University of Piraeus

SPOUDAI
Journal of Economics and Business
Σπουδαί
http://spoudai.unipi.gr

A Study about the Role of the Human Factor in Maritime Cybersecurity

Thanasis Pseftelis[a], Gregory Chondrokoukis[b]

[a]Ph.D. Candidate, Dept. of Industrial Management and Technology,
University of Piraeus, Greece, Email: pseftelis@unipi.gr
[b]Professor, Dept. of Industrial Management and Technology,
University of Piraeus, Greece, Email: gregory@unipi.gr

Abstract

Shipping is the sector of the economy via which approximately 85% of all world trade is transported and which is technologically developing with enormous leaps. Its digital transformation has highlighted new opportunities, but at the same time new threats. Due to the great demand from the maritime community for digital operations (specifically digitization and automation), maritime cyber security is becoming an issue of utmost importance. A protection framework through which shipping can be shielded against cyber-threats is absolutely necessary.

As hackers are becoming increasingly aware of cyber-vulnerabilities within the maritime sector and shipping is undoubtedly a key pillar of the Greek economy, this study fills the existing gap by presenting a survey carried out within the Greek maritime community with the aim to investigate the human factors and the awareness stakeholders have about maritime cybersecurity.

Our detailed research resulted in two main findings. Firstly, it was found that the basic principles of security (availability, integrity, confidentiality) and the related information and communication technologies (ICT) have not been adequately understood in order to be protected from cyber-attacks. Secondly, our perception that the human factor can contribute to maritime cybersecurity in a positive or negative way was confirmed.

JEL classification: L86, L92
Keywords: Cybersecurity, human factor, maritime, empirical research

1. Introduction

It is clear that despite the great number of environmental and economic challenges facing international shipping, the majority of world trade, is carried out in the sea. The world fleet consists of container vessels, bulk carriers, tankers, passenger vessels, small cargo vessels etc. Various technologies have been internationally developed to provide safe and reliable

navigation, communication and management. The standards for these technologies are based on the International Convention for Safety of Life at Sea (SOLAS 74) which is constantly revised as circumstances change and new technologies are developed. These systems consist of a combination of onshore and maritime technologies.

While interconnectivity between ships, and onshore devices has improved the operational and the physical safety, it has also enabled an increase of cyber-attacks. Generally, a system is considered functioning, or broken. *With cyber-attacks, the traditional distinction between functioning and broken systems is blurred since a non-functioning system may not be broken, and a functioning system may not be trustworthy*.

In 2011 the European Union(E.U.) Agency for Cybersecurity(ENISA) published a report (Enisa, 2011) on the cyber security challenges in the maritime sector. The initiative of this study was the assumption that the maritime sector activity relies on ICT and is exposed to a lot of cyber-threats. For this reason, ENISA, carried out an analysis to find the gaps linked to ICT systems so that the highest security level could be achieved.

The report was based on data collected via desk research, individual interviews, and questionnaires which were completed during a workshop in Belgium. Stakeholders from both public and private sectors were contacted and asked to share their views on this subject. The key findings of this workshop were that *the maritime cyber-security is at a low to non-existent level* due, among others, to the small number of known cyber security incidents, no publicity for them, and absence of mechanisms to identify the incidents.

In addition, the report proposes:

- the implementation of cyber security campaigns and training actions for the various parties involved.
- the implementation of security strategies for Maritime Information and Communication Technologies (security by design).
- addition of cyber security to maritime policies.
- identification and registration of critical goods in the maritime sector.
- establishment of common security policies between the European Union and the International Maritime Organization (IMO).
- better exchange of information between the parties involved.

According to what we know so far and the relevant studies almost 80% of the maritime casualties are caused, at least in part, by human error. This assumption also applies to the maritime cyber security. In this context, training and awareness-raising is needed to prevent cyber-attacks in order for the shipping personnel to be able to identify and eliminate the cyber-threats (Enisa, 2011).

Taking into account these findings, a survey was conducted with the cooperation of 86 employees of the maritime sector in Greece. This survey focuses on the contribution of the human factor in terms of maritime cyber-security and on whether directives and good practices are accepted.

In this context, two pilot applications (expert system shell, Prolog web application) and a questionnaire were created. Our survey also contains the following:

- the fundamental concepts of cyber-security
- information security guidelines of the IMO
- good practices of the international maritime union
- an original research work presenting a framework for assessing the vulnerabilities of ships in relation to their cyber-security

- the NIS Directive of the European Union
- related publications of vulnerabilities, to create appropriate questions

This study contributes, through the confirmation of research cases, to a better understanding of the issues which need attention, to increasing general cyber risk knowledge and helping the maritime community in strategically reducing risks against both known and potential threats.

In conclusion this paper consists of the literature review, the description of the methodology, the results of our research with an explanatory discussion and the conclusion that contains suggestions for future studies.

2. Literature Review

2.1 Basic Terms

Since maritime technologies are essential for the smooth operation in the seas, their cyber-vulnerabilities are of interest to many potential attackers. Thus, it is important to be aware of the effects of likely cyber-attacks and whether the attacker's aim is to misguide, confuse, deter, or damage. In order to address the issue of potential safety successfully and to fully comprehend the environmental and

commercial consequences of a cyber incident. It is also essential to go through the

basic terms which will help us towards a better understanding of an appropriate

approach in implementing cyber risk management.

