Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 6 Issue 12, December - 2019

The New Cyber Security Framework in Shipping Industy

A.Dimakopoulou
Dept. of Industrial Design and Production Engineering
University of West Attica
Athens, Greece

N.Nikitakos
Dept. of Shipping Trade & Transport,
University of Aegean
Greece

I. Dagkinis
Dpt. of Shipping trade & Transport
University of Aegean,
Greece

Th. Lilas
Dpt. of Shipping trade & Transport
University of Aegean
Greece

D.Papachristos
Dept. of Industrial Design and Production Engineering
University of West Attica
Athens, Greece

M.Papoutsidakis
Dept. of Industrial Design and Production Engineering
University of West Attica
Athens, Greece
mipapou@uniwa.gr

***Abstract*— In the world of information and electronic data sharing, the need for security is increasing. The business world is increasingly interested in Cyber Security. It is a fact that technology is evolving at a very fast pace and this makes it more difficult for people to adapt to it. The shipping industry is a part of the business world that is at risk every day and is a global concern. IMO, by adopting regulations, aims to contribute to enhancing security in the maritime cyberspace. The shipping companies also follow the guidelines of BIMCO is aligned with the IMO and are covered by the ISM track and insurance. Also important is the role of Classification societies who play a more consultative role to this subject of the moment. Finally, the purpose of this paper is to answer specific questions that focus on Greek shipping and Cyber Security. Consequently, a quantitative survey is carried out on company's managers and shipowners the questions relate to the processes and regulations applied by companies and how they manage to strengthen their systems.**

Keywords*— *Cyber security; Cyber Security in Shipping; data protection; data security; information security; risk management; risk assessment; confidentiality; integrity; availability; security systems; security management system; threats; penetration test; resilience; classification societies; regulations; procedures; safety management standards

I. INTRODUCTION

Entering the digital age is a fact and the need for Cyber Security is growing over time [28]. Everyday incidents of personal data and information breaches lead to finding solutions and practical methods related to this issue [28], [31]. Services, organizations, and everyone, are now more suspicious of Internet attacks and the security of personal data. This global trend that is becoming a habit in people's daily lives will be dealt with below in the field of shipping.

Shipping is a global superpower and it is not a coincidence that Cyber Security has come in this area too [3], [22]. In addition to several regulations that apply to other organizations, additional regulations apply to shipping which are designed to safeguard information in particular when communicating between ships and ashore [30]. This makes it more difficult to implement Cyber Security in this area. One reason that mandatory regulations and procedures on Cyber Security are now in place is the case with Maersk, a company that is the largest container carrier in the world [5], [19]. Maersk had said that expected losses were between $ 200- $ 300 million, due to a major shutdown of their system that was simply the result of a virus that managed to infiltrate the system causing the company to temporarily shut down all critical systems that had been infected [5]. It is obvious that in this sector it is more difficult to achieve security than in other sectors that do not utilities satellite internet communication [19], [21]. Also, the issue of security will be a long-time concern because 100% security cannot be achieved [27].

II. BACKGROUND

The presence of the “Cyber” everywhere is expansive [29]. The importance of the issue is highlighted in national security business and the Internet, shipping and maritime transport [1], [2], [4], [22]. Understanding security policy is a key part of achieving Cyber Security and this is achieved by taking cyber-attack prevention measures, understanding the contexts and regulations as well as the impacts [30].

The development of technology and the interaction of people with it is an important factor for continuous training in new technologies [29], [27]. This means that isolation is not an option, but it is important to understand the risks to information security and addressed them [30], [31]. This is achieved by perceiving and managing business threats through risk assessment processes based on IMO-approved regulations and guidelines such as BIMCO [13]. Also considering the precautionary measures a company must take and the costs and time it will take to respond to a threat [29], [30]. On the other hand, the EU has been applying the GDPR Regulation since May 2018 [17]. This regulation concerns the protection of personal data and is mandatory. Risks usually come from motivation and fall into two categories. The natural hazards associated with the environment and the hazards of human activity [23], [27]. Usually, the human factor uses malware that penetrates even the most up-to-date systems, usually using the key clerk to carry out the attack finding the endpoint security problem [27]. The end point is every employee who has access to the information system across the network [27].

