) to infect the mobile device of seafarers? P=1 ; C=2	By sending fake links / 0 By sending suspicious attachments / 0 I do not know / 4
Q11	Usually, how many different sites do you visit while browsing web when you are off duty? P=1 ; C=N/A	More than 10 / 4 Between 6-9 / 3 Between 3-5 / 2 Less than 3 / 1
Q12	How much time do you spend connected on ship's WI-FI network, daily? P=2 ; C=2	More than 6 hours / 4 Between 3-5 hours / 3 Between 1-3 hours / 2 Less than 1 hour / 1
Q13	Are you using Administrator or Normal user account to log on into ship's PC? P=2 ; C=3	Administrator / 4 Normal user / 1
Q14	Do you regularly update PC? P=2 ; C=3	Yes / 0 No / 4
Q15	Do you know the adverse effects of seafarers' Bring-Your-Own-Device (BYOD) on board? P=2 ; C=2	Yes / 0 No / 4

Q16	Patching, updating and maintaining of ship's navigation system (e.g. ECDIS) is always crucial. Does your company have these security controls in its cyber-risk assessment plan? P=2 ; C=3	Yes / 0 No / 4
Q17	Is it true that a cyber-incident can go unnoticed for a substantial period and does not have to involve an obvious system fault or alarming ransomware messages? P=2 ; C=3	Yes / 0 No / 4
Q18	What is the typical sign that your vessel's IT/OT infrastructure is cyber-attacked? P=2 ; C=3	System is slow or unresponsive / 0 System displays warnings and alarms to inform the user about an on-going cyber-attack / 4 I do not know / 4

The minimum and maximum probability of cyber incident can be scaled based on survey results by using the equation (2):

$$\sum_i w_i p_i \tag{2}$$

Calculations are presented in Table 4, where possible survey values are grouped evenly and scaled to represent the probability level of risk parameter.

Table 4 is the risk table constructed for the probability of cyber-security incident parameter. As per Table 4, maximum possible value for survey result is 136, while minimum value is 5. For the purpose of this research, the interval of 'very high probability' is set to 27, while for other scales it is set to 25.

Using the same principle and replacing *i* with *j* in equation (2), the authors obtained the minimum and maximum values of the survey output to measure the consequences of cyber incident (Table 5).

Table 4.
Risk table representing probability of cyber incident upon survey results.

Survey result	Qualitative scale	Quantitative scale [T1]
5-30	Very low probability	1
31-56	Low probability	2
57-82	Medium probability	3
83-108	High probability	4
109-136	Very high probability	5

Table 5.
Risk table representing consequences of cyber incident upon survey results.

Survey result	Qualitative scale	Quantitative scale [T2]
2-37	Negligible consequences	1
38-73	Minor consequences	2
74-109	Important consequences	3
110-145	Serious consequences	4
146-184	Very serious consequences	5

Table 5 is the risk table constructed for the consequence of cyber-security incident parameter. As per Table 5, the maximum possible value for the survey result is 184, while the minimum value is 2. For the purpose of this research, the interval of 'very high probability' is set to 38, while for other scales it is set to 35.

Quantitative risk matrix used for this research is presented in Table 6. It is a modified version of the risk matrix which is frequently seen on board merchant vessels and is widely used for risk assessment of daily tasks (Maritime and Coastguard Agency, 2019). Multiplying quantitative values of probability and consequences, the final value of the risk is obtained.

Table 6.
Risk matrix.

Likelihood of harm (probability - P)	**Severity of harm (consequences - C)**				
	1 = Negligible	2 = Minor	3 = Important	4 = Serious	5 = Very serious
1 = Very low	1 = Very low risk	2 = Very low risk	3 = Very low risk	4 = Low risk	5 = Low risk
2 = Low	2 = Very low risk	4 = Low risk	6 = Low risk	8 = Medium risk	10 = Medium risk
3 = Medium	3 = Very low risk	6 = Low risk	9 = Medium risk	12 = Medium risk	15 = High risk
4 = High	4 = Low risk	8 = Medium risk	12 = Medium risk	16 = High risk	20 = Very high risk
5 = Very high	5 = Low risk	10 = Medium risk	15 = High risk	20 = Very high risk	25 = Very high risk

Once the previous steps were completed, questions were distributed to 638 people who are active seafarers. Out of that number, 429 people fully responded to the questionnaire. Due to space constraints, Table 7 represents an extract of all the collected data, with average calculated probability [T1] and consequences [T2] of risk.