Cyber-security is defined as (NIST, 2019) "The ability to protect or defend the use of cyberspace from cyber-attacks."

A Cyber-attack is defined as (NIST, 2019) "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment / infrastructure or destroying the integrity of the data or stealing controlled information."

Cyber safety incidents (BIMCO, 2018) can arise as the result of:

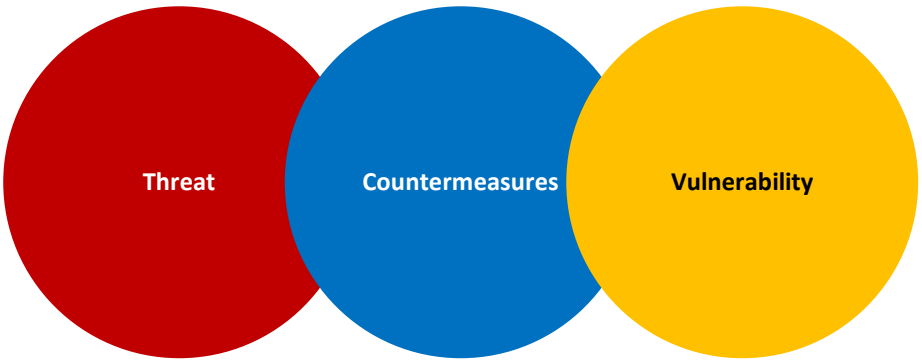
- a cyber security incident, which affects the availability and integrity of Operational technology (OT), for example corruption of chart data held in an Electronic Chart Display and Information System (ECDIS)
- a failure occurring during software maintenance and patching
- loss of or manipulation of external sensor data, critical for the operation of a ship – this includes but is not limited to Global Navigation Satellite Systems (GNSS).

A threat is defined as (NIST, 2019) (Figure 1) "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability."

Countermeasures are defined as (NIST, 2019) (Figure 1) "Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system."

A vulnerability is defined as (NIST, 2019) (Figure 1) "A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."

Figure 1 : Threat – Countermeasures – Vulnerability



The elements that require protection are people, data, processes and technologies. The value of the above resources is determined by the owners themselves.

2.2 International Maritime Organization

IMO has a high interest in maritime safety. Its main role is to examine the various potential risks that could lead to the disruption of the smooth operation of the ships and to pollution incidents.

In 2017, the guidelines for the management of maritime cyber risks were issued (IMO, 2017). It was suggested that cyber risks be appropriately addressed in existing safety management systems, as defined in the International Safety Management Code (ISM Code) no later than the first annual verification of the company's Document of Compliance certificate (DOC) after 1 January 2021 (IMO - MSC, 2017). The ISM Code applies to the owner or anyone who assumes responsibility for the operation of the ship, otherwise both owners and operators (if different) will need to comply.

Nearly all of the international shipping community is required to comply with the ISM Code, as respective countries are parties to SOLAS. Therefore, to comply with the ISM Code, internationally voyaging vessels must address cyber risks within their safety management systems.

2.2.1 Cyber Risk Management

According to the IMO Guidelines on maritime cyber risk management, "*the goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.*" (IMO, 2017)

The cyber risk management is divided into five steps:

identify, protect, detect, respond and recover.

These five functions were selected because they represent the five primary pillars for a successful and holistic cybersecurity program. They aid organizations in easily expressing

their management of cybersecurity risk at a high level and enable their risk management decisions.

- *Identify*
  The Identify Function assists in developing an organizational understanding of the managing of the cybersecurity risks to systems, people, assets, data, and capabilities.
- *Protect*
  The Protect Function outlines appropriate safeguards to ensure the delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.
- Detect
  The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables the timely discovery of cybersecurity events.
- Respond
  The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.
- Recover
  The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports the timely recovery to normal operations, thus reducing the impact of a cybersecurity incident.

2.3 The Baltic and International Maritime Council (BIMCO)

The Baltic and International Maritime Council (BIMCO) is the largest of the international shipping associations representing shipowners. Its membership controls around 65 percent of the world's tonnage and it has members in more than 120 countries, including managers, brokers and agents.

It has published "The Guidelines on Cybersecurity on Board Ships" (BIMCO, 2018). The purpose of this text is to guide shipowners and managers in a set of actions in the field of cyber risk management, which will contribute to increasing the security of systems of the ships and of the companies.

The Guidelines on Cyber Security Onboard Ships are aligned with IMO's guidelines and provide practical recommendations on maritime cyber risk management covering both cyber security and cyber safety by using a six- step procedure as follows: identify threats, identify vulnerabilities, assess risk exposure, develop protection and detection measures, establish contingency plans, respond to and recover from cyber security incidents.

2.4 MACRA: Maritime Cyber-Risk Assessment

The Maritime Cyber-Risk Assessment (MaCRA) is a model-based framework for maritime cyber-risk assessment (Tam, 2019). A framework has been developed for the quantification and promotion of maritime cyber risks. To demonstrate plausibility, intentional cyber-attacks are extrapolated from past accidents that occurred due to similar system vulnerabilities.