Situations that put people at risk dealing with business infrastructure, the environment, scientific and technological tools that help detect, prevent, recover, mitigate and repair the impact of such situations [26], [27]. In addition, training human factor in Cyber Security is probably the most important [20], [27]. Maritime safety is a key to world trade [13], [22]. The transportation of extremely large goods in shipping is based on cybernetics and infrastructures that control them by examining the vulnerabilities and threats of the systems, while the importance of staff training [18], [22] on the automation of ship systems and their interactions with the office [3], [19]. That is why regulations have been adopted which are now applied by companies, some are necessary, and others are not. In any case, they help to strengthen their systems [6], [7], [8], [9], [10], [11], [12], [13], [14], [15].

In this context the following shipping regulations are listed:

- IMO-MSC

The IMO has issued relevant guidelines contained in MSC-FAL.1 / Circ.3 for the management and security of marine cyberspace. The guidelines of IMO provide high-level recommendations on cyber-management in shipping in order to safeguard shipping against current and emerging cyber-threats and vulnerabilities [7].

- BIMCO

Provides some guidelines for controlling cyber security in shipping [13].

- GDPR

Is the General Data Protection Regulation (GDPR).

This determines:

1) Protecting privacy and data security.

2) Valid for all EU Member States from 25 May 2018.

3) The era of "Big Data" aims to harmonize various data protection laws across the EU [14], [15].

- TMSA3 in case of tankers

TMSA 3 is the tanker rating system and regarding cyber security in tankers mentions element 13 of TMSA 3 and is mandatory from 1 January 2018 [11].

- VIQ 7

The Vetting Inspection Questionnaire (VIQ) deals with inspections of the highest importance on fuel and chemical tankers. In the case of Shell, BP etc. VIQ is required. Special emphasis is placed on Chapter 7 of the Regulation (VIQ version 7.0.05, 2019) in relation to Cyber security. This is a questionnaire that should be answered correctly by the company in such inspections [12].

- IACS

On Cyber security in shipping IACS has made some recommendations on cyber security. The IACS recommendations stem from extensive industry-wide collaboration and provide much needed guidance on how to develop and maintain the Cyber Security of vessels.

- ISO 27001 (optional)

ISO 27001 provides the minimum requirements for information security management. It is targeted at security executives in an organization. It describes a common basis for developing levels of security within the organization, effectively managing information security, and building trust in transactions between organizations. This standard is not above the legal requirements of each country and any system applied to companies should combine the requirements of the standard with the legal requirements of each country [9].

A. Cyber Security Review

According to ENISA it is mentioned “Is there a need for a definition? Cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers. Therefore, a contextual definition, based on one that is relevant, fits, and is already used a particular SDO or organisation should be considered. This document provides recommendations for stakeholders and policymakers, for terminology and for SDOs.” This means that cybersecurity cannot be accurately translated through a definition. Concerning the security of personal data and information. However, it cannot be covered by a simple definition. Finally, if necessary, to give this a definition Cyber security according to the oxford dictionary is defined as: “The state of protection against criminal or unauthorized use of electronic data or the measures taken to achieve this objective.” But again, it gives us a generalized view of the subject.

Another definition [3] says that "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." It follows that it should be known that what is directly affected by a cyber-attack is the network based on the IP address of the computers [4]. Cybercriminals try to infiltrate the systems using malware that includes viruses, worms, spyware and Trojans [31]. Companies need to be prepared to apply new technologies and train their staff to be able to understand the consequences of an attack [30], [31].

B. Cyber Security in Maritime Industry

Cyber Security in maritime industry is the protection about personal data when communicating ships with shore. This is done by regulations and requirements that they come from organizations that they make this on shipping [28].

As part of the ISM and IMO, regulations and procedures have been put in place to help companies strengthen their systems and provide appropriate training to staff on cyber security [6], [7], [8]. Another regulation is the GDPR concerning data protection and has been mandated by an EU directive [14], [15]. In addition, the IACS has also adopted 12 cyber security recommendations [10]. Tankers apply TMSA 3 and VIQ 7 mandatory [11], [12]. Finally, companies on their own initiative can comply with ISO 27001 which provides the minimum requirements for cyber security of an organization [9]. Of the above regulations and procedures some are mandatory and others not but with one common goal and that is Cyber Security.