Calculated risk based on the conducted-survey questionnaire, by application of fundamental risk equation (1) is 11.18, which can be described as medium level risk.

Table 7.
Survey results.

Respondent # m *[m=n]*	Probability of cyber incident $\sum_i w_i p_i$, where $i = 429$	T1	Consequences of cyber incident $\sum_j w_j p_j$, where $j = 429$	T2
Respondent # 1	88	4	88	3
Respondent # 2	96	4	128	4
Respondent # 3	80	3	116	4
Respondent # 4	48	2	68	2
Respondent # 5	80	3	80	3
…	…	…	…	…
Respondent # m	…	…	…	…
…	…	…	…	…
Respondent # 429	72	3	76	3
	$\left(\frac{(\sum_m [T_1 (\sum_i w_i p_i)])}{m}\right)$ =	3.26	$\left(\frac{(\sum_m [T_2 (\sum_j w_j p_j)])}{n}\right)$ =	3.43

6. SOLUTIONS

Maritime industry is being rapidly digitalised, and IT is playing a crucial role in this regard. Before knowing how to prevent cyber-attacks, it is essential to know how these attacks are detected. Typically, seafarers are unaware of the attack and remain oblivious until a real loss occurs. It is indispensable for seafarers not only to adopt and understand new technologies, but also to keep themselves abreast of threats and attacks in the face of the ship's IT infrastructure.

Based on the conducted quantitative survey and ISRAM risk assessment methodology, authors measured the risk level of cyber-security awareness of Montenegrin seafarers. Rated as a medium-level risk, it can be treated as a clear indicator of necessity of urgent actions.

The human factor is always crucial when it comes to the cyber security of a ship, and this is also an important subject of this research paper. To that end, the authors proposed a model of the training course that should be set as mandatory for all crewmembers. The model course is presented in Table 8. The proposed training course should be set mandatory for all crewmembers, and it should continue in form of refresh courses on a regular 5-year basis. Implementation into the existing IMO model course 3.27 – Security awareness training for all seafarers, is also possible.

As per Table 8, the course should consist of 8 topics and should last for 8 hours, out of which 2.5 hrs are dedicated to demonstration purposes.

Table 8.
Proposed model course for cyber-security awareness.

	Topic	Duration in hrs	
		Theory	Demonstration
1.	Introduction to cyber security	0.5	
2.	SMS vs. cyber security – IMO requirements and legal framework	0.5	
3.	Identification of threats – Types of cyber-attack (DDoS, Phishing, etc.)	1.0	1.0
4.	Identification of vulnerable shipboard systems (IBS, engine/cargo/ballast control systems and NMEA 0183 standard)	1.0	
5.	Cyber-security risk assessment	0.5	0.5
6.	Measures for prevention and detection of cyber-attack – technological and behavioural	1.0	1.0
7.	Reporting cyber attacks	0.5	
8.	Conclusion	0.5	
	TOTAL	8,0 hrs	

Proposed training would educate Montenegrin Seafarers about ship's IT security policies, procedures, and best practices that are required to better work in a ship's IT environment.

Security familiarisation training is also essential before joining the ship's duties. The Shipboard familiarisation checklist should be expanded to include cyber-security related training, which should be performed by the Ship Security Officer or an equally qualified seafarer. Familiarisation process should be adequately structured to guide a newly joining seafarer how to report a security incident, how to act in IT security-related emergencies and to explain which security solution is required in the event of a cyber-security incident.

7. CONCLUSION

In the world of digital warfare, the global shipping community including vessels, ports, terminals and various other facilities are relying heavily on the Internet to establish connectivity. Automated equipment, GNSS, ECDIS, AIS, engine/ballast/cargo control systems, and consignment tracking systems are just some of the items dependent on adequate cyber security.