In order to capture threats, the systems are categorized into the following:

- Navigation systems
- Positioning systems

- Communication and Networking systems
- Cargo and Machinery management systems
- Human Factor

As it has been stated, maritime casualties may be due to acts or omissions of the human factor. The lack of cybersecurity training makes the human factor a potentially easy target, which under certain conditions can constitute a major threat to the ships and the environmental safety.

2.5 Well-known vulnerabilities

The technologies have various vulnerabilities, which exposed them to cyber-attacks. The most well-known vulnerabilities concerning the maritime cyber-security are the following.

2.5.1 Electronic chart display and information system – ECDIS

ECDIS displays the nautical charts for the design and view of the ship's course. The relevant software package is installed on an operating system, which is placed on the bridge. ECDIS has at least three sensors (position, compass and speed), and it can be updated via portable storage media (USB) or via the Internet using e-mail. It is usually connected to the other ships systems and sensors.

ECDIS is a complex, safety-relevant, software-based system with multiple options for display and integration. The ongoing safe and effective use of ECDIS involves many stakeholders including seafarers, equipment manufacturers, chart producers, hardware and software maintenance providers, shipowners and operators, and training providers.

In 2009, IMO recognizing the advantages of electronic charts for navigation made their carriage mandatory. Relevant regulation entered into force on 1 January 2011, making ECDIS mandatory for new ships and also phasing-in the requirement for its installation in existing ships.

However, in a network simulation environment (Svilicic B., 2019) of six ECDIS stations, by using the Nessus Professional vulnerable finding tool (Nessus, 2020), it was found that ECDIS is an ideal environment for executing malicious code. This was caused by the fact that the software package was running on operating systems that no longer accept upgrades (e.g. Windows 7, XP, etc.), resulting in a plethora of known vulnerabilities making these systems easy targets.

2.5.2 Automatic identification system – AIS

Since 2004, the IMO has established the Automatic Identification System (AIS) (IMO, AIS, 2000), on ships with a specific capacity and on all passenger ships. Its contribution is to collision avoidance, traffic control and search/rescue in the event of an accident. It automatically provides information on a screen, about the vessel (identity – IMO number, port of departure - arrival, etc.) without the involvement of the personnel on the ship or the seamen having watch on the bridges of other ships in the area and at the coastal stations. The system transmits messages through electromagnetic waves.

The information transmitted is in plain text. The AIS protocols do not provide mechanisms to ensure the integrity of the message or its encryption. Malicious users can intercept messages or transmit messages that contain misleading information and false fact (Kessler G.C., 2018).

2.5.3 Global Navigation Satellite System - GNSS

The Global Navigation Satellite System - GNSS (EGSA, 2017) displays the position of the ship. GNS is based on satellites providing signals from space and transmitting data to GNSS receivers. The criteria that determine its reliability are accuracy, integrity, continuity and availability. It is considered the most vulnerable system after the AIS. In addition to natural phenomena, it is exposed to jamming and spoofing attacks. Jamming attacks can be achieved through commercially available low-cost devices. Spoofing attacks are more complex, as satellite signal simulation with greater power should be achieved (Awan & Al Ghamdi, 2019) (M., 2018).

2.5.4 Navigation Telex - NAVTEX

NAVTEX is an internationally offered service aiming at the dissemination, of navigational and meteorological urgent information concerning the shore / sea areas in relation the ships (Navy, Hellenic, 1986). The information is gathered automatically and printed directly by telex so that each ship must have a device for receiving messages transmitted at specific frequencies.

In this context it is a service that provides safety information on shipping and meteorological issues. The messages are also available through web pages (Sedov, 2020).

NAVTEX may face dangers from interference, from the storage devices, from the Internet and form the other connected systems. The consequences of these threats are the incorrect reception of messages or the interruption of the service (Kevin Jones, 2018).

2.5.5 Voyage Data Recorders - VDR

A Voyage Data Recorder (VDR) is a piece of equipment fitted onboard ships that records the various data on a ship and can be used for the reconstruction of the voyage details and vital information during an accident investigation (IMO, 2002).

IMO defines VDR as a complete system, including any items required to interface with the sources of input signals, their processing and encoding, the final recording medium, the playback equipment, the power supply and the dedicated reserve power source. Information related to the speed, the direction, the position, the engine, the fuel, and the conversations of the last 12 hours are recorded.

Information is stored in a secure and retrievable form and relates to the position, movement, physical status, and command and control of a ship during and following an incident. This information is used during any subsequent safety investigation to identify the cause(s) of the incident. Aside from its usage in accident investigation, it can also be used for preventive maintenance, performance efficiency monitoring, heavy weather damage analysis, accident avoidance and training purposes to improve safety and reduce running costs.

Furthermore, a ship’s VDR is far superior to the black box of the airplanes as it stores a variety of data for not less than a period of 12 hours. The data records covering the last 12 hours are continuously overwritten by the latest data.