Shipping companies apply cyber security procedures and their systems are divides into two categories. OT systems that control the physical world and IT systems that handle data [18], [19]. OT systems are different from traditional IT systems. The OT system is hardware and software that directly monitors / controls physical devices and processes. On the other hand, the IT system covers a range of information processing technologies, including software, hardware and communication technologies [18], [19].

Companies, for the better use of their systems and to avoid errors and consequently attacks, are guided either by their own trained staff or with the help of classification societies who now play consulting roles or even by third party consulting companies. The above are a guideline from BIMCO that covers a very large and important part in terms of security [13]. They are also covered by insurance as long as they follow the guidelines properly and have their staff well trained to avoid frivolous errors that can occur and cost the company [24], [25].

In the figure below we look at the Cyber Security management approach as outlined in the BIMCO guidelines [13].

Fig. 1. *Cyber risk management approach as set out in the guidelines [13]*

This paper presents a quantitative research in collaboration with DNVGL. Questionnaires have been sent and managers of shipping companies in Greece have been invited to respond. This presents results for Cyber Security in shipping. If companies follow the required procedures, if they are properly prepared about regulations, how they manage a threat, how protected they feel, etc.

III. METHODOLOGY

In the present paper the method used in conducting the research is the quantitative methodology. Quantitative research is carried out using a questionnaire and the data are analyzed statistically [16]. The questionnaire was sent to executives of major Greek shipping companies. These executives make up the management of the company, HSQE department, the legal and IT department. 87 questionnaires were sent out of which 39 of them were answered. Thus, research can be described as a small empirical study that records the views of employees in positions of responsibility. The present research applies the quantitative methodology which is based on the positivism philosophy. The data collected in response to the survey questions are collected by means of a questionnaire using the sampling method. In quantitative methodology we have a productive approach [17]. Also, this research is descriptive in that it answers questions in a specific time period (June - July 2019) [17].

A. Propose and Research objectives

The purpose of this paper is to study the implementation of cyber security in shipping. Is therefore to answer the following research questions:

a) Which procedures and regulations followed for the organization of shipping companies in relation to Cyber Security?

b) To examine Cyber Security System Empowerment Factors.

c) To investigated of attacks.

B. Research Tool

The research tool used was the use of a questionnaire embedded in Google forms and then emailed to the respondents. Subsequently, the results were processed in one place of using SPSS and the rest were Descriptively answered due to the type of questionnaire.

C. Some Common Mistakes.

IV. DATA ANALYSIS

Since the survey, were received 39 responses from 89 questionnaires , which is about 50%. The questionnaire was divided into 4 chapters. the chapters relate to respondents' personal information, company personal information, company information on cybersecurity and finally how important the data given to them in chapter 4 was. The first three of these chapters were descriptively analysed while the last chapter about the importance of the questions for the companies of the respondents was analysed using the SPSS program. This was because these questions were based on a Likert scale ranging from 1 “very important” to 5 “not at all important”.

A. Respondents' Personal Informations

1) Age Group

TABLE I. AGE GROUP

Age Group	Answers
25-39	25.6%
40-59	61.5%
60+	12.8%

The TABLE I above shows that the age group with the most answers is 40-59 years old with 61,5%. Followed by the 25-39 age group with 25,6% which means that more and more young people are taking responsibility positions in the companies. Finally, the age group of 60+ exists at a very low rate of 12,8% and we could say that it is significant due to the many years of experience in shipping.

2) Job Position in The Company

TABLE II. POSITION HELD IN THE COMPANY

Position Held in The Company	Answers
DPA	2
HSQE	4
Technical Department	20
IT Department	8
Managing Director/ CEO/ COO	5
Ship-Owner	1
Other	1

B. Company's Personal Informations

1) Kind of Vessels

TABLE III. KIND OF VESSELS

Kind of Vessels	Answers
Bulkers	26
Tankers	19
Containers	7
Gas Carriers	3
Other	1

2) Age of Company's Vessels

TABLE IV. AGE OF VESSELS

Age of Vessels	Answers
1-5	0
5-10	28
10-15	9
15+	2

3) Number of Company's Vessels

TABLE V. NUMBER OF VESSELS

Number of Vessels	Answers
1-5	3
6-15	16
16-25	5
25+	15

C. Survey Results about Cyber Security

1) Research Objective1: Procedures and Regulations

Regarding on the first research objective about the procedures and regulations applicable to Greek shipping companies, the research questions of this survey are listed in the following table.

