HANDE YILMAZ

MS. Thesis

PRU 2024

T.C. PÎRÎ REİS UNIVERSITY
INSTITUTE FOR GRADUATE STUDIES

CYBERSECURITY APPLICATIONS AT SEA; EVALUATION OF CYBERSECURITY AWARENESS LEVELS OF TURKISH SEAFARERS AND TURKISH MARITIME INDUSTRY EMPLOYEES

MS. THESIS

HANDE YILMAZ

MAY 2024

T.C. PÎRÎ REİS UNIVERSITY
INSTITUTE FOR GRADUATE STUDIES

CYBERSECURITY APPLICATIONS AT SEA; EVALUATION OF CYBERSECURITY AWARENESS LEVELS OF TURKISH SEAFARERS AND TURKISH MARITIME INDUSTRY EMPLOYEES

MASTER THESIS

by
HANDE YILMAZ
B. S., Econometrics, Istanbul University, 2012

Maritime Business and Economics

Thesis Advisor:
Prof. Dr. M. Taner ALBAYRAK

MAY 2024

APPROVAL of the INSTITUTE for GRADUATE STUDIES

PRU, Graduate Studies Institute's student “21331201002” and “Hande YILMAZ” prepared her thesis titled

“CYBERSECURITY APPLICATIONS AT SEA; EVALUATION OF CYBERSECURITY AWARENESS LEVELS OF TURKISH SEAFARERS AND TURKISH MARITIME INDUSTRY EMPLOYEES”

by fulfilling all the necessary conditions determined by the relevant regulations and successfully presented it to the jury whose signatures are below.

Approval of the Institute for Graduate Studies

_____

(Title and Name)
Director

_____

(Title and Name)
Head of Department

_____

(Title and Name)
Advisor

Examining Committee Members

(Title and Name) _____

(Title and Name) _____

(Title and Name) _____

(Title and Name) _____

Date of Approval: dd.mm.yyyy

ABSTRACT

CYBERSECURITY APPLICATIONS AT SEA; EVALUATION OF CYBERSECURITY AWARENESS LEVELS OF TURKISH SEAFARERS AND TURKISH MARITIME INDUSTRY EMPLOYEES

Cybersecurity is one of the leading contemporary challenges for the entire maritime industry. The increasing digitalization of maritime industry technology makes it increasingly vulnerable to cyber-attacks as ships and maritime infrastructure become more and more interconnected. In this context, cybersecurity is one of the most pressing issues facing the maritime industry today, not only for ensuring system safety and preventing accidents, loss of life and environmental damage, but also for national security and the global economy.

From a maritime cybersecurity awareness perspective, end users are the most important building blocks for securing systems and protecting the information they process, as they are the maritime workers themselves.

In this study, the cybersecurity issues and current threat dynamics in the maritime sector are examined within the framework of cybersecurity approaches. To evaluate the cybersecurity awareness levels of Turkish maritime employees, a "Five Point Likert Type Questionnaire" method was used. The study assessed the employees' knowledge and awareness of cyber security, the training they have received, the effectiveness of this training in ensuring cybersecurity, and the technological devices used. The data was analysed using "SPSS," and based on the findings, solution suggestions were developed to increase the level of awareness.

Keywords: maritime cybersecurity, cyber threat, digitalization, maritime industry, vulnerabilities.

HANDE YILMAZ
MARITIME BUSINESS AND ECONOMICS MASTER'S PROGRAM

Thesis Supervisor: Prof. Dr. M. Taner ALBAYRAK

May, 2024, 95 Pages

ÖZET

DENİZDE SİBER GÜVENLİK UYGULAMALARI; TÜRK DENİZCİLERİ VE TÜRK DENİZCİLİK ENDÜSTRİSİ ÇALIŞANLARININ SİBER GÜVENLİK FARKINDALIK DÜZEYLERİNİN DEĞERLENDİRİLMESİ

Siber güvenlik, tüm denizcilik sektörü için önde gelen çağdaş zorluklardan biridir. Denizcilik endüstrisi teknolojisinin artan dijitalleşmesi, gemiler ve denizcilik altyapısı giderek daha fazla birbirine bağlı hale geldiği için gün geçtikçe siber saldırılara karşı savunmasız hale gelmektedir. Bu bağlamda, günümüzde denizcilik sektörünün karşı karşıya olduğu en acil sorunlardan biri olan siber güvenlik; yalnızca sistem güvenliğinin sağlanması, kazaların, can kayıplarının ve çevresel zararların önlenmesi için değil, aynı zamanda ulusal güvenlik ve küresel ekonomi için de kritik öneme sahiptir.

Denizciliğe siber güvenlik farkındalığı açısından bakıldığında son kullanıcılar, deniz çalışanlarının kendileri oldukları için sistemlerin güvenliğini sağlamak ve işledikleri bilgileri korumak için en önemli yapı taşlarıdır.

Bu çalışmada, siber güvenlik yaklaşımları denizcilik sektöründeki siber güvenlik alanındaki gelişmeleri ve güncel tehdit dinamikleri dikkate alınarak incelenmektedir. Türk Denizcilik sektörünün deniz ve kara çalışanlarının siber güvenlik farkındalık düzeylerini farklı değişkenler açısından değerlendirmek amacıyla "Beşli Likert Tipi Anket" yöntemini kullanarak, çalışanların konu hakkındaki bilgi ve farkındalık düzeyleri, aldıkları eğitim bilgileri, siber güvenlik alanında eğitim ve kullanılan teknolojik cihazlara göre siber güvenliği sağlama düzeyi "SPSS" kullanılarak değerlendirilerek farkındalık düzeylerini artırmaya yönelik çözüm önerileri ortaya konmuştur.

Anahtar Kelimeler: deniz siber güvenliği, siber tehdit, dijitalleşme, denizcilik sektörü, güvenlik açıkları.

HANDE YILMAZ
DENİZ İŞLETMECİLİĞİ VE EKONOMİ YÜKSEK LİSANS PROGRAMI

Tez Danışmanı: Prof. Dr. M. Taner ALBAYRAK

Mayıs, 2024, 95 Pages

DEDICATION

To My Lovely Husband and My Parents

ACKNOWLEDGMENTS

Firstly, I extend my deepest gratitude to my advisor, Prof. Dr. M. Taner ALBAYRAK, who embodies the concept of teaching as described by Gazi Mustafa Kemal ATATÜRK in his saying, "The assurance of our future is based on a solid education; education is based on the teacher." Starting from the coursework period, he illuminated my path like the sun, helping me find my direction. His support and invaluable contributions during the thesis process were instrumental in bringing my work to its current state.

To my beloved spouse, Oceangoing Master Gökay YILMAZ, who has been my greatest supporter at every moment and on every path I walked. Your unwavering support, the sharing of your experiences and valuable ideas, encouragement, meticulous guidance, and belief in me have been my greatest fortune in life. I offer my special thanks to you. Your boundless love and understanding have been my pillar of strength, and the motivation you provided made this journey possible.

To my dear mother Handan, my father Birol, and my brother Birhan; I wholeheartedly thank you for your efforts in bringing me to this point, for sharing the joy and pride I experienced during the thesis process, and for always being my support. Your endless love, guidance, and belief in me have been my guiding light through every challenge. To my extended family who contributed to my journey, stood by my side, and left their marks on my life; my little Princess Duru, dear Dilan, Aynur, Birdal, Nurten, and everyone whose names I could not mention, thank you very much.

This achievement is as much yours as it is mine. I am grateful for your presence in my life.

Lastly, I thank my thesis committee members, my dear teacher Assist. Prof. Dr. Hüseyin GENÇER and Assoc. Prof. Dr. Hasan Bora USLUER, for their valuable comments and contributions.

As I take the success I achieved with this work as the beginning of my academic career, I walk towards the horizon with inspiration from the words of the founder of our Republic, Gazi Mustafa Kemal ATATÜRK, who said, "No victory is an end in itself. Victory is only a means to achieve a greater goal."

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

ACM: Association for Computing Machinery

AGFI: Adjusted Goodness of Fit Index

AI: Artificial Intelligence

AI/ML: Artificial Intelligence and Machine Learning

AIS: Automatic Identification System

AMOS: Analysis of Moment Structures

ANOVA: Analysis of Variance

ATT&CK: Adversarial Tactics, Techniques & Common Knowledge

BIMCO: The Baltic and International Maritime Council

BNWAS: Bridge Navigation Watch Alert System

CCTV: Close Circuit TeleVision

CFI: Comparative Fit Index

CLIA: Cruise Lines International Association

COSCO: China Ocean Shipping (Group) Company

CPS: Cyber-Physical Systems

DCSA: The Digital Container Shipping Association

DDoS: Distributed Denial of Service

DNS: Domain Name System

DNV: Det Norske Veritas

DoS: Denial of Service Attack

ECDIS: Electronic Chart Display and Information System

ENISA: European Union Cybersecurity Agency

FMECA: Failure Modes, Effects, and Criticality Analysis

GFI: Goodness of Fit Index Value

GMDSS: Global Maritime Distress Safety System

GNSS: Global Navigation Satellite Systems

GPS: Global Positioning System

IACS: The International Association of Classification Societies

ICPS: The integration of Industrial Cyber-Physical Systems

ICS: Industrial Control System

IFI: Incremental Fit Index

IIoT: ndustrial Internet of Things

IMO: International Maritime Organization

INTERCARGO: The International Association of Dry Cargo Shipowners

INTERMANAGER: The International Trade Association for the Ship Management Industry

INTERTANKO: The International Association of Independent Tanker Owners

IoT: Internet of Things

ISO/IEC: International Organization for Standardization/International Electrotechnical Commission

IT: Information Technology

IUMI: International Union of Marine Insurance

KMO: Kaiser-Meyer-Olkin

LAN: Local Area Network

MASS: Maritime Autonomous Surface Ships

METI: Maritime Training and Education Institutions

MINE-EMI: Innovatıve Network Of Educatıon For Emergıng Marıtıme Issues

MITM: Man In The Middle

MSC: Mediterranean Shipping Company

MSW: Maritime Single Windows

NFI: Normed Fit Index

NIST: National Institute of Standards and Technology

OCIMF: Oil Companies International Marine Forum

OS: Operating System

OT: Operational Technology

PCS: Port Community Systems

RADAR: Radio Detection And Ranging

RMSEA: Root Mean Square Error of Approximation

SCADA: Supervisory, Control and Data Acquisition

SMS: Safety Management System

SMS: Short Message Service

SOLAS: Safety of Life at Sea

SOS: Save Our Ship

SPSS: Statistical Package for the Social Sciences

SQL: Structured Query Language

STCW: Standards of Training, Certification, and Watchkeeping

UAV: Unmanned Aerial Vehicle

USB: Universal Serial Bus

VDR: Voyage Data Recorders

VSAT: Very Small Aperture Terminal

WI-FI: Wireless Fidelity

XSS: Cross Site Scripting

1. INTRODUCTION

Global maritime transport is the most important building block for the flawless continuation of economic activities in the world and the unhindered continuation of international trade. The importance of global maritime transport is increasing exponentially as a result of both the growth in the world population and the integration of investment and trade tools at the international level. As a result of all these, the diversified operations of the maritime industry are becoming more complex and sensitive.