From the incidents that have occurred so far, it has been established that it is exposed to malicious actions of people operating inside the ship (intruders) (University Carnegie Mellon, 2016) (Kaspersky, 2016). This is also supported by the fact that it is not usually connected directly to the Internet, but to a Local Area Network (Ethernet) that connects it to other vulnerable systems or devices. The security of VDR has exposed weaknesses, such as weak encryption, insecure authentication, and non-updated firmware (IOActive, 2016)

2.5.6 Sailing Directions

Sailing Directions (Pilots) provide essential information to support port entry and coastal navigation for all classes of ships at sea (IMO SD, 1985). In their 76 volumes, one can find the world's main commercial shipping routes and ports.

Each volume of the Sailing Directions offers:

- Information on navigational hazards, buoyage, pilotage, regulations, general notes on countries, port facilities, seasonal currents, ice and climatic conditions. This information, when used alongside official charts, can help to increase situational awareness on the bridge.
- High quality diagrams and photography to help bridge-crews understand critical information during the passage planning stage.
- Worldwide official coverage to support safe and compatible navigation within main commercial shipping routes and ports. This coverage is split across 76 volumes for purchase flexibility.

They supplement the Electronic Navigational Charts (ENC) used by ECDIS, with details that contribute to the safety of the ship in relation to the course to be followed during her journey.

2.5.7 Global Maritime Distress and Safety System - GMDSS (IMO GMDSS, 1992)

The Global Maritime Distress and Safety System (GMDSS) is the technical, operational and administrative structure for maritime distress and safety communications worldwide. It was established in 1988 by the IMO and it was implemented globally between 1992 and 1997. GMDSS establishes the radiocommunications equipment that ships are required to carry, how this equipment shall be maintained and used, and it provides the context within which governments should establish the appropriate shore-based facilities to support GMDSS communications.

In the old days, vessels in distress relied almost exclusively on their ability to alert other ships in order to obtain assistance by using their radio equipment. GMDSS, for the first time, changed this procedure and established a new fundamental principle that a ship in distress should send its alert to a shore, which would then accept the responsibility of coordinating the necessary rescue efforts. Thus, GMDSS became inextricably linked to the parallel implementation of the International Search and Rescue Convention (SAR Convention) and the development of shore facilities within the structure of the World-Wide SAR Plan.

In addition to improving the capability of ships to declare their distress and receive assistance coordinated from the shore, GMDSS also provided for the broadcast of essential safety-related information – Maritime Safety Information (MSI) – which could be received automatically on-board ships at sea and would offer ships the chance to navigate more safely on a routine basis.

A number of vulnerabilities related to individual systems have been identified (Kevin Jones, 2018).

2.5.8 Long Ranged Identification and Tracking - LRIT

The Long-Range Identification and Tracking System (LRIT) provides information related to the ship's identity (EMSA, 2009). Due to the use of Satellite communications only, it provides a relatively safer data transfer. It plays a vital role in the search and rescue missions, together with GMDSS. The most likely attack that it can receive is the Denial of Service (DoS).

2.5.9 Phishing

Phishing is a type of social engineering attack often used to steal user data (Enisa, 2016). It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link or file, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

In shipping various applications are used by the management operating officers and the sailors in order to carry out their work. A typical example is the e-mail applications that have a prominent place in the daily operation of the ship, since usually a large volume of communication is done through them. The phishing attack is one of the most important challenges that only humans can successfully stop. In this regard training is the best way to mitigate the risks from phishing attacks.

3. Methodology

As mentioned above, training and awareness-raising is essential to prevent cyber-attacks for the shipping personnel to be able to detect and eliminate cyber threats. In this respect, the role of the human factor in maritime cybersecurity needs to be investigated. The lack of data makes its valuation impossible. In this study, a questionnaire based on known vulnerabilities was created. The aim was to focus on the contribution of the human factor in terms of maritime cyber-security and whether directives and good practices are well-known.

Research Questions:

RQ1 Maritime cybersecurity is at a low level.

RQ2 The contribution of human factor at maritime cybersecurity is crucial.

A survey of 37 items (Forms by Microsoft, 2020) was created. It was sent via personal messages to one hundred ten (110) shipping employees. Eighty-six (86) of them responded.

Eight (8) were masters - engineers, twenty-three (23) were managers, twenty-four (24) were technicians and thirty-one (31) were shipowners, agents, and other personnel.

For the valuation of our research questions, the well-known maritime vulnerabilities were taken into account, through the following questions:

1. How can you update the electronic chart display and information system (ECDIS)?
    a. Email b. Usb Stick c. Email & Usb Stick d. Wrong Answers
2. What is the electronic chart display and information system (ECDIS)?
    a. Software b. Operating System c. Software & OS d. Wrong answers
3. What is affected in relation to cybersecurity in case of data transmission via AIS for a ghost ship?

    a. Availability b. Integrity c. Availability & Integrity d. Wrong answers
4. What is affected in relation to the cybersecurity when the AIS device is out of order?

    a. Availability b. Integrity c. Availability & Integrity d. Wrong answers
5. What is affected in relation to the cybersecurity in case of attack via spoofing or jamming?

a. Availability b. Integrity c. Availability & Integrity d. Wrong answers

6. The NAVTEX messages are available through

   a. radio waves b. Internet c. radio waves and Internet d. Wrong answers

7. How can we connect to the data collecting unit?

   a. Ethernet b. USB c. Ethernet & USB 4. Wrong answers

8. Do you need to check the sailing directions before a voyage?

   a. Yes b. No

9. Does the GMDSS have any vulnerabilities?

10. Do you think the LRIT (long ranged identification & tracking) can be attacked via DOS (Denial of Service)?

    a. Yes b. No

11. Do you know what the phishing is?

    a. Yes b. No

The above questions were also available through an online application, developed using the Prolog programming language, which was evaluated by the participants with 4.2 out of 5 (Prolog, Pseftelis, 2020).