Policies and procedures on board ships should be structured and planned, accompanied by an appropriate IT infrastructure including firewalls, anti-malwares, etc. Ship's IT infrastructure is vulnerable to cyber-attacks, and human error can play its part in

this regard. Therefore, achieving the overall cyber security of the ship is out of the question without a proper and effective training of seafarers. The conducted risk assessment based on survey questionnaire implicitly shows that human resources are a hot topic in terms of cyber security on board ships.

Montenegrin seafarers are mostly novices with regard to IT and cyber security. In addition, they have not acquired any IT and cyber-security related education from shore-based institutions either. For example, neither Maritime High Schools nor Maritime Faculties in Montenegro are providing any sort of education about cyber security at sea. Thus, maritime cyber security of Montenegrin seafarers is not up to the mark and needs urgent attention.

Therefore, a holistic approach to cyber security should start with the increase of people's awareness and focusing of knowledge on the mindset with appropriate training. If their training is planned to make them aware and ready to act on any threat, there is no doubt that the overall risk will be significantly reduced.

Implementation of the authors' proposed training course would set a milestone on security at sea. The proposed model course in cyber-security awareness would help in protecting confidentiality, integrity, and accessibility of information through various measures relating to people, processes, and IT systems on board ships.

Further research should focus on developing unique teaching syllabus of cyber security that will suit the needs of both Montenegrin seafarers and their employers.

REFERENCE

A.P. Moller - Maersk, 2017. Interim Report Q3 2017. Available at: https://investor.maersk.com/static-files/1226cd7b-d1b4-4281-b42c-5f032b0e1595.

BIMCO, 2017. The guidelines on cyber security onboard ships, Version 3, available at: http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16.

Bolat, P., Yüksel, G. & Yüksel, S., 2016. A Study For Understanding Cyber Security Awareness Among Turkish Seafarers. The Second Global Conference on Innovation in Marine Technology and the Future of Maritime Transportation. Bodrum: Union of Chambers of Turkish Engineers and Architects – The Chamber of Marine Engineers of Turkey, pp. 278–279.

Boyes, H. and Isbell, R., 2017. Code of Practice Cyber Security for Ships. London: Institution of Engineering and Technology.

Cimpanu, C., 2018. Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack, Bleeping Computer. Available at: https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/, accessed on: 7 December 2018.

Committee on Foundations of Risk Analysis, 2015. Society for Risk Analysis Glossary. Available at: https://www.sra.org/sites/default/files/pdf/SRA_glossary_20150622.pdf.

DNV GL (no date) Maritime Cyber Security Awareness E-learning. Available at: https://www.dnvgl.com/maritime/maritime-academy/cyber-security-elearning.html, accessed on: 23 February 2020.

Furnell, S., Millet, K. & Papadaki, M., 2019. Fifteen years of phishing: can technology save us? Computer Fraud & Security, 2019(7), pp.11–16. Available at: http://dx.doi.org/10.1016/s1361-3723(19)30074-0.

Gantz, S. D. and Philpott, D. R., 2013. FISMA and the Risk Management Framework. Available at: http://dx.doi.org/10.1016/c2010-0-66566-7.

Hareide, O.S. et al., 2018. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. Journal of Navigation, 71(5), pp.1025–1039. Available at: http://dx.doi.org/10.1017/s0373463318000164.

Hu, H., Peng, P. & Wang, G., 2018. Towards Understanding the Adoption of Anti-Spoofing Protocols in Email Systems. 2018 IEEE Cybersecurity Development (SecDev). Available at: http://dx.doi.org/10.1109/secdev.2018.00020.

International Maritime Organization , 2017a. MSC-FAL.1/Circ.3: Guidelines on maritime cyber risk management. Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3 - Guidelines On Maritime Cyber Risk Management (Secretariat).pdf.

International Maritime Organization, 2017b. MSC.428(98): Maritime cyber risk management in safety management systems. Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution MSC.428(98).pdf.

ISO, 2009. ISO/Guide 73:2009 Risk management — Vocabulary. Available at: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en, accessed on: 20 February 2020.

ISO, no date. ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity, 2012. Available at: https://www.iso.org/standard/44375.html, accessed on: 24 February 2020.