The maritime industry is a constant source of concern with its virtual security, which is in the process of continuous development and covers both physical and systems. With the intertwining of high-tech systems, whose use has become increasingly important, with digitalization in the maritime industry, the interdependence of ships underway and maritime infrastructures on land is increasing.
This integration brings the cybersecurity problem to the sector. For unhindered and flawless international trade, the continuation of the maritime industry and its instruments safely without interruption depends on the functioning of cybersecurity applications, which have become a contemporary challenge.

The maritime industry systems, equipped with high technology and digitized, are open to attacks by possible malicious actors, namely cyber risks. The cyber risk degrees of software and hardware connected to the systems are increasing in direct proportion with digitalization. Because every connected system contains many components that contain security vulnerabilities in terms of cyber threats.

IMO defines maritime cyber risk as the possibility that a potential threat could lead to a failure in the safety and security of technology and information systems (IMO., 2023).
These attackers, who create cyber risks, can cause devastating damage to the stakeholders of the maritime industry, theft of data, and consequences that endanger the physical safety of ships underway. Since cyber attacks in the maritime sector are not noticed until it is too

late; It is very important to take steps to reduce the risks that exist before an attack occurs within the possible scenarios. Considering all these, it is a necessity to develop effective strategies.

The International Maritime Organization defines cyber risk management as a process. This process starts with risk identification and continues with risk assessment. It ends with prevention and reduction to an acceptable level, taking into account the costs and benefits of the measures taken (IMO., 2023). The main purpose of establishing the cyber risk management defined by IMO is to ensure the continuity of the maritime industry operations in a safe, flawless and unhindered manner (IMO., 2022).

IMO Guidelines, which provide advice on cyber risk management, are complementary to the practices of safety and security management, and also contain functional elements to protect against cyber risks. In the light of all these, the concept of cybersecurity in the maritime field stands out as an important issue not only in terms of ensuring system security, preventing accidents, loss of life and environmental damage, but also in terms of national security and economy.

Since the end users in the maritime sector are the ones who work on the ships themselves, the most important building blocks to ensure the security of the systems and protect the information they process are the employees themselves. The maritime industry is going through a digital revolution. This revolution continues with the adoption of artificial intelligence and increasing levels of automation. Cybersecurity is becoming an increasingly important issue for the maritime industry due to rapid digital transformation, resulting in the need for preventive regulations against threats.

In this study, cybersecurity issues in the maritime sector will be examined within the framework of security approaches; new applications and approaches developed and being developed by taking into account current threat dynamics. Since end users in the maritime sector are the most important building blocks in ensuring the security of the systems and protecting the information they process; In order to evaluate the cybersecurity awareness levels of Turkish seafarers and Turkish maritime industry employees in terms of different

variables, the "Five Point Likert Type Questionnaire" method is used to examine the knowledge and awareness levels of the employees on cybersecurity and solutions and suggestions are developed to increase the awareness levels.

1.1 Types of Cyber Attack

With the developing technology, digital connections between devices are becoming indispensable. As a result of digitalization that provides ease of use, security vulnerabilities, i.e., possible cyber-attacks, are seen as the biggest concern. In the maritime industry, cybersecurity applications are becoming increasingly important to protect communication systems, data, recorded information and documents, virtual and physical entities from possible cyber-attacks. To produce and manage these applications competently, the types of cyber-attacks should be examined first. The most common types of cyber-attacks that pose a cyber threat can be listed as follows.

Table 1: Types of Cyber Attack (Source: (Crowdstrike, 2022))

Types of Cyber Attack	**Definition**
Malware	It is a type of software created to access or damage a system without the knowledge of the people using it. This type of software includes ransomware, trojans, spyware, viruses, worms, keyloggers, bots, crypto jacking, etc.
Denial of Service Attack (DoS)	It is a type of website attack that invades the attacked systems with data packets. After the attack, the resources and accounts of the system controlled by this network are not allowed to be accessed.
Phishing	It is a type of attack that convinces the system to download a file via e-mail, SMS, link sent to the system by pretending to come from a real and official institution. When this file is downloaded, it forces the system to share critical data such as password, account information, etc.

Spoofing	It is a cyber-attack that can enter the computer as a reliable source and at the same time hide itself. With this attack, cyber attackers can install viruses on systems that they can use for their own purposes.
Identity-Based Attacks	The cyber attacker, who obtains the information of the person using the system in any way, starts using the system as the user himself. For this reason, this attack is one of the most difficult attacks to understand. The most common types can be listed as follows: Man-in-the-Middle (MITM) Attack, Password Spraying, Hybrid Pass Attack, etc.
Code Injection Attacks	It is a type of attack created by a cyber attacker by injecting malicious code into the system to be affected. These attack types can be listed as follows: SQL Injection, Cross-Site Scripting (XSS), Malicious Advertising.
Supply Chain Attacks	The type of cyber-attack targeting supply chain stakeholders is of two types: software attack and hardware attack. While attacks that threaten software are carried out by injecting malicious code; attacks that threaten hardware threaten physical tools.
Insider Threats	In this type of attack, the cyber attacker is a former employee or active employee who is authorized to access that system.
DNS Tunneling	It is a cyber-attack that suppresses the existing security in the systems and transmits the code that will affect the system using DNS.
IoT Based Attacks	It is a cyber-attack aimed at taking control of IoT-connected vehicles and stakeholders. Once control is seized, all connected systems are threatened by data theft, DoS or DDoS attacks and all kinds of malware.

1.2. Critical Systems for Cybersecurity on Board and Ports

Ships create a more secure environment as they have more and more digitalized systems with technological development. However, they become vulnerable to attacks due to security vulnerabilities that may occur in the critical systems they are connected to. The critical infrastructures on ships and the threats related to them can be summarized as follows.

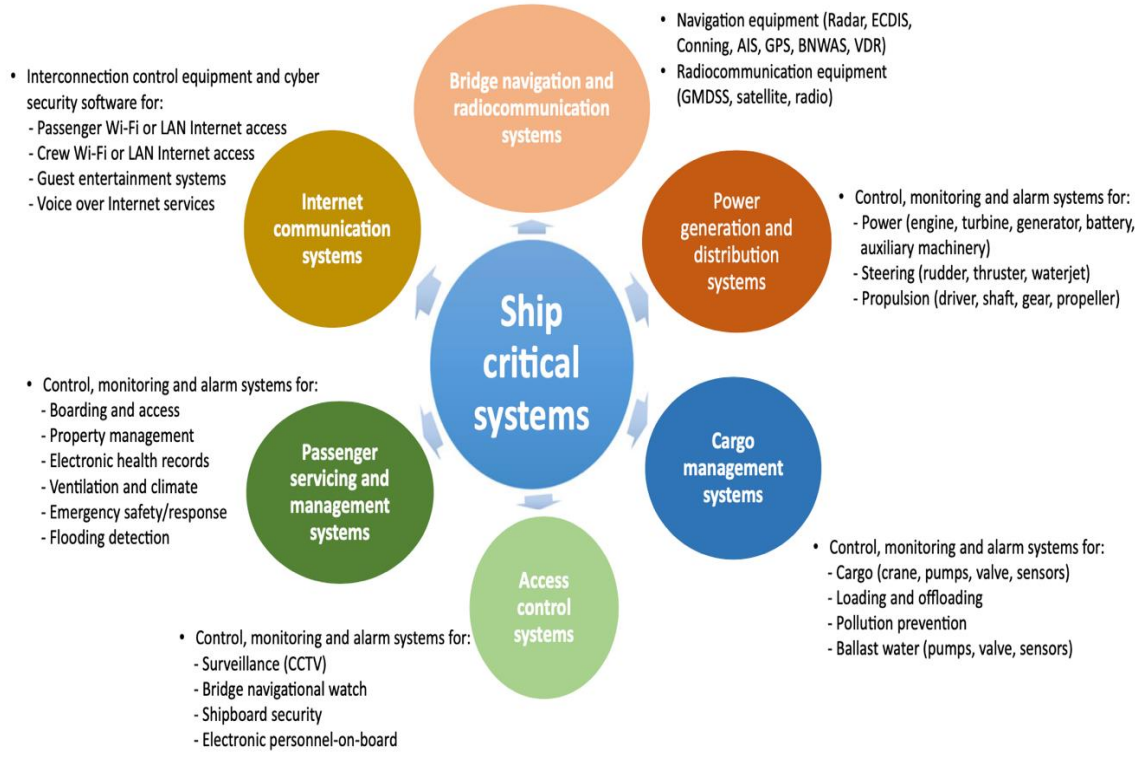

Figure 1: Ship critical systems and assets (Source: (Svilicic, et al., 2019))

As shown in Figure 1, Bridge navigation and radiocommunication systems, connected equipment contains threats in the form of network security, software security, cyber incident handling procedures, and the use of portable devices. To eliminate these threats; the operating system and applications should be checked for updates, a possible incident detection, analysis and response plan should be made, the security status of devices such as USB should be implemented (Sivilicic, et al., 2019).

The extensive use of automation and IT systems in modern and autonomous ship systems depending on critical infrastructures leads to cyber-attacks by hackers and malicious actors, which can lead to incidents and cause major losses. Figure 2 shows the main vulnerabilities and consequences of modern and autonomous ship systems connected to bridge navigation and radio communication systems.

Critically important systems such as AIS, GPS, GNSS, ECDIS, VSAT, RADAR are compromised by malicious people using these systems for their own purposes with signal jamming, broadcasting fake messages, sending wrong signals, transmitting virus, etc. It can lead to disastrous consequences. For example, attacks on GPS and navigation technology pose a medium to high risk because there is the possibility of data and service protocol breaches as well as physical damage. A cyber-attack on GNSS could also lead to disruption of other ship systems (e.g., AIS). In the event of a cyber-attack, RADAR may provide false information about nearby objects due to false echoes caused by external radar waves. This false information can cause ship collision accidents. If it finds an open VSAT interface, it can change GPS coordinates and settings as well as download malware. These vulnerabilities and their consequences, summarized in Figure 2, provide information about the size of the attack surface that needs to be defended and possible cyber-attack for the maritime industry to understand the vulnerabilities of the system (Akpan, et al., 2022).