The demographic elements of the participants regarding their gender, age, education and job are shown in Tables 1, 2, 3 and 4 respectively.

Table 1: Gender of the participants

Male	*Female*
76.7 %	23.3%

Table 2: Age of the participants

Age group	*Frequency*
20-30	12.8 %
30-40	22.1 %
40-50	36.0 %
50-60	17.4 %
60+	11.6 %

Table 3: Education of the participants

Education	*Frequency*
High school	7.0 %
University	48.8 %
Master - PhD	44.2 %

Table 4: Job of the participants

Job Position	*Frequency*
Deck- Engine Crew	9.3%
Administrative	26.7%
Marine Inspector	27.9%
Other (shipowners, agents etc.)	36.0%

4. Results

Based on the above, the results are as follows:

4.1 RQ1 Maritime cybersecurity is at a low level

The report of the ENISA for shipping (Enisa, 2011) considers that the cyber security is at a low level. This report was the reason for the formulation of the first research question.

A quantitative variable was created which gathers the overall score for each respondent, from a set of ten-unit questions, on identified vulnerabilities of maritime systems in relation to cyber-security (Figure 2).

The purpose is to control the average value of the variable, with a control value of seven. This value is chosen because several cyber-security certifications (EC-Council, 2020) require a score of more than or equal to 70% for their successful acquisition.

The cases are as follows:

- H_0: $\mu = 7$ (the mean value of the respondents' score is 7)
- H_1: $\mu \neq 7$ (the mean value of the respondents' score is different from 7)

The appropriate statistical test is the One Sample T-test parametric control, which requires a normal distribution. The lack of normality ($p = 0{,}001 < 0{,}050$) leads us to the use of the Wilcoxon Signed-Rank test (IBM, 2020).

The non-parametric check rejects the null hypothesis ($p < 0.050$). The mean value of the respondents is different from 7 (figure 3).

Furthermore, the comparison of the means between independent groups of the job position, can be achieved with the Kruskal-Wallis test.

The cases are as follows:

- H_0: $\mu1 = \mu2 = \mu3 = \mu4$ (all 4 populations are equal)
- H_1: at least one of the *4* population means is not equal to the others

The non-parametric check cannot reject the null hypothesis ($p = 0.842 > 0.050$). There is no statistical evidence that the associated population means are significantly different (figure 4).