TABLE VI. RESEARCH OBJECTIVE 1

	Research Questions
Research Objective 1	1.1 Does the company have documented privacy policies and procedures in place for the management of personal data and who is its manager?
	1.2 Significance of the Guidelines that companies follow to achieve cyber security.

Approximately 92% of the sample population applies a documented cyber security policy to their company. This policy is based on regulations and procedures that either necessarily apply or play a guiding role in them. The regulations are IMO, ISO

27001,GDPR TMSA3, BIMCO guideline etc. Corporate mentoring is done internally in combination with the IT and HSQE departments. This is done by specialized staff with the exception of a small percentage (about 8%) using external companies to meet this goal. Also, a majority of about 54% find it important to be able to prove documented policy in relation to these procedures at any time. Finally, risk assessment and risk management are implemented at regular intervals and in this way they can prevent or manage an attack. Risk management and risk assessment are part of the regulations.

2) Research Objective 2: System Strangthening Agents

Regarding on the second research objective about the strengthening factors of shipping companies' communication systems, the research questions of this survey are listed in the following table.

TABLE VII. RESEARCH OBJECTIVE 2

	Research Questions
Research Objective 2	Do companies apply up-to-date new firewall technologies and firewalls to avoid threats?
	How much does staff training influence the strengthening of the company's Cyber Security system?
	Do companies apply risk assessment and risk management?

Companies are trying to strengthen their systems by applying modern technologies as well as up-to-date firewalls and find it very important to be able to ensure that the company is secure with about 67%. Another factor is the control of their suppliers as well as access to the company's system with rates of about 95% and 60% respectively. Also, staff training is another factor in strengthening their systems and may even be considered to be the most important factor with about 95% of the responses. in addition, they carry out risk assessment and management of about 72%, penetration tests on their systems to prevent attacks at about 50%, and find it important to record policies and procedures and review about 82%. Finally, they consider it very important to identify agents at about 87% upon entry into the system and to have a system in place to enhance their systems and be able to react quickly in the event of 90% and 98% respectively.

3) Research Objective 3: Investigation of Attacks

Regarding on the third research objective about the investigation of attacks to the shipping companies, the research questions of this survey are listed in the following table.

TABLE VIII. RESEARCH OBJECTIVE 3

	Research Questions
Research Objective 3	Is there any experience of any threat to the company's system in the last three years?
	In which department are most threats presented and they are mainly natural or human?
	Has changed the way that companies operates after an attack?

Companies have been exposed to cyberattacks on their systems for about 40% over the last three years. Threats mainly concerned ship and office emails (25/39 replies), less the financial part of the company (19/39 replies) and fewer ship management systems (11/39 replies). this information may be the most important in the present research because it gives us information about what needs to be paid attention to. Finally, the changes that have been noticed in the way the company operates are significant at about 50%.

V. CONCLUSIONS

The development of technology has helped to create a secure cyberspace. It is generally acknowledged that this is achieved by training staff and strengthening ship and office systems [20], [21]. Companies also apply regulations that apply to these systems and follow BIMCO's insurance coverage guidelines and not only. Companies also apply regulations that apply to these systems and follow BIMCO's insurance coverage guidelines and beyond. they also have a documented security policy that they establish on their own or with the help of consulting companies. This policy is communicated to all employees and Applied to personnel information systems, as well as buildings and ships of its fleet.

Cyber Security in Shipping is now part of the ISM Code and will be mandatory from January 2021. Companies are already preparing for this, paying particular attention to procedures, regulations, staff training and intrusive systems or systems. their systems. Assistance comes from consulting companies or their specialized staff.

Regarding the topic of the survey, the responses were positive because the majority of respondents said that in addition to their knowledge of the subject, they also wanted to become better and more visible in Cyber Security. This means that Shipping is informed about Cyber Security and that its evolution is a given. Also the present research could be considered

important due to the professional status of the respondents. They are all of the largest executives in Greek shipping.

On the other hand, even though companies are aware of the regulations and procedures that apply and consider it important, they are not fully prepared. For this reason, it is proposed in the future to carry out further research on their preparation for the regulations.