Systems	Vulnerabilities	Consequences
Automatic Identification System (AIS)	- Signal interference - False information sharing - Malware - Spoofing - No encryption - Signal jamming	- Ship hijacking - Destruction of data - Theft of valuable data
Electronic Chart Display Information System (ECDIS)	- Obsolete OSs - Insecure update mediums	- Loss of communication with the NS - Hijacking of a ship - Sensitive data theft - Compromising computers and OSs
GNSS and GPS	- Jamming attacks - Weak signal strength - Interference - Spoofing attacks - DoS/DDoS attacks - Packet modification	- Ship hijacking - Problems with the NS - GPS signal false information - Disrupt vessel operation - Delays in services

Radar	- Jamming attacks - Spoofing attacks - DoS/DDoS attacks	- Loss of communication with the NS - Loss of lives and cargo - Delays in cargo management
Global Maritime Distress System (GMDSS)	- Malware - Spoofing attacks - DoS/DDoS attacks	- Wrong position of the ship - Further attacks on ECDIS
Industrial Control Systems (ICSs)	- Inadequate ACM - No support for integrity check - Information exposure - Poor patch management - Hardware failures - Improper security configuration - Lack of network segmentation - Weak password policies - Lack of firewalls - Lack of encryption - Weak remote access policies - Weak USB policy - Lack of training for SOS	- Ship hijacking - Unavailability of the ICS - Data leakage - Physical damage to facilities - Interference with safety systems - Unplanned shutdowns - Damage to equipment
Propulsion and machinery management and power control systems	- Malware attack - DoS/DDoS attacks - Smuggling - Stealing - Manipulation attacks	- Ship hijacking - Diversion of the ship - PS could be interrupted - Ship damage - Financial damage - Disclosure of sensitive data
Very Small Aperture Terminal (VSAT)	- Fake signals - Malware attack - Stealing	- Theft of sensitive data - Upload of malware - Change of GPS coordinates
IT network systems	- Poor access control - DoS/DDoS attacks - Weak password policies - Malware attacks - Poor patch management - Improper security configuration - Poor security documentation - Lack of network segmentation - Lack of firewalls - Lack of encryption - Weak remote access policies - Weak USB policy - Lack of training for SOS	- Upload malware - Unauthorised physical access - Unauthorised logical access - Loss of confidential documents - Financial damage - Theft of sensitive data - Reputation damage

Figure 2: The vulnerabilities of modern ship systems and their consequences (Source: (Akpan, et al., 2022).

Energy generation and distribution systems and associated equipment, which are mentioned in the ship critical systems in Figure 1, contain threats in the form of physical and cyber access controls, authentication controls, authorized access procedure. To eliminate these threats; all access should be provided only to authorized personnel, all control mechanisms should be implemented, security related events should be recorded (Sivilicic, et al., 2019).

Cargo management systems connected equipment have inherent problems such as problems with remote authentication controls, physical access problems for non-authorized personnel, lack of periodic review of policies and procedures, lack of training prior to actual use of a program. To eliminate these problems; remote authentication using only cryptography should be implemented, all default passwords should be changed to provide controlled access for authorized persons, a possible incident detection, analysis and response plan should be made, extra measures for physical and environmental protection should be reviewed (Sivilicic, et al., 2019).

Access control systems have the same problems and solutions as cargo management systems, albeit with different equipment.

Passenger servicing and management systems connected equipment have the following problems: lack of access control policies, lack of procedures during failures, lack of control over authorized access policies, lack of training on security measures. In order to eliminate these problems, authorized users and their privileges should be identified and documented, and backup procedures should be designed and implemented. Sharing passwords or using joint accounts should be prevented. Measures should be taken and planning should be made against possible incidents (Sivilicic, et al., 2019).

Internet communication systems, the equipment connected to them, have problems of network privacy protection, lack of updating of systems, virus recognition programs and their lack of updating. To overcome these problems, firewalls should be designed and controlled by rules and policies. Centralized management and reporting systems should be developed (Sivilicic, et al., 2019).

Ports are one of the most important elements in the international supply chain. The flawless functioning of the supply chain depends on the security of the operations carried out in ports. As developing technology increasingly connects ports and ships to each other, automated systems that replace the human factor also bring security vulnerabilities. Cyber threats caused by these vulnerabilities can enable actions such as drug smuggling, cargo theft,

violating the cargo tracking program and customs, and cargo theft (Tusher, Munim, Notteboom, Kim, & Nazir, 2022). Critical infrastructures at ports that may be exposed to cyber-attacks include services connected to ships, commercial services and security-related services.

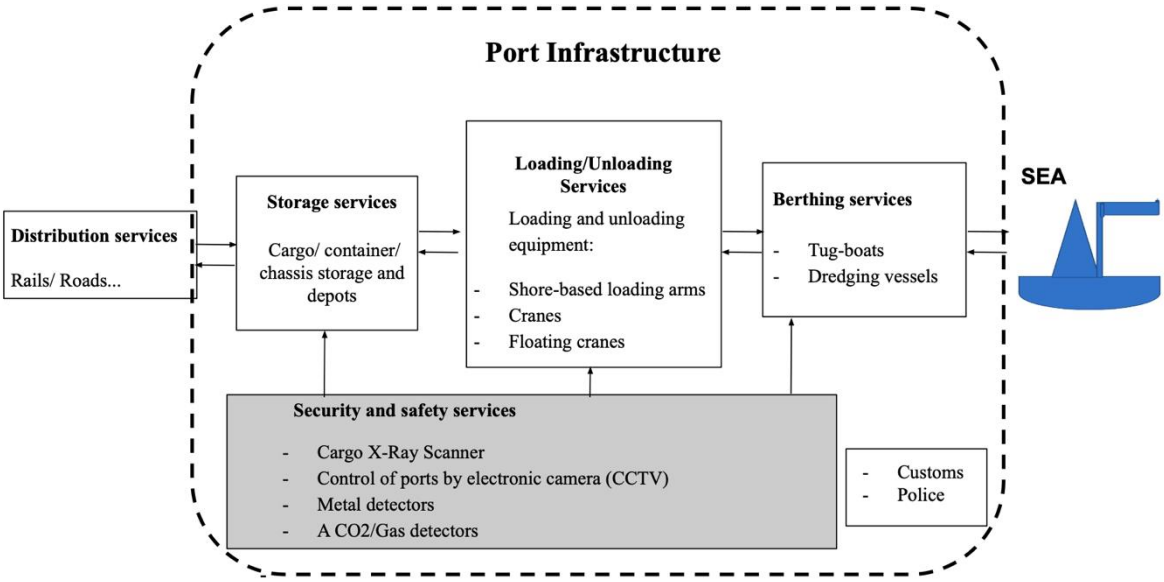

Figure 3: Port Infrastructure (Source: (Farah, et al., 2022)

Figure 3 illustrates the port infrastructure. The aim of in-port security is to ensure the effective safety of people and to protect life. The various services provided for this purpose can be summarized as Cargo X-ray Scanner, Electronic camera (CCTV) control of ports, Metal detectors.

Equipment used within the scope of in-port operations are cranes, tugboats, and dredging vessels. The use of new technologies in the quest to improve service delivery also creates new vulnerabilities for hackers to maliciously take control to cause significant damage.

Platforms such as Port Community Systems (PCS) and Maritime Single Windows (MSW), where data and information are exchanged, are the most likely systems to be targeted by cybercriminals in ports.

A Community System (PCS) is an open platform that provides connectivity between various systems, enabling secure and intelligent information exchange between different systems. Timely ready access to information in port operations minimizes delays, reduces paperwork and improves service quality (Farah, et al., 2022). The system consists of Cargo module, Tracking and tracing module, Berth management module, Storage allocation module, Interface to other transport modes, Billing module, Statistics module. These modules provide users with information on critical issues within their scope, such as information on ships, details of loaded cargo, time to be spent at the dock, location and graphics of warehouses, transportation modes, updates on invoices. This system is of critical importance as it provides easy access to the most relevant information at every stage of port operations (Farah, et al., 2022). Ports are generally more vulnerable to cyber risks. As attacks are often carried out through Wi-Fi networked systems, it is vital to protect these modes.

Single Window System, which facilitates communication between ports and governments by standardizing services at ports, provides documents such as authorizations and certificates with a single login for all users (Farah, et al., 2022). It is vital that the Single Window System is protected against unauthorized access and cyber-attacks.

Port management consists of ship-to-shore operation systems, transshipment system, storage system and delivery system. Cyber-attacks disrupt the normal functioning of the port by affecting the port from all aspects.

1.3. Recent Cyber Attacks in Maritime Industry

The increasing presence of digitalization and smart devices in the maritime sector with advanced technology makes the sector vulnerable to cyber-attacks considering the critical infrastructures of ships and ports. The cyber-attacks that have occurred in the sector from past to present show how these dangers are used by cyber pirates. Intervening after a cyber attack brings with it various losses. For this reason, it is vital to take measures, studies and practices on cybersecurity. The cyber attacks that have occurred in the sector from past to present are listed below.

Ransomware attack 2023	• DNV: A ransomware attack on a major ship software supplier hit over 1,000 ships. DNV said that it had been targeted by ransomware and had to shut down IT servers that were linked to ShipManager systems.
Malicious software attack 2023	• Lispon Port: A cyberattack was launched, causing the port's website and internal computer systems to crash. A $1.5 million ransom was demanded.
Ransomware attack 2022	• Germany: Oil businesses Oiltanking and Mabanaft were victimized by a hack that rendered their loading and unloading systems inoperable.
Ransomware attack 2021	• South Africa: Systems have been rendered inoperable following a significant attack on the Cape Town, Ngqura, Port Elizabeth, and Durban port authorities.
Software flaw 2021	• Houston Port: The port was the victim of a cyberattack that took advantage of a fundamental weakness in its password management technology.
Ransomware attack 2020	• Marseille Port: The port that was struck by ransomware. The major focus of the attack was internal connections with information systems, not naval facilities.

Ransomware attack 2020	• Iran Port of Shahid Rajaee: Ships, vehicles, and computers that control the flow of products all failed in an instant, producing major halts and disturbances on the canals and highways leading to the plant.
Ransomware attack 2020	• Mediterranean Shipping Company (MSC) Group: The company's headquarters experienced a network outage for several days as a result of the cyber attack, preventing the usage of the company's digital tools and website.
GPS Spoofing attack 2019	• Eastern Mediterranean: For a long time, ships cruising in this region, ships in anchorage zones, and offshore platforms have reported GPS interference.
DDoS attack 2018	• Port of Vancouver: The port was subjected to a DDoS attack that analyzed roughly 225,000 user accounts on the same day.
Ransomware attack 2018	• COSCO: This cyber attack harmed Cosco's Shipping Lines' systems, websites, e-mails, and phones. It took a week for the company to resume normal operations.
GPS Spoofing attack 2017	• Black Sea: More than 20 ships were reported to have displayed an inaccurate location at a spot far different from their GPS location as a result of an attack that affected multiple ships near the Black Sea Russia.
NotPetya Ransomware attack 2017	• Maersk: The hack, dubbed NotPetya, targeted Maersk computer servers. As a result of this encrypted malware attack, all Maersk systems and services were targeted, and 17 container terminals were compromised. It cost about $200 million in financial damage.