Figure 2: Maritime Cybersecurity is at a low level

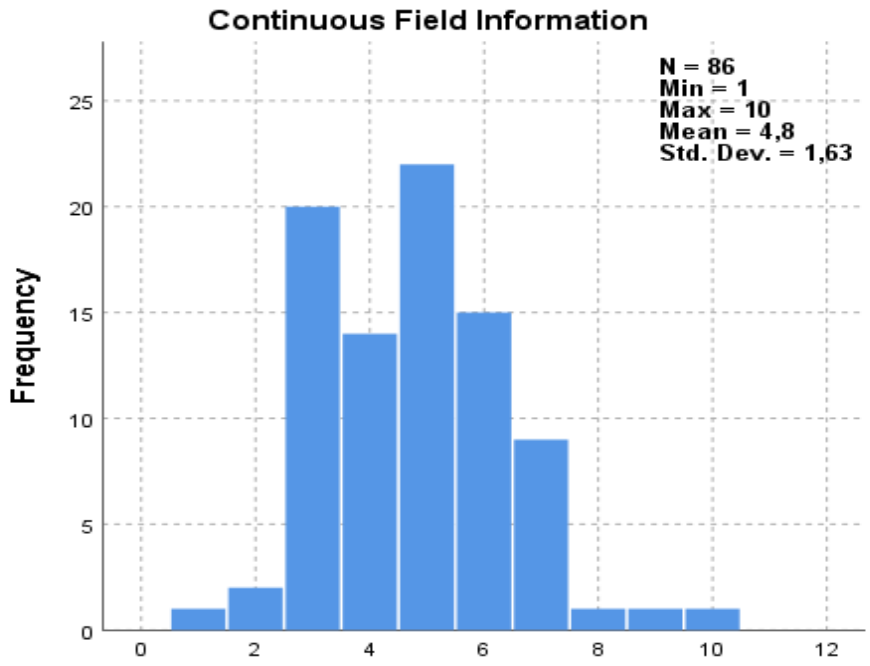


Figure 3: Maritime Cybersecurity is at a low level

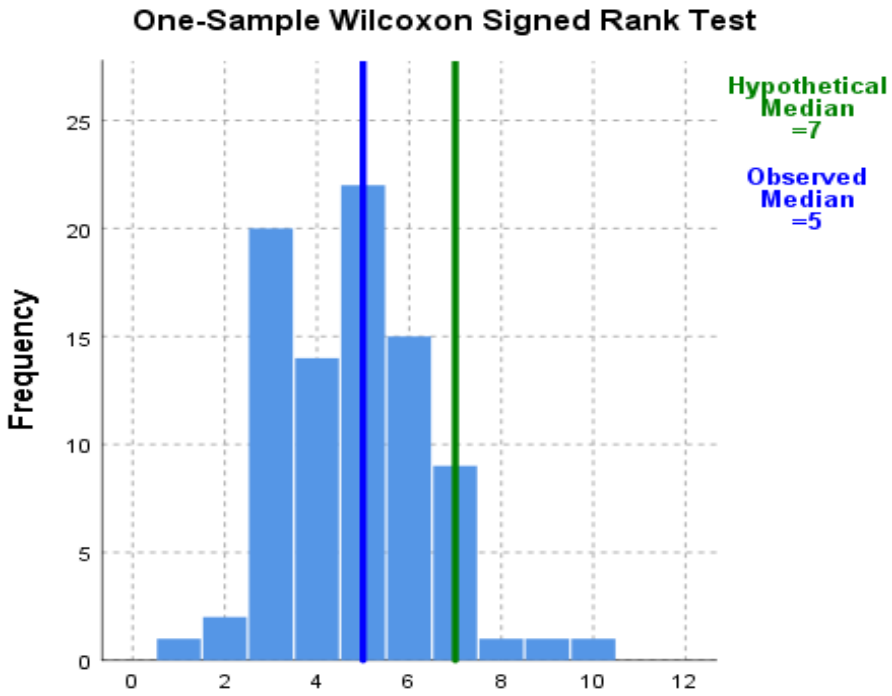
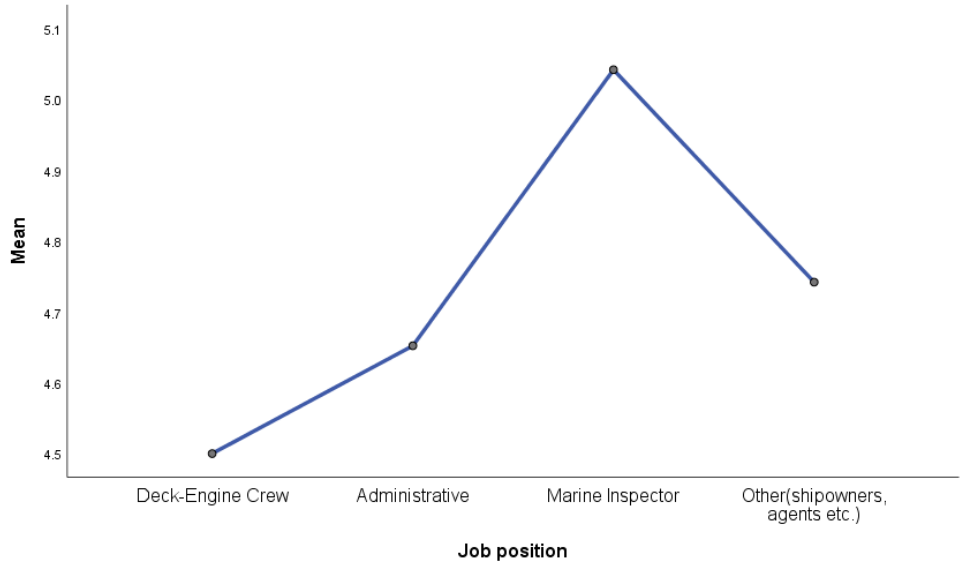


Figure 4: Mean values for the job position



Finally, the randomness of the quantitative variable values through the non-parametric Runs Test (p = 0.396> 0.050) is pointed out (NIST, 2013).

4.2 RQ2 The contribution of human factor at maritime cybersecurity is crucial

This question arises as a general finding of all organizations dealing with maritime cyber-security issues.

To investigate RQ2, x^2 (chi - square) independence tests (Kent State Universtity, Chi Square Test, 2020) were conducted between the questions and the demographics of the participants, with a probability value α = 0,050.

Table 5: Chi-square Tests

	Age group	*Education*	*Job position*
Q1	.221	.013	.099
Q2	.075	.363	.342
Q3	.244	.024	.567
Q4	.620	.067	.244
Q5	.300	.703	.315
Q6	.508	.281	.585
Q7	.993	.670	.637
Q8	.845	.083	.389
Q9	.886	.297	.285
Q10	.847	.993	.228

The variables, which meet the test criteria, are independent and it is proved that the demographics elements do not determine how the respondents answered the questions. The contribution of human factor at maritime cybersecurity is crucial.

5. Discussion

5.1 RQ1: Maritime cybersecurity is at a low level

The well – known (identified) vulnerabilities were collected from the relevant publications and from the categorization of the ship's systems listed in the literature review. The mean (average value) of responses is 4,8 (one unit per question - total ten questions). This value is far from the values required by the various certifications (EC-Council, 2020), which ensure that the user has a minimum level of knowledge that makes him capable against cyber-attacks.

Based on the data, the research hypothesis "Maritime cybersecurity is at a low level" could not be disproved. Difficulties in grasping basic concepts of cyber security (such as availability and integrity) and in basic systems on the safety of the ship are apparent in the shipping workers' responses.