ACKNOWLEDGMENT

All authors would like to thank the University of West Attica and specifically the Post Graduate Program of Studies (MSc) "New Technologies in Shipping and Transportations", for the financial support provided to them to undertake this research project.

REFERENCES

[1] Dan Cimpean, Johan Meire, Vincent Bouckaert, Stijn Vande Casteele, Aurore Pelle, Luc Hellebooge “Analysis of cyber security aspects in the maritime sector”, November 2011.

[2] Charles Brookson, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg, Jon Shamah, Sławomir Górniak “Definition of Cybersecurity Gaps and overlaps in standardisation” v1.0 | December 2015, ENISA.

[3] Switzerland. International Telecommunications Union: ‘Series X: Data Networks, Open System Communications and Security, Telecommunications security: Overview of cybersecurity’ (I. T. U. (ITU-T X.1205), Geneva, 2008

[4] Huge Boyes, “Maritime Cyber Security-Securing the Digital Seaways”. January 2014.

[5] Maersk shipping Reports $300M Loss Stemming from NotPetya Attack https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/ , 10 July 2017

[6] IMO - ANNEX 10: RESOLUTION MSC.428(98), “MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS”, 16 June 2017. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf

[7] IMO – “ISM Code and Guidelines on Implementation of the ISM Code” http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx

[8] IMO – “Maritime cyber risk” - MSC-FAL.1/Circ.3, 5 July 2017 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

[9] INTERNATIONAL STANDARD ISO/IEC 27001:2016 4th edition 2016-02-15 http://mahdi.hashemitabar.com/cms/images/Download/ISO/iso-iec-27000-2016-english.pdf

[10] IACS- “Recommendations on Cyber Safety Mark Step change of Cyber Security resilient”, http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-change-in-delivery-of-cyber-resilient-ships/

[11] TMSA 3 - TMSA 3- “MARITIME SECURITY – ELEMENT 13” VERSION 2017

[12] VIQ version 7.0.05, 2019

[13] BIMCO - ICS CS ON BOARD SHIPS “The guideline on cyber security on board ships v.3” (Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL) http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

[14] GDPR - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 https://gdpr-info.eu/

[15] GDPR – “Communication from the Commission to the European Parliament and the Council Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018” - https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf

[16] Kimberly Tam, Kevin Jones, “Factors Affecting Cyber Risk in Maritime”, June 2019.

[17] Kimberly Tam, Kevin Jones, “Forensic Readiness within Maritime Sector”. June 2019

[18] Krzysztof Cabaj, Dulce Domingos, Zbigniew Kotulski, Ana Respicio, “Cybersecurity education: Evolution of the discipline and analysis of master programs”, January 2018.

[19] Kimberly Tam, Kevin Jones, Maria Papadaki, “Threats and Impacts in Maritime Cyber Security”, January 2012.

[20] Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, “Improving cyber security awareness in maritime transport: A way forward”, October 2017.

[21] Ivo Friedberg, Kieran McLaughlin, Paul Smith, David Laverty, Sakir Sezer “STPA-SafeSec: Safety and security analysis for cyber-physical systems”, June 2016.

[22] Nick Ridle, Stephen Wares, “The Risk of Cyber Attack to the Maritime Sector”, July 2014

[23] B. Svilicic, David BrCiC, “Raising Awareness on Cyber Security Of ECDIS”, March 2019.

[24] Jennifer L. Bayuk – Jason Healey– Paul Rohmeyer– Marcus H. Sachs– Jeffrey Schmidt– Joseph Weiss, “Cyber Security Policy Guidebook”, 2012.

[25] Kenneth J. Knapp, “Cyber security and Information Assurance”, 2009.

[26] Joseph DiRenzo - Nicole K. Drumhiller - Fred S. Roberts. “Issues in Maritime Cyber Security”, 2017.

[27] John G.Voeller, “Cyber Security”, 2014.

[28] Rishikesh Sahay, Daniel Sepúlveda Estay, “CyberShip Project Cyber resilience for the shipping industry Work Package 3 & 4 Report” November 7,2018.

[29] Sashan Adem, “Cyber Security Thesis”, July 2018.

[30] B. Svilicic, Junzo Kamahara, Yoshiji Yano, Matthew Rooks, “Maritime Cyber Risk Management: An Experimental Ship Assessment”, February 2019.