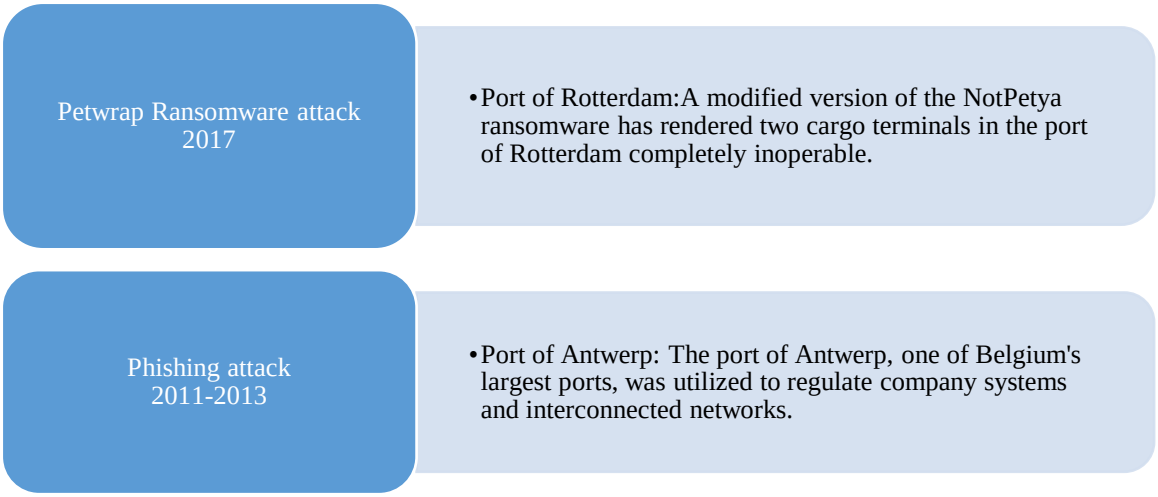

Figure 4: Recent Cyber Attacks in Maritime Industry (This table was compiled by the author from various sources.)

1.4. Cybersecurity Approaches and Practices in Maritime Sector

Protecting automation systems used in maritime operations against cyber risks is vital to ensure the continuity of the industry. In addition, cyber risks are not only caused by security vulnerabilities created by systems or processes. At the same time, how these systems are used is also of great importance, meaning that the most important factor when it comes to cybersecurity is the human factor.

Considering the importance of the industry in the supply chain, being prepared for a cyber-attack is a necessity today. The impact of a possible cyber-attack on the maritime industry can bring the entire supply chain to a standstill like a snowball. Therefore, an investment in cybersecurity will increase the control power in the maritime industry in the event of a possible attack and reduce the damage and losses that may occur.

The concept of maritime security is a whole. It means being free from all threats or perceptions of threats, natural and human. The best way to create and implement actions in accordance with the concept of security at sea at the highest level is to develop protocols at the international level. For this purpose, IMO was established as a legal body in 1958 (IMO., 2019). In addition to the guidelines for ensuring physical security, it has also established

advisory guidelines on cyber risk management. These guidelines for protection against cyber threats include managing potential vulnerabilities and appropriate actions (IMO., 2023). Because the maritime sector has characteristics that make it vulnerable in terms of cybersecurity (BIMCO, 2021):

- Authorization of numerous stakeholders to charter and operate on the same vessel leads to a lack of responsibility in IT and OT systems.
- Operating systems used in the sector not being updated on time or continuing to use obsolete systems.
- Use of operating systems that do not allow running anti-virus programs.
- Security gaps when using the created online interface.
- Security vulnerabilities that may occur due to sector equipment that can be monitored remotely.
- Integration of automation systems and computer-controlled critical infrastructures without taking cyber risks into account.
- Lack of training, exercises, and drills in the sector regarding cybersecurity.

A cyber risk management approach can be defined as specifying the responsibilities of key personnel, identifying equipment and components that may pose a risk, providing technical and procedural measures and creating a contingency plan.

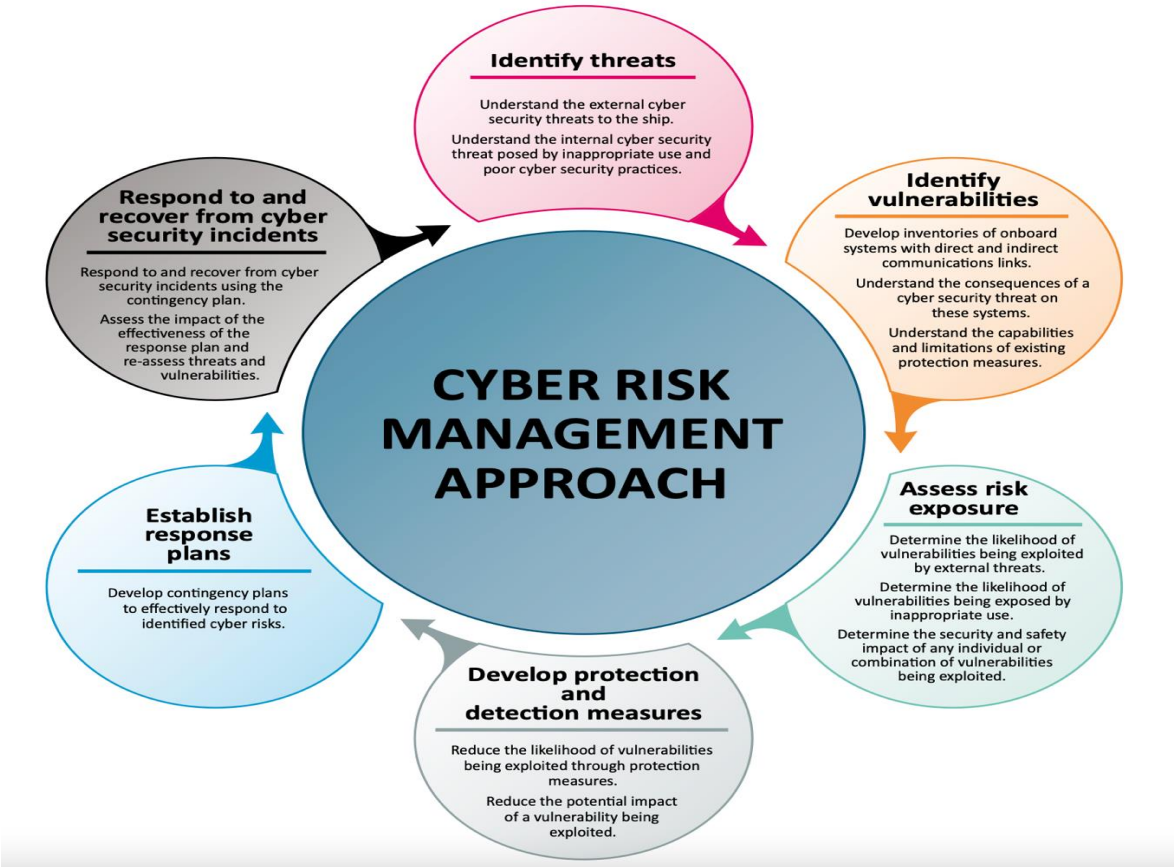

Figure 5: Cyber Risk Management Approach (Source: (BIMCO, 2021))

IMO guidelines for protection against cyber threats describe the elements of managing cyber risks. These elements are (IMO., 2022):

- Cyber risk management consists of an interconnected process like the links of a chain.
- The purpose of cyber risk management is to create a robust process.
- The applicability of cyber risk management is possible by creating a culture of awareness in the sector employees starting from the highest level.
- It is best to take the plans and programs of similar sectors as an example to create a cyber risk management program.
- Cyber risk management should be simultaneous and continuous in practice. The following steps should be followed to ensure this continuity.

Identify: Identifying the factors that cause vulnerabilities and potential threats is important to identify the weaknesses of the sector and systems. In the event of a possible cyber risk, it is a priority in cyber risk management that the personnel in charge are aware of their roles and responsibilities from the lowest to the highest level.

Protection: The measures are based on the resilience of equipment integrated with digital systems against cyber threats. In the event of a possible cyber threat, the existence of a control process is the biggest advantage.

Detection: The most important part of the cyber defense culture is to detect a possible cyber incident before it occurs and to create a plan accordingly.

Response: After a cyber-attack occurs, the most important step is to take it under control. Cybersecurity plans should be implemented without wasting time.

Recovery: For the uninterrupted continuation of the supply chain, the recovered information should be analyzed, and the system should be restored to full operation without wasting time.

The first step to a competent response is to have an effective plan. These plans for recovering systems should be accessible to all stakeholders and employees. The main goal is to recover the data completely and restore the systems to a healthy working condition as soon as possible. The priority for ships, ports, port operators and maritime sector stakeholders is to ensure human safety so that the ship can continue its voyage safely (BIMCO, 2021).

With a multi-layered system to be created, risks in cyber risk management can be minimized (Arora & Antoniadou, 2020):

- People should be educated about what cyber risk is, what the threats are and how to avoid them. They should be informed about the need to report any suspicious situation and what to do if IT/OT systems are down.

- It should be a habit to scan every application and system used for viruses and not to open the attachment in every e-mail.
- Learn more about cyber risk management using resources such as the ISO/IEC 27001 standards, the US-NIST framework and the onboard cybersecurity guide prepared by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and the World Shipping Council.
- Industry stakeholders should regularly audit their cybersecurity measures and update them as appropriate. Appropriate contingency plans should be developed and ready for implementation when needed.
- Sector stakeholders should organize regular and up-to-date trainings. These trainings are the most important building block to raise employee awareness.

In addition to these, some governments, and organizations such as IMO etc. have guidelines on cybersecurity issues, practices, and cybersecurity management plans.
IMO has adopted resolution MSC.428(98) on Maritime Cyber Risk Management in the Safety Management System (SMS). This resolution enacts the requirement for an approved SMS to include cyber risk management and is the main regulation on maritime cyber risk management (IMO., 2023). The inclusion of cyber risk in the SMS puts the concept of cybersecurity into practice, ensuring that it is not just on paper. Developing a security culture that considers cyber threats is the golden key in this sector.

The ISO/IEC 27001 standard, published jointly by the International Organization for Standardization (ISO) and the Electrotechnical Commission (IEC), addresses information technology and security management methods. It is a standard on security techniques. It provides a framework for the implementation of an information security management system. Many maritime organizations adopt this standard as the basis for their cybersecurity programs. The standard specifies requirements for establishing policies, controls, risk assessments and incident response procedures (IMO., 2022).

Alongside the IMO resolution, the Cybersecurity Framework of the US National Institute of Standards and Technology (NIST) helps industry stakeholders implement the most effective

approaches to manage any cyber threats they may face. It demonstrates the need to prioritize appropriate behavioral models to mitigate cyber risks (BIMCO, 2021). NIST defines 4 phases in incident response:

1. Preparation
2. Detection and analysis
3. Containment and eradication
4. Post-incident recovery.

The preparation phase includes locating critical equipment, backing up data, creating workarounds, developing, and implementing a contingency plan.

Detection and analysis phase includes determining how the incident occurred, identifying which systems were affected, and determining whether the threat persists.

Containment and eradication phase includes disabling the affected networks and systems, making sure virus programs are up to date.

The post-incident recovery phase involves securely restoring data and getting the system up and running.