5.2 RQ2: The contribution of the human factor at maritime cybersecurity is crucial

Chi - square tests were carried out to investigate this research question. The existence of independence between the majority of questions and demographics (job position or age), confirmed the research question. The human factor can make a decisive contribution, whether positive or negative, to maritime cybersecurity.

In the first question "How can you update the electronic chart display and information system (ECDIS)?", the majority (6 out of 10) know that the ECDIS upgrade can be done either via USB flash drive or via web. The existence of a procedure specifying the frequency of the upgrade time by the competent persons is a necessary step to shield it. Finally, the answers given by the participants are independent of their age group.

In the second question "What is the electronic chart display and information system (ECDIS)?", the majority (8 to 10) do not know that the ECDIS is software. This is probably due to the way it is structured on the ship's bridge, making it exposed to threats that exploit vulnerabilities of outdated operating systems. The answers of participants are independent from their job position.

In the third question "What is affected in relation to cybersecurity in case of transmission of data via AIS for a ghost ship?", the majority (7 to 10) do not know one of the basic concepts of cyber - security, the integrity (integrity - the resource can be modified only by an authorized person). The answers of the participants are independent from their job position.

In the fourth question "What is affected in relation to the cybersecurity when AIS device is out of order?", the majority (9 to 10) does not know one of basic concepts of cyber - security, the availability (availability –the resource can be used by all authorized persons). It was not possible to check whether or not there was independence between the question and a demographic element.

In the fifth question "What is affected in relation to cybersecurity in case of attack via spoofing or jamming?", the majority (6 out of 10) answered correctly. Based on the previous two questions (3 and 4), the concepts of integrity and availability are not clear to the participants. The answers of participants are independent from their job position.

In question six "The NAVTEX messages are available through", the majority (7 out of 10) answered wrongly. NAVTEX messages are also available via the Internet and not only via radio waves. The answers of the participants are independent from their job position.

In question seven "How can we connect to the data collecting unit?", half of the participants answered correctly. The connection to this critical system, which is the black box of the ship,

is done through USB port or Ethernet cable. The answers of the participants are independent from their age group.

In question eight "Do you need to check the sailing directions before a voyage?", almost all of the participants answered correctly. It was not possible to check whether or not there was independence between the question and a demographic element.

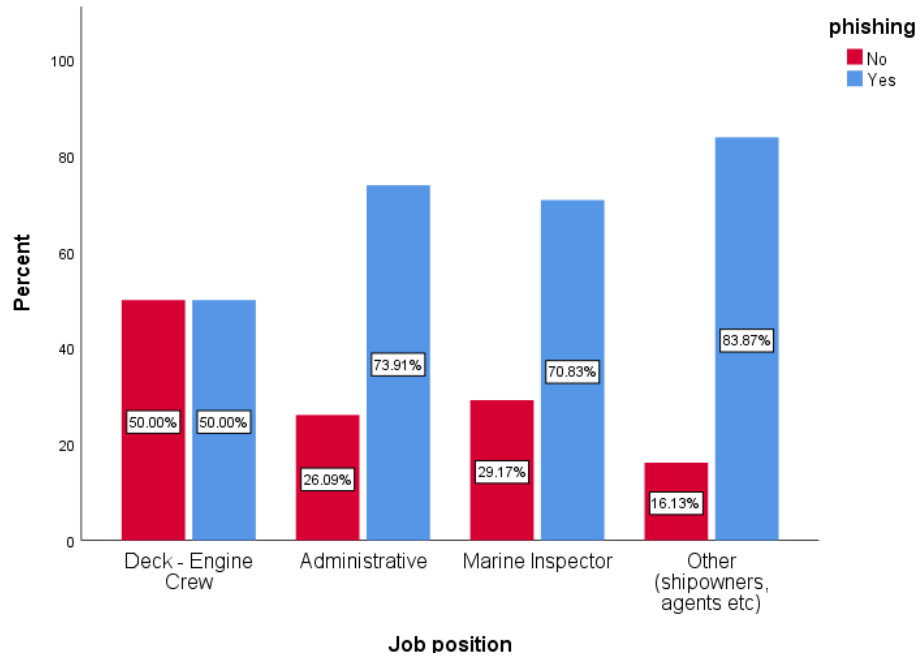
In question nine "Does the GMDSS have any vulnerabilities?", half of the participants answered correctly. It is important that participants recognize the existence of potential vulnerabilities in the various critical systems, the purpose of which is to ensure human life and avoid marine pollution. The answers of the participants are independent from their age group.

In the tenth question "Do you think the LRIT (Long Ranged Identification & Tracking) be attacked via DOS (Denial of Service)?", the majority (7 out of 10) answered correctly. Participants understand the case of system failure, which makes them potentially receptive to the concept of DoS. The answers of the participants are independent from their job position.

5.3 Phishing

When asked "Do you know what the Phishing is?", 74.42% said they were aware of this type of attack (Figure 5).

Figure 5: Clustered bar chart for phishing and job position



Since phishing is the first step in most cyber-attacks, it is good that participants are aware of the attack. Spam emails, which have a malicious link or a malicious attachment, seek access to the recipient's computer.