Karabacak, B. & Sogukpinar, I., 2005. ISRAM: information security risk analysis method. Computers & Security, 24(2), pp.147–159. Available at: http://dx.doi.org/10.1016/j.cose.2004.07.004.

Li, C. et al., 2018. Detection and defense of DDoS attack-based on deep learning in OpenFlow-based SDN. International Journal of Communication Systems, 31(5), p.e3497. Available at: http://dx.doi.org/10.1002/dac.3497.

Lloyd's Register, no date. Cyber and data protection awareness training. Available at: https://www.lr.org/en/training/cyber-security-training/, accessed on: 23 February 2020.

Maritime and Coastguard Agency, 2019. Code of Safe Working Practices for Merchant Seafarers. London: TSO. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/848506/Code_of_safe_working_practices_for_merchant_seafarers_COSWP_2019.pdf.

Ministry of Transport and Maritime Affairs, 2015. Rulebook on the types of ranks and competencies, requirements for obtaining ranks and issuing certificates of competencies for crew members of seagoing ships. Official Gazette of the Republic of Montenegro, 15(51).

Ministry of Transport and Maritime Affairs, 2018. Rulebook amending the Rulebook on the types of ranks and competencies, requirements for obtaining ranks and issuing certificates of competencies for crew members of seagoing ships. Official Gazette of the Republic of Montenegro, 15(51), 16(44), 63

NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Available at: http://dx.doi.org/10.6028/nist.cswp.04162018.

Prowse, D. L., 2017. CompTIA Security+ SY0-501 Cert Guide, Pearson Education.

Riviera, 2020. Ships are riddled with malware. Available at: https://www.rivieramm.com/opinion/opinion/ships-are-riddled-with-malware-28356.

Sharma, A. et al., 2018. Computer Supported Collaborative Learning as an Intervention for Maritime Education and Training. Advances in Human Factors in Training, Education, and Learning Sciences, pp.3–12. Available at: http://dx.doi.org/10.1007/978-3-319-93882-0_1.

Svensson, L., 2017. Evaluation of quantitative assessment extensions to a qualitative risk analysis method. Linköping University. Available at: http://www.ep.liu.se/.

Svilicic et al., 2019. A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. Journal of Marine Science and Engineering, 7(10), p.364. Available at: http://dx.doi.org/10.3390/jmse7100364.

Svilicic, B. et al., 2019. Maritime Cyber Risk Management: An Experimental Ship Assessment. Journal of Navigation, 72(5), pp.1108–1120. Available at: http://dx.doi.org/10.1017/s0373463318001157.

The European parliament and the Council of the European Union, 2016. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

The government of Montenegro, 2013. Law on Safety of Navigation. Official Gazette of the Republic of Montenegro, 13(62).

The government of Montenegro, 2017. Law Amending the Law on safety of navigation. Official Gazette of the Republic of Montenegro, 13(62), 14(06), 15(47), 17(71).

TMSA, 2019. Cyber security guidelines for vessels. Available at: https://www.shipownersclub.com/media/2019/01/TMSA-3-Cyber-Security-On-board-ships-1217.pdf.

USCG, 2015. United States Coast Guard Cyber Strategy. Available at: https://www.work.uscg.mil/Portals/6/Documents/PDF/CG_Cyber_Strategy.pdf?ver=2016-10-13-122915-863.

USCG, 2016. CG-5P Policy letter No. 08-16: Reporting suspicious activity and breaches of security. Available at: https://homeport.uscg.mil/Lists/Content/Attachments/2676/CG-5P Policy Letter 08-16_3.pdf.

Vinnem, J.-E. & Røed, W., 2020. Offshore Risk Assessment Vol. 1. Springer Series in Reliability Engineering. Available at: http://dx.doi.org/10.1007/978-1-4471-7444-8.

Witherby Publishing Group, BIMCO and The International Chamber of Shipping (ICS), 2019. Cyber Security Workbook for On Board Ship Use (eBook). 1st Ed. Witherby Publishing Group.

Yousefi, H. & Seyedjavadin, R., 2012. Crew Resource Management: The Role of Human Factors and Bridge Resource Management in Reducing Maritime Casualties, TransNav, International Journal on Marine Navigation and Safety of Sea Transportation.