The Digital Container Shipping Association (DCSA) "DCSA Implementation Guide for Cyber Security on Ships" is also available. This guide is based on the analysis of the NIST framework. One of the key elements of the DCSA guidelines is the container industry. Compliance with the DCSA guideline provides shipowners with every vulnerability identified in the risk assessment. will provide advice on compliant cybersecurity measures and notes describing cyber risks that may be present (DCSA, 2021).

The International Association of Classification Societies (IACS) has published "Recommendation (No. 166) on Cyber Resilience". This recommendation consolidates

previous IACS recommendations on cyber resilience and provides a framework that applies only to newbuildings but can be considered as a guideline for all existing ships.

BIMCO, IUMI, ICS, Intertanko, Intercargo, Cruise Lines International Association and the International Maritime Forum of Oil Companies have come together to produce a booklet entitled "Guidelines for Cyber Security on Ships Version 4". This guide is a recommendation; it describes how operations should be assessed and the protocols required to create a security shield for cyber systems. It also includes recommendations on how to respond to and eliminate cyber threats. The guide covers areas such as employee awareness training, network segmentation, access controls, encryption and security monitoring. It aims to mitigate common threats such as malware infections, ransomware attacks and data breaches (BIMCO, 2021).

The ISPS Code is part of the SOLAS Convention for the Safety of Life at Sea (SOLAS), which provides minimum security regulations for ships, ports and government agencies; industry stakeholders subject to the Code must also consider cyber risks in accordance with the security regulation. With cyber risks becoming more and more prevalent, it is in the interest of maritime stakeholders to identify cybersecurity issues and include them in the security assessment. Developing national and global cybersecurity strategies will be the greatest weapon to meet this challenge (OAS, 2021).

The 2nd Maritime Cyber Security Conference, organized by the European Union Cybersecurity Agency (ENISA), aimed to explore the dynamics behind cyber risks and the challenges facing the maritime sector. It allows for a dialogue between relevant stakeholders to address the main current cybersecurity challenges as well as the ongoing digitization process. It reveals that ransomware is the primary threat in shipping and then becomes the main target of the corporate side (ENISA., 2022).

In conclusion, Cyber Risk Assessments cover people, processes, and technological equipment (MissionSecure, 2021) :

- Ensure the implementation of cybersecurity policies at all levels of the organization, on board and ashore.
- Plans and policies should be reviewed, and deficiencies should be addressed.
- Safety audits should be repeated, and drills should be conducted on board and ashore.
- Establish and improve the security management system to create an ongoing feedback mechanism process regarding cyber risk management.
- Cybersecurity awareness trainings in general should be provided and updated and repeated.
- Establish and supervise cybersecurity liaison between shore and ship personnel.

The main findings of the DNV Maritime Cyber Priority 2023 report is a comprehensive study on how to stay secure in an era of connectivity and draws on a survey of 801 maritime professionals and in-depth interviews with leaders and experts. It provides insights into changing attitudes and approaches to cybersecurity in the maritime industry, as well as recommendations for improving maritime cybersecurity.

With the data obtained from this study, DNV reports that the maritime industry faces cybersecurity challenges in five key areas: investment, regulation, supply chains, organizational culture and access to talent. These challenges can be listed as follows (DNV, 2023):

Invesment: In the maritime sector, investments are needed to take measures against cyber threats and attacks, but funding is insufficient.

Regulation: Cybersecurity regulations in the maritime sector are on the rise, primarily serving as defenses against previously encountered incidents, threats, and attacks. However, the industry faces challenges in raising awareness about emerging cyber risk threats and vulnerabilities while striving to comply with existing regulations. It is imperative to redefine cybersecurity risks as safety risks, acknowledging that potential cyber attacks can lead to significant harm to life, property, and the environment.

Supply Chain: Organizations in the maritime sector procure software and technology from various layers of the supply chain, integrating these into critical infrastructure. To ensure comprehensive cybersecurity, operators must rigorously audit the cybersecurity requirements of their suppliers throughout the purchase, installation, and operation of equipment, systems, and software.

Organization Culture: There is a reluctance to share information because a cyber incident reveals potential vulnerabilities that competitors could exploit, placing firms at a competitive disadvantage. Nevertheless, information sharing is crucial for establishing industry standards that provide organizations with best practice guidelines and assist them in developing a security posture that complies with regulatory requirements.

Talent Shortages: The dynamic evolution of cyber threats intensifies the difficulty of sourcing professionals possessing requisite skills. Additionally, challenges arise from employee inadvertence, which may inadvertently facilitate cyberattacks. Comprehensive and standardized training assumes a pivotal role in cultivating a more risk-conscious workforce and fostering a culture of cybersecurity. The industry's imperative stance on security training necessitates an equivalent emphasis on cyber training.

According to the DNV Maritime Cyber Priority 2023 report, the following are some of the recommendations for improving maritime cybersecurity (DNV, 2023):

- View cybersecurity as a facilitator: Cybersecurity leaders ought to be integrated into broader strategic dialogues from inception, with cybersecurity serving as a pivotal component in the procurement and advancement of novel technologies.
- Allocate resources to cybersecurity: Regard investment in cybersecurity not merely as a business expense, but as a strategic investment fostering confidence, competitiveness, and innovation.
- Develop a risk-based approach; Organizations should develop a risk-based approach to cybersecurity that is tailored to their specific needs and circumstances.

- Foster a culture of cyber awareness; Organizations should foster a culture of cyber awareness among all employees, including training programs and regular testing.
- Collaborate with industry partners; Collaboration with industry partners can help organizations stay up to date on emerging threats and best practices for mitigating them.
- Implement robust incident response plans; Organizations should have robust incident response plans in place that are regularly tested and updated to ensure they are effective in the event of a breach or attack.

1.5. Cybersecurity Risk Management and Culture Approaches in Maritime Sector

The maritime sector is increasingly digitalized, driven by benefits such as improved efficiency, productivity, and safety. However, this transition to digital technologies also introduces new cybersecurity risks that threaten operations, safety, and data privacy. The main objective in the face of cyber threats is to intervene in the cyber incident and restore the system under attack and make the system function smoothly. The most important element to support this goal is the development of a cyber risk management strategy and culture. Developing a strong cybersecurity culture and implementing proper cybersecurity practices are critical for maritime organizations to mitigate these risks.

In the maritime industry, cyber risk management should focus on the security and resilience of automation and networked systems in their integration, both onshore and offshore, which should be integrated with the results of risk assessment. Effective cybersecurity resilience is based on human, process, and technology factors (Kayişoğlu & Bolat, 2022):

Human Factor: Lack of awareness is one of the main reasons for the rapid spread of cyber threats and risks. The competence of all relevant personnel, both onshore and offshore, is the primary defense against cyber risks. IMO guidelines emphasize that effective cyber risk management requires ensuring appropriate levels of cyber risk awareness at all levels of an organization.

Process Factor: The most important step in the cyber risk assessment process is to understand the potential impact. By including the assessment of potential impacts in the risk analysis approach; it shows that the loss of information confidentiality can jeopardize security. In the context of cybersecurity, the likelihood of a cybersecurity incident will depend on the factors of discoverability, exploitability, repeatability.

Technology Factor: OT and IT systems are separate, but increasingly integrated with the internet and evolving technology. IMO recommends a holistic approach to maritime cybersecurity, meaning that both IT and OT systems should be addressed in the cyber risk management plan and appropriate defensive measures should be taken against cyber incidents involving any of them.

Cybersecurity risk assessment, cybersecurity risk resilience and flexibility, and the measures developed within this scope are integrated with each other and integrated into the relevant system as a whole, monitored, recorded, measures are developed, and the results are analyzed and shared with other stakeholders, forming the cybersecurity risk management and culture in the maritime sector (Kayişoğlu & Bolat, 2022).

The article "Developing a maritime cyber safety culture: Improving safety of operations" suggests several strategies for developing a maritime cyber safety culture. These include (Hopcraft, et al., 2022).

- Promoting open dialogue among personnel regarding safety and cyber risks.
- Formulating and disseminating safety policies and statements, alongside reporting discoveries.
- Fostering in-person interactions among personnel to foster engagement with safety concerns.
- Establishing and executing an efficient cyber risk management framework, aiding crew members in identifying, safeguarding against, detecting, responding to, and recovering from cyber incidents.

- Delivering training and fostering awareness of associated risks and mitigation strategies.

A cybersecurity culture encompasses awareness, knowledge, and behaviors that prioritize security. For the maritime sector, this means integrating cybersecurity as a core value and responsibility at all levels. Senior leadership must demonstrate commitment and allocate sufficient resources. Employees need training to understand potential threats, their roles and responsibilities, and how to identify and report incidents. A culture of vigilance and continuous improvement must be instilled.

The establishment of a cyber safety culture holds significant ramifications for the overarching safety standards within maritime operations. With the increasing integration of digital systems across vessels and operations, crew safety becomes increasingly contingent upon these systems. A cyber safety culture ensures that personnel are equipped to make informed safety decisions and are cognizant of the cyber risks inherent in their roles. Through the cultivation of such a culture, organizations enhance their capacity to navigate, safeguard against, detect, respond to, and recuperate from cyber incidents. Consequently, this initiative serves to avert accidents, minimize operational downtime, and fortify resilience against financial losses attributable to cyber threats. In sum, a robust cyber safety culture constitutes an indispensable component of comprehensive maritime risk management (Hopcraft, et al., 2022).

Specific cybersecurity practices and approaches will vary based on a company's size, operations, and technologies. However, there are some common elements. Companies should develop cybersecurity policies outlining acceptable use, data protection, and incident response. They should implement technical controls like network segmentation, endpoint protection, firewalls, and multi-factor authentication. Vulnerabilities should be identified through risk assessments and penetration testing. Access controls should restrict who can view and modify critical systems and data. Event monitoring tools can detect anomalies and threats in real time. Backups and disaster recovery plans are essential to minimize downtime and data loss from incidents.

Establishing a cybersecurity culture within the maritime industry yields several advantages. It fosters heightened awareness of cyber risks among organizations and facilitates the development of efficacious risk management strategies. Consequently, this initiative contributes to enhanced safety and security for personnel, alongside mitigating operational downtime and financial losses stemming from cyber incidents. Furthermore, numerous Classification Societies tasked with ensuring regulatory compliance of ships have implemented cyber notations, serving as attestation to the adept management of cyber risks onboard vessels and by their crews. Moreover, the cultivation of a cybersecurity culture can result in reduced insurance premiums for organizations. In essence, fostering a cybersecurity culture stands as an indispensable component of contemporary maritime risk management practices in an increasingly digital landscape.

In summary, as the maritime sector continues digitizing, a holistic approach that focuses on both the human and technical aspects of cybersecurity will be required. A strong cybersecurity culture where all employees understand their role, combined with proper policies, controls, and technologies, can help maritime organizations defend against cyber threats and protect their critical operations, infrastructure, and data.