Organizations need to continuously train their personnel to enable them to recognize malicious emails (Enisa, 2016).

6. Conclusion

Due to the lack of data for Greece capable of describing the current situation, a pilot web application and a survey were developed. They were answered by 86 shipping employees in order to assess the role of the human factor in the cyber-security, in terms of its level, its contribution and whether directives and good practices are well known.

This study found that *maritime cybersecurity is at a low level*. The human factor has a crucial role to play, and it can contribute to this field. As a part of the resources, the human factor is the most valuable. It can support various processes such as to updating the outdated operating systems and software, configuring networks and systems and supporting the recovery plans.

Furthermore, the shipping companies must create massive cybersecurity campaigns for their employees. Relevant policies, guidelines and best practices are tools that help them understand the issues. The cooperation between the participants of the sector is very important for the success of the maritime cybersecurity.

The development of a larger empirical research and of a framework that assesses the knowledge of the human factor and its level is a necessary future step for the systematic study of maritime cybersecurity.

References

IMO SD, 1985. [Online]
Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/Charts.aspx

IMO - MSC, 2017. [Online]
Available at:
http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf
[Accessed September 2020].

Awan, M. & Al Ghamdi, M., 2019. Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS). *J. Mar. Sci. Eng.*, 7(10).

BIMCO, 2018. *https://www.bimco.org/*. [Online]
Available at: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
[Accessed September 2020].

EC-Council, 2020. [Online]
Available at: https://www.eccouncil.org/programs/certified-secure-computer-user-cscu/
[Accessed September 2020].

EGSA, 2017. *https://www.gsa.europa.eu/*. [Online]
Available at: https://www.gsa.europa.eu/european-gnss/what-gnss
[Accessed September 2020].

EMSA, L., 2009. [Online]
Available at: http://www.emsa.europa.eu/lrit-main/lrit-home/how-it-works.html
[Accessed September 2020].

Enisa, 2011. *https://www.enisa.europa.eu*. [Online]
Available at: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

Enisa, P., 2016. [Online]
Available at: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing

Enisa, P. o. t. r., 2017. [Online]
[Accessed September 2020].
Forms by Microsoft, P., 2020. [Online]
Available at: https://forms.microsoft.com/Pages/ResponsePage.aspx?id=497I2YtVPUi1AtMfoMsk3g33scHLTLZHvNBLjMJl_9pUNUJBSUpUNzgxQUJISkdMQk1ONDhWMFBTTi4u
[Accessed September 2020].
IBM, O. S. W. T., 2020. [Online]
Available at: https://www.ibm.com/support/pages/can-spss-statistics-produce-one-sample-wilcoxon-test
[Accessed September 2020].
IMO GMDSS, 1992. [Online]
Available at: http://www.imo.org/en/OurWork/Safety/RadioCommunicationsAndSearchAndRescue/Radiocommunications/Pages/Introduction-history.aspx
IMO, AIS, 2000. *http://www.imo.org.* [Online]
Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx
IMO, 2017. *http://www.imo.org.* [Online]
Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf
[Accessed September 2020].
IMO, V., 2002. [Online]
Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/VDR.aspx
IOActive, 2016. [Online]
Available at: https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/
[Accessed September 2020].
Kaspersky, 2016. [Online]
Available at: https://www.kaspersky.com/blog/ship-black-boxes-vulnerability/10957/
[Accessed September 2020].
Kent State Universtity, Chi Square Test, 2020. [Online]
Available at: https://libguides.library.kent.edu/SPSS/ChiSquare
[Accessed September 2020].
Kessler G.C., C. J. H. J., 2018. A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System.. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 12(3).
Kevin Jones, K. T., 2018. [Online]
Available at: https://www.c-mric.com/wp-content/uploads/2018/06/Kevin_Cybersecurity2018.pdf
LRIT, I., 1974. [Online]
Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/LRIT.aspx
M., F., 2018. Foundations of GNSS Spoofing Detection and Mitigation with Distributed GNSS SDR Receiver.. *the International Journal on Marine Navigation and Safety of Sea Transportation*, 12(4).
Navy, Hellenic, 1986. [Online]
Available at: https://www.hnhs.gr/en/2015-05-28-16-58-21/2015-05-28-16-59-41/navtex
Nessus, 2020. *https://www.tenable.com/products/nessus/nessus-professional.* [Online].
NIST, 2019. [Online]
Available at: https://doi.org/10.6028/NIST.IR.7298r3
[Accessed September 2020].
NIST, R. t., 2013. [Online]
Available at: https://www.itl.nist.gov/div898/handbook/eda/section3/eda35d.htm
[Accessed September 2020].

Prolog, Pseftelis, 2020. [Online]
Available at: http://cybermaritime.tex.unipi.gr
Sedov, K., 2020. [Online]
Available at: http://www.navtex.lv/navtex/MainTable
Svilicic B., B. D. Ž. S. K. D., 2019. Raising Awareness on Cyber Security of ECDIS.. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 13(1).
Tam, K. J. K., 2019. MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU J Marit Affairs* .
University Carnegie Mellon, 2016. [Online]
Available at: https://www.kb.cert.org/vuls/id/820196/
[Accessed September 2020].