1.6. Digitalization: Smart Port and Autonomous Ship with Cybersecurity

Digital transformation plays a pivotal role in revolutionizing decision-making across all sectors of industry, facilitating enhanced data analysis, workflow automation, and the adoption of innovative business models. At the core of this shift towards modernized systems lies information technology. In the realm of ports, digital transformation has ushered in the era of smart ports, while concurrently propelling ships towards autonomy (Solmaz, 2023).

Smart ports epitomize sustainability, connectivity, and digitization, seamlessly integrating with logistics networks, industrial frameworks, and ecological imperatives. These ports leverage cutting-edge technologies to streamline operations while prioritizing environmental stewardship.

The advancement of smart ports has been propelled by the integration of various digital technologies, including the Internet of Things (IoT), digital twins, and blockchain. IoT facilitates the interconnection of diverse objects, enabling data collection, information sharing, and remote command execution. Meanwhile, digital twin technology involves creating virtual replicas of physical devices or systems, which are animated using data transmitted from their real-world counterparts via IoT. This allows for experimentation, simulation, and analysis without impacting the actual system. Blockchain technology, on the other hand, offers robust data encryption mechanisms aimed at safeguarding sensitive information (Solmaz, 2023).

Big data and artificial intelligence (AI) technologies play a pivotal role in enhancing the efficiency of port operations by analyzing data sourced from myriad channels within smart ports. Among the most notable examples of smart ports worldwide is the Port of Rotterdam in the Netherlands, renowned as Europe's largest port and a trailblazer in digital transformation and innovation.

In smart ports like Rotterdam, cutting-edge digital technologies such as IoT sensors, data analytics, and cloud computing are leveraged to optimize port activities and bolster operational efficacy. These technologies facilitate the real-time monitoring of ship movements, cargo handling operations, and port infrastructure. Notably, the port has made significant investments in smart infrastructure, including automated container terminals, intelligent traffic management systems, and digital platforms fostering seamless communication among stakeholders (Basulo-Riberio, et al., 2024). For instance, leading ports such as Rotterdam, Singapore, Barcelona, and Hamburg have embraced the concept of the digital twin, creating virtual replicas of their ports in virtual environments. These digital twins are fed real-time data from IoT sensors, providing a comprehensive overview of port activities and conditions.

In the case of the Port of Rotterdam, data collected from IoT sensors encompasses a wide array of parameters, including tide, current, salinity, temperature, wind speed and direction,

water levels, and visibility conditions (Basulo-Riberio, et al., 2024). This wealth of information is meticulously analyzed by AI algorithms, enabling the port to make informed decisions, execute corrective actions, and address diverse operational challenges in real-time. Thus, AI-powered analysis of big data sourced from IoT sensors serves as a cornerstone in optimizing port operations and fostering continuous improvement within the maritime domain.

Interfering with the IT systems of a smart port can have far-reaching consequences, disrupting critical operations such as the utilization of the port's digital twin, data from IoT sensors, security camera feeds, and lighting systems. Such interference can lead to disruptions in various facets of port operations, including the entry and exit of ships, cargo handling processes, vehicular and pedestrian traffic within the port premises, as well as planning and communication procedures. Moreover, safety and security practices may be compromised, posing significant risks to personnel and assets (Solmaz, 2023).

The ramifications of such disruptions extend beyond the confines of the port itself, impacting maritime shipping companies and, ultimately, the global economy. The inability to effectively manage port operations can result in delays, financial losses, and reputational damage for all stakeholders involved.

To mitigate the risks associated with cyber threats, smart ports must prioritize the development and implementation of comprehensive cybersecurity strategies. These strategies should encompass robust security measures, including but not limited to, network segmentation, encryption protocols, access control mechanisms, intrusion detection systems, and regular security audits. Moreover, fostering a culture of cybersecurity awareness among port personnel and stakeholders is essential to bolstering resilience against cyberattacks and ensuring the continued functionality and security of port operations in an increasingly digitized maritime landscape.

In Figure 6, Danube Ports Network divides the smart port model into its components as logistics, mobility, governance, environment, people and economy and summarizes its benefits (DanubePortsNetwork, 2019):

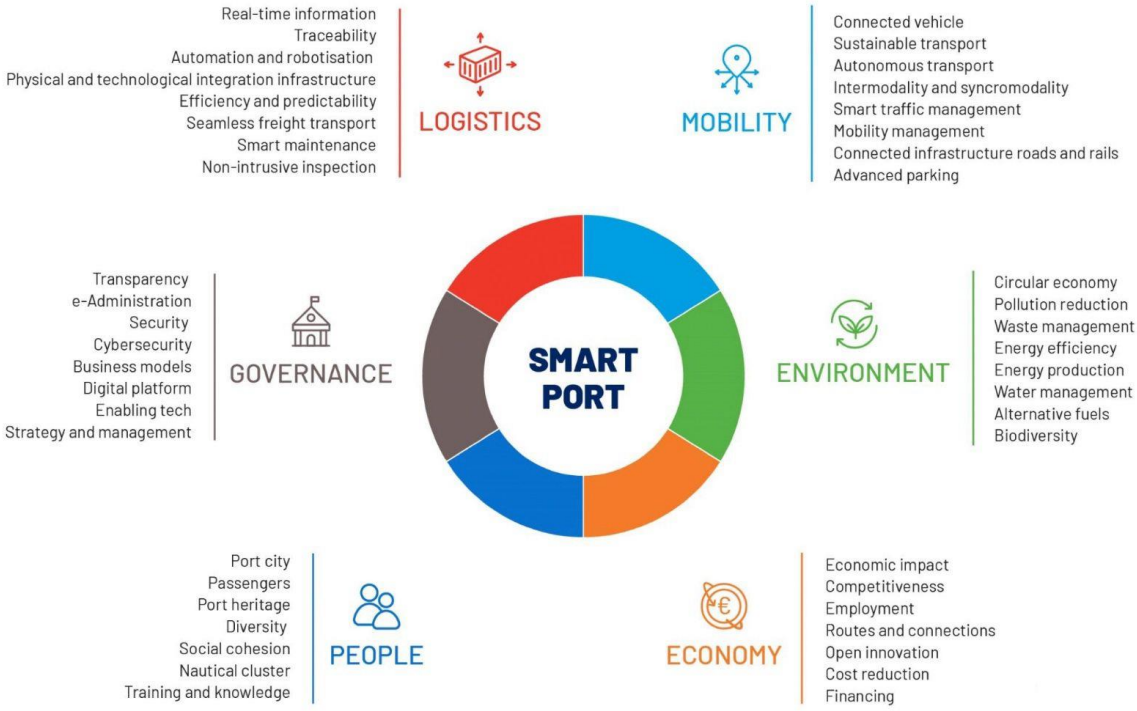

Figure 6: Components of Smart Port (Source: (DanubePortsNetwork, 2019)

In essence, the transition from conventional ports to smart ports is propelled by digitalization. Embracing this digital transformation empowers smart ports to enhance productivity, minimize environmental footprint, and foster societal welfare in adjacent areas. Undoubtedly, smart ports emerge as pivotal agents in shaping the trajectory of maritime transportation. They do so by championing innovation, sustainability, and operational efficiency, all of which are vital in navigating the dynamic contours of the contemporary global trade arena (Basulo-Riberio, et al., 2024).

In essence, the digital revolution within port operations has culminated in the emergence of what we now recognize as smart ports.

The maritime industry is on the cusp of a technological revolution with the advent of autonomous ships. These advanced vessels promise to transform the landscape of global shipping, offering enhanced operational efficiency, improved safety, and increased sustainability. However, as the maritime ecosystem embraces the potential of autonomous ships, it also faces an unprecedented challenge: ensuring robust cybersecurity in this rapidly evolving domain.

In the maritime industry, heavy dependence on technology inevitably increases the ship's presence in cyberspace, increasing the ship's attack surface and the chance of being targeted. The cyber attack surface of autonomous ships is closely related to the ship's level of autonomy. Because the attack surface varies depending on the complexity and number of systems and human interfaces used to control, monitor and override ships. Regarding the levels of autonomy, the International Maritime Organization (IMO) has proposed four levels for the scoping exercise. Figure 7 summarizes these levels (Cho, et al., 2022).

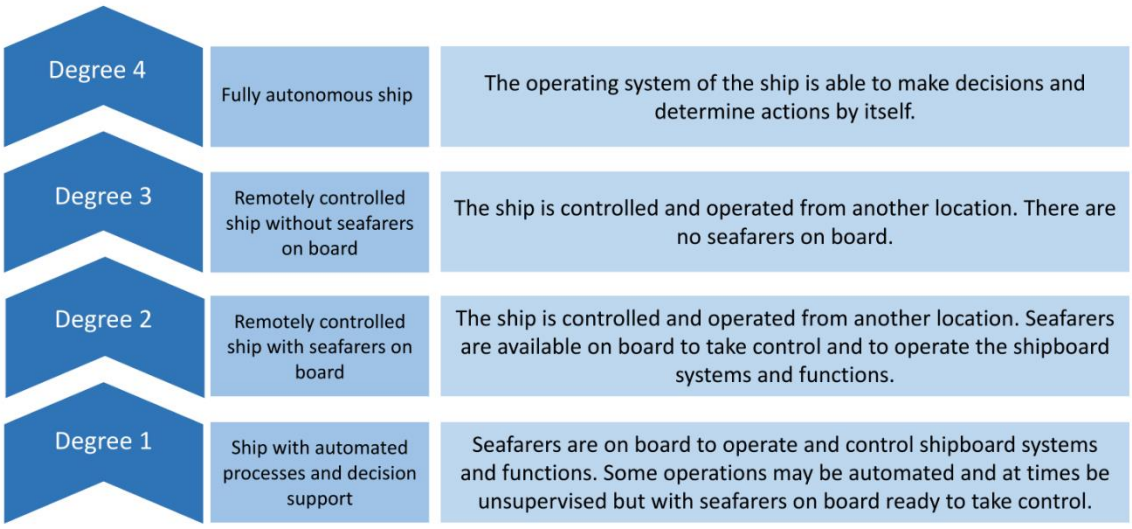

Figure 7: Four levels of Autonomous Ship (Source: (Li, et al., 2023))

The deployment of autonomous ships in the maritime industry brings numerous advantages such as increased efficiency, cost savings, and improved safety. However, it also introduces several cybersecurity risks and challenges that need to be addressed. Here are some of the key considerations (Silverajan, et al., 2018):

- Autonomous ships heavily rely on interconnected systems and networks. Hackers may attempt to gain unauthorized access to these systems, potentially leading to unauthorized control of the ship. This could result in navigation manipulation, cargo tampering, or even ship hijacking.
- Autonomous ships generate vast amounts of data, including sensitive information about cargo, routes, and operational details. Data breaches can lead to financial loss, reputational damage, or even sabotage. Cybercriminals might target data storage systems or attempt to intercept data during transmission.
- Autonomous ships, like any other connected system, are susceptible to malware and ransomware attacks. Malicious software can disrupt ship operations, compromise critical systems, or encrypt data, demanding ransom for its release. Such attacks can significantly impact the ship's functionality and disrupt maritime operations.
- Autonomous ships rely heavily on Global Positioning System (GPS) signals for navigation and positioning. Cyber attackers can spoof or manipulate GPS signals, leading to incorrect ship positioning or altering the ship's course. Additionally, GPS jamming can disrupt satellite signals, affecting ship navigation and posing a threat to maritime safety.
- The deployment of autonomous ships involves various stakeholders, including ship manufacturers, software developers, and third-party service providers. Each participant in the supply chain can become a potential entry point for cyber threats. Weak security practices or vulnerabilities in any component can expose the entire system to risk.
- Insiders with authorized access to autonomous ship systems, such as employees or contractors, may pose a security risk. These individuals could intentionally or unintentionally compromise the ship's security through actions like malicious software installation, data theft, or unauthorized system modifications.
- As autonomous ships are a relatively new technology, there is still a lack of standardized cybersecurity practices and regulations specific to this domain. This absence can lead to inconsistent security measures and make it challenging to ensure a high level of cybersecurity across the industry.

Addressing these risks and challenges requires a comprehensive cybersecurity approach. This includes implementing robust authentication and access controls, encrypting data in transit and at rest, regularly updating and patching software and systems, conducting thorough risk assessments, promoting security awareness among stakeholders, and establishing industry-wide standards and regulations. The consequences of a successful cyber attack on an autonomous vessel extend beyond compromised operations and financial losses; they pose significant risks to crew safety, the integrity of cargo, and the overall stability of maritime trade networks.

In recent years, autonomous ships have attracted great attention due to their potential to revolutionize maritime operations. Equipped with cutting-edge technologies such as artificial intelligence (AI), machine learning and advanced sensors, these ships will have the capacity to navigate, communicate and make decisions without direct human intervention. Such autonomy promises to unlock remarkable benefits such as increased safety through optimized route planning, reduced fuel consumption and minimization of human errors. In addition, artificial intelligence technologies used by autonomous ships are also vulnerable to cyber attacks. Most existing AI systems are powered by machine learning, which extracts knowledge by learning many examples in a dataset. Since the AI technologies used by autonomous ships depend on the dataset, they will be compromised if the dataset is corrupted or poisoned by an attacker (Cho, et al., 2022). When designing, developing and operating autonomous ships, a risk management approach should be developed and implemented to identify and implement appropriate countermeasures commensurate with the risk.

Understanding the benefits and risks related to autonomous ships and cybersecurity and making security-related issues and plans early are of great importance for safe and efficient operations. By actively addressing cybersecurity risks and incorporating resilient defenses, the shipping industry can safely navigate the uncharted waters of autonomous shipping and ensure the safety and sustainability of future maritime operations.

2. LITERATURE REVIEW

Understanding the complexities and nuances of cybersecurity requires a deep dive into the extensive body of existing literature, which spans various domains, including computer science, information technology, law, psychology, and sociology.

This literature review aims to provide a comprehensive analysis of the current state of cybersecurity research and shed light on the multifaceted challenges and solutions surrounding this rapidly evolving field. By synthesizing the findings of numerous scholarly articles, research papers this review aims to identify the key trends, gaps in cybersecurity research. The literature review is in the table below:

Table 2. Recent Studies on Maritime Cybersecurity

Authors	**Year**	**Title**	**Findings**
Erlend Erstad, Rory Hopcraft, Avanthika Vineetha Harish, Kimberly Tam	2023	A human-centred design approach for the development and conducting of maritime cyber resilience training	The main findings of this article are the benefits and potential drawbacks of utilizing a human-centred design approach for maritime cyber resilience training. The paper demonstrates how to develop and conduct a maritime cyber incident scenario as a training tool using this approach. The output is primarily intended for Maritime Training and Education Institutions (METI) (Erstad, et al., 2023).
J. Bacasdoon, J. Bolmsten	2022	A Multiple Case Study of METI Cybersecurity Education and Training: A Basis for the Development of a Guiding Framework for Educational Approaches	The main findings of this article are related to a multiple case study of METI cybersecurity education and training. The study provides a basis for the development of a guiding framework for educational

			approaches in the maritime industry. The study highlights the need for increased cybersecurity awareness and skills among seafarers to avoid catastrophic mistakes while using the internet and other information technology devices and systems onboard the ship (Bacasdoon & Bolmsten, 2022).
Boris Svilicic, Igor Rudan, Alen Jugovic and Damir Zec	2019	A Study on Cyber Security Threats in a Shipboard Integrated Navigational System	The main findings of the article are that shipboard integrated navigational systems are vulnerable to cyber-attacks, and that the same types of cyber threats can affect different navigation systems from different manufacturers installed on different types of ships. The article also highlights the need for increased awareness and training among ship operators to mitigate the risks of cyber-attacks on their navigational systems (Svilicic, et al., 2019).
Boyan Mednikarov, Yuliyan Tsonev, Andon Lazarov	2020	Analysis of Cybersecurity Issues in the Maritime Industry	The main findings of this article are the analysis of cybersecurity issues in the maritime industry, including the components of the shipping industry's cybersecurity policy, the types of cyber-attacks, and the vulnerability assessment of on-board information and communication systems. Also suggests measures for cyber defense and outlines requirements for computer networks, navigation, communication, and managing components on mariner vessels and ashore equipment (Mednikarov, et al., 2020).

Andrej Androjna, Tanja Brcko, Ivica Pavic, Harm Greidan	2020	Assessing Cyber Challenges of Maritime Navigation	The primary findings of the article encompass the distinct challenges associated with maritime cybersecurity, the complexities involved in securing both vessels at sea and shore-based infrastructure, and the potential trajectories of cyberattacks on maritime systems related to navigation, propulsion, and cargo. Additionally, the article underscores the necessity for a focused and strategic approach to enhance cyber and information security within the maritime industry (Androjna, et al., 2020).
Kristen Kuhn, Salih Bicakci, Siraj Ahmed Shaikh	2021	COVID-19 digitization in maritime: understanding cyber risks	The main findings of this article are that digitization is reshaping the maritime industry, and COVID-19 has accelerated this process. While technology offers improvements and competitive advantages, it also creates new digital opportunity structures that increase cyber risks. Cyber-attacks can cripple critical systems and services at significant cost, motivating stakeholders to engage with these risks. Also offers insights into how capacity building exercises can help prepare for secure use of cyberspace in the maritime environment and address key disconnects in crisis response (Kuhn, et al., 2021).
Juan Ignacio Alcaide, Ruth Garcia Llave	2020	Critical infrastructures cybersecurity and the ma aritime sector	The main findings of the article are that the maritime sector exhibits vulnerabilities and critical components in terms of

			cybersecurity. However, understanding cyber-attacks in the maritime field presents greater challenges when the dimension of the problem remains highly unidentified. The article emphasizes that in this internet age and post-globalization of maritime transport, with the digital transformation of the logistics chain and its different components, we must strengthen the resilience of its fundamental elements (Alcaide & Llave, 2020).
Hasan Mahbub Tusher, Ziaul Haque Munim, Theo E. Notteboom, Tae-Eun Kim, Salman Nazir	2022	Cyber security risk assessment in autonomous shipping	The principal findings of this article indicate the proposal of a multi-criteria decision-making framework for evaluating cybersecurity risks within the context of autonomous shipping. The research was substantiated through surveys conducted among subject matter experts, system designers, and seafarers. Various types of equipment and systems were ranked based on their perceived susceptibility to cyber threats. The study presents recommendations to guide the prioritization of areas within the maritime industry that require the implementation of safeguards against cyber threats (Tusher et al., 2022).
Abubakar Sadiq Mohammed, Philipp	2022	Cybersecurıty Challenges In The Offshore Oil And Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective	The main findings of this article are that the offshore oil and gas industry is undergoing a digitalisation drive, which has led to an increase in cyber-

Reinecke, Pete Burnap, Omer Rana, Eirini Anthi			attacks. The integration of Industrial Cyber-Physical Systems (ICPS), Supervisory, Control and Data Acquisition (SCADA) systems, and Industrial Internet of Things (IIoT) technologies has expanded the attack surface available for cyber attackers to exploit. A successful cyber-attack against an offshore oil and gas asset could have a devastating impact on the environment, marine ecosystem, and safety of personnel. The article provides a timeline of documented cyber-attacks on upstream oil and gas assets and highlights possible areas of cyber-attack infiltration (Mohammed, et al., 2022).
Ignacio de la Pen˜a Zarzuelo	2021	Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue	The main findings of this article are that cybersecurity is an important issue in the port industry due to the potential criminal attacks and terrorism that seaports and terminals may face as critical infrastructures. The article emphasizes the need for raising awareness on this issue and conducting risk analysis to ensure the security of ports and maritime industry (Zarzuelo, 2021).
O. Onishchenko, K. Shumilova, S. Volyanskyy, Y. Volyanskaya, Y. Volianskyi	2022	Ensuring Cyber Resilience of Ship Information Systems	The principal findings of this article reveal that the maritime industry is experiencing a rise in cyberattacks, which have the potential to inflict substantial harm on the global economy. A significant concern is the pervasive lack of awareness among contemporary companies regarding protection against cyber

			threats and the risks associated with the leakage of confidential information. The research identifies the inadvertent actions of crew members as the most critical vulnerability, as seafarers may inadvertently introduce viruses into equipment or click on malicious links. Additionally, the article outlines a fundamental response plan for identifying and assessing risks, which can be continuously updated in accordance with the identified areas of system vulnerabilities (Onishchenko, et al., 2022).
Ahmed Amro, Vasileios Gkioulos	2023	Evaluation of a Cyber Risk Assessment Approach for Cyber-Physical Systems: Maritime and Energy Use Cases	The main findings of this article are related to the evaluation of a cyber risk assessment approach for Cyber-Physical Systems (CPS) in the maritime and energy domains. The paper presents an evaluation methodology for assessing the effectiveness of the FMECA-ATT&CK approach, which is a risk assessment method that combines Failure Modes, Effects, and Criticality Analysis (FMECA) with Adversarial Tactics, Techniques & Common Knowledge (ATT&CK). The evaluation results show that FMECA-ATT&CK is effective in identifying cyber risks in CPS and can be useful for evaluating other risk assessment processes. The article also highlights some limitations of the approach and suggests future

			directions for research (Amro & Gkioulos, 2023).
Oleksiy Melnyk, Svitlana Onyshchenko, Nataliia Pavlova, Oleksandra Kravchenko, Svitlana Borovyk	2022	Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System	The principal findings of this article underscore the escalation of accidents within the global fleet owing to the expansion of global trade and international shipping. Moreover, the article highlights the attendant risks to maritime safety stemming from unauthorized access and manipulation of vessel information and data. To address these challenges, the article proffers recommendations for integrating cyber risk management practices within the shipping industry, aimed at fortifying resilience against external cyber threats and enhancing the safety and security of seagoing vessels. Additionally, the article delineates key technological, procedural, and regulatory avenues for safeguarding ships against cyberattacks that jeopardize information security (Melnyk, et al., 2022).
Kimberly Tam, Kevin Jones	2019	MaCRA: a model-based framework for maritime cyber-risk assessment	The main finding of article is the proposal of a comprehensive framework that can be used to assess cyber-risks in the maritime industry. The framework takes into account the unique nature of maritime cyber-threats and provides a tool for companies, organizations, and individuals to assess risks given any possible maritime cyber-scenario. By fully populating the proposed model with real-world data and creating an

			array of customizable views, one can discover risks not previously considered. The framework can also adapt as maritime technology evolves and as attackers find new vulnerabilities and incentives (Tam & Jones, 2019).
Saiful Karim	2022	Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat?	The main finding of this article is that the current international legal framework, including the existing IMO legal instruments, is inadequate for effectively dealing with maritime cybersecurity threats. The article argues that further initiative may be taken for an effective international legal reform through multidimensional cooperation involving State and non-state actors (Karim, 2022).
Mawuli Afenyo, Livingstone D. Caesar	2023	Maritime cybersecurity threats: Gaps and directions for future research	The main finding of the review article is that there is a significant gap in knowledge and research on maritime cybersecurity issues, and that intensive research is required to keep up with current realities. The authors suggest that policymakers and practitioners need to work together to enact policies and build resilient systems to address the increasing cyber vulnerability of maritime supply chains (Afenyo & Caesar, 2023).
J. Scanlan, R. Hopcraft, R. Cowburn, J.M. Trovåg, M. Lützhöft	2021	Maritime Education for a Digital Industry	The principal findings of the article indicate that the maritime industry is experiencing a digital revolution, offering both opportunities for innovation and improvements,

			alongside significant challenges. The educational requirements of the sector have evolved and will continue to do so in response to this ongoing digital transition. A critical focus within this context is cyber risk management, emphasizing the necessity of equipping seafarers with the requisite skills to navigate and adapt to the emerging technological landscape (Scanlan, et al., 2021).
Michael L. Thomas	2022	Maritime Hacking Using Land-Based Skills	The main findings of the article are that the maritime shipping industry is vulnerable to cyberattacks due to a lack of skill across the industry, critical maritime chokepoints as ambush locations, and an engrained tendency to view the sea as buffering shipping from land-based threats. The article also highlights that hacking skills from land-based systems and environments are easily transposable to a maritime environment. The article discusses potential economic and global impacts of cyberattacks on shipping traffic and suggests ways in which national defense professionals and the maritime industry can work together to prevent and mitigate the effects of such attacks (Thomas, 2022).
Boris Svilicic, Miho Kristić, Srđan Žuškin, David Brčić	2020	Paperless ship navigation: cyber security weaknesses	The main findings of the article are related to the analysis of cybersecurity weaknesses of paperless ship navigation, specifically focusing on the

			Electronic Chart Display and Information System (ECDIS). The analysis identified eight cyber threat vectors, and critical severity. The vulnerabilities were analyzed in the context of ECDIS backup arrangement and safeguarding measures implemented on board the paperless ship (Svilicic, et al., 2020).
D.S. Ilcev	2022	Software Solutions for GMDSS Network and Equipment	The main findings of article are the introduction of software solutions for communication, equipment control, and management of oceangoing ships for enhanced Global Maritime Distress and Safety System (GMDSS) network and equipment. This software controls all maritime transmission systems and integrates communications software at the level of server and workstations. The solutions proposed in the paper include the use of software to ensure the continued availability of GMDSS in case of disruptions to ships' radio or satellite communications via jamming. Additionally, cyber risk management onboard oceangoing ships is crucial due to the increasing reliance on digitization, integration, security, and automation in modern GMDSS and digital oceangoing ships (Ilcev, 2022).
A. Alop	2019	The Main Challenges and Barriers to the Successful "Smart Shipping"	The main findings and solutions of the article discusses the challenges and potential threats that can make successful operation of smart shipping complicated or unrealistic.

			The article also mentions that a quick and painless transition to smart shipping is unlikely. The paper suggests that necessary changes for smart shipping need to be drastic and comprehensive, but it does not provide specific solutions for overcoming the challenges (Alop, 2019).
Kimberly Tam, Kemedi Moara-Nkwe, Kevin D. Jones	2021	The use of cyber ranges in the maritime context: Assessing maritime- cyber risks, raising awareness, and providing training	The principal findings and proposed solutions of this article center on the application of cyber ranges within the maritime sector to evaluate maritime-cyber risks, enhance awareness, and facilitate training. The paper addresses the necessity for improvements in scalability, education, and "federation" within cyber ranges. Furthermore, it explores how context-specific cyber ranges can enhance maritime training and risk assessment for both mariners and security professionals. This study is part of a European project aimed at augmenting the capabilities of cybersecurity professionals and increasing awareness of cyber risks through the deployment of next-generation cyber range environments (Tam, et al., 2021).
Maurantonio Caprolu, Roberto Di Pietro, Simone Raponi, Savio Sciancalepore,	2020	Vessels Cybersecurity: Issues, Challenges, and the Road Ahead	The primary findings elucidated in the article pertain to vulnerabilities in the systems and communication technologies deployed within contemporary maritime vessels. Additionally, the paper delineates key vulnerabilities requisite for

Pietro Tedeschi			mitigation in alignment with the latest resolutions from the International Maritime Organization (IMO). Moreover, it outlines preemptive measures to counter the identified threats and underscores future research avenues necessitated by both industry and academia to fortify vessel cybersecurity. The proposed solutions encompass the adoption of technical controls to mitigate risks, comprehensive cybersecurity risk analyses for all vessels, and the implementation of appropriate countermeasures to address identified threats (Caprolu, et al., 2020).
Pınar Özdemir, Alaettin Sevim, Taner Albayrak	2023	Closing the gap between present and future through education: MINE-EMI project	The main finding of the article is the need for a new postgraduate program that addresses emerging issues, innovation, and skills development in maritime management. The project aims to fill the gap between the current curriculum of postgraduate programs and the contemporary requirements of the maritime sector (Ozdemir, et al., 2023).
Rafael Diaza, Katherine Smitha, Serena Bertagnab, Vittorio Buccib	2023	Digital Transformation, Applications, and Vulnerabilities in Maritime and Digital Transformation, Applications, and Vulnerabilities	The main findings of this article are related to the digital transformation, applications, and vulnerabilities in maritime and shipbuilding ecosystems. The article discusses how Industry 4.0 technologies can revolutionize traditional approaches adopted in the shipbuilding industry, but also highlights the challenges and limitations that may arise during their implementation. The paper provides

			case studies and methodologies to address these challenges and improve the efficiency of ship design and production processes (Diaza, et al., 2023).
Randy J. Hinrichs, Viatcheslav M. Popovsky, Barbara Endicott-Popovsky	2023	Bringing the Industry Partner to the Cybersecurity Education Table as an Active Participant	The focus of the article is to explore ways to integrate academic and industry content and processes in cybersecurity education. The authors suggest that finding industry partners to accelerate this partnership is key to responding to the workforce shortage and increasing the relevancy of solutions. They also propose several research directions, including studying collaborations, online immersion and interactivity, augmented cognition, predicting cybersecurity talent through competency assessment, and managing the Learning and Employment Record for a skills-based economy (Hinrichs, et al., 2023).
Xue Li, Poong Oh, Yusheng Zhou, Kum Fai Yuen	2023	Operational risk identification of maritime surface autonomous ship: A network analysis approach	The principal findings of the article involve the identification of potential operational risks associated with Maritime Autonomous Surface Ships (MASS) and an examination of their interrelated causal relationships through network modeling. The results elucidate the architecture of these operational risks, offering a comprehensive understanding of the causes and consequences of risks associated with MASS. Additionally, the findings provide managerial

			implications for the control and mitigation of MASS risks, benefiting stakeholders in maritime transport (Li, et al., 2023).
Rory Hopcraft, Avanthika Vineetha Harish, Kimberly Tam, Kevin Jones	2023	Raising the Standard of Maritime Voyage Data Recorder Security	The principal conclusions drawn from the article underscore the inadequacy of current security protocols for Voyage Data Recorders (VDRs) in mitigating cyber threats, underscoring the imperative for augmenting extant standards. Proposals for bolstering VDR security are delineated by the authors, subsequently validated through consultations with industry specialists during a maritime-focused symposium. These recommendations proffer solutions addressing contemporary and anticipated risks to VDRs, while also acknowledging the foreseeable financial and procedural complexities inherent in their adoption (Hopcraft, et al., 2023).
Min-Kyu Kim, Jong-Hwa Kim, Hyun Yang	2023	Optimal Route Generation and Route-Following Control for Autonomous Vessel	The principal findings and solutions presented in the article involve the determination of an optimal route that accounts for both vessel fuel consumption and safety, as well as the proposal of a route-following control method that can accurately adhere to the designated route. These solutions are intended to enhance the efficiency and safety of autonomous vessels (Kim, et al., 2023).
Omer Soner, Gizem Kayisoğlu,	2024	Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks	The main findings of this article are; seafarers must be equipped with sound scientific methods to

Pelin Bolat, Kimberley Tam			effectively identify, prevent and manage cyber risks. Training programs, manual backups and HRA techniques are crucial to detecting cyber risks and increasing cyber resilience in the maritime industry. Overall, the study highlights the importance of addressing human factors, implementing training programs and using appropriate tools and frameworks to strengthen cyber resilience in the maritime industry, reduce cyber threats and ensure the security of AIS systems (Soner, et al., 2024).
Rafael Diaz, Ricardo Ungo, Katie Smith, Lida Haghnegahdar, Bikash Singh, Tran Phuong	2024	Applications of AI /ML in Maritime Cyber Supply Chains	The article provides insights into leveraging AI/ML technologies to address challenges in maritime cyber supply chains, offering solutions to enhance resilience, manage risks, analyze cybersecurity threats, integrate blockchain technology, mitigate supply chain disruptions, assess port resilience, and develop data-sharing platforms for improved safety and efficiency in maritime operations. These solutions aim to address cybersecurity challenges in maritime supply chains by leveraging AI/ML technologies to detect vulnerabilities, enhance security for UAV swarms, reinforce resilience against cyberattacks, improve data connectivity, and ensure privacy in data sharing for maritime operations (Diaz, et al., 2024).

Xinqiang Chen, Dongfang Ma, Ryan Wen Liu	2024	Application of Artificial Intelligence in Maritime Transportation	The article discusses the importance of cybersecurity in the maritime industry, and the key findings on cybersecurity highlight the importance of cybersecurity measures, human factors, and risk assessment in ensuring the safety and security of maritime operations in the face of cyber threats and possible accidents. These findings aim to optimize maritime operations, improve safety, increase efficiency, and reduce energy consumption in the shipping industry through the application of artificial intelligence techniques (Chen, et al., 2024).
Nimra Tabish, Tsai Chaur-Luh	2024	Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives	The main findings of this article are; MASS faces significant threats such as unauthorized access, data breaches, and denial of service attacks, highlighting the need for robust security measures. Electrification and digitalization of ships is making progress in terms of safety and efficiency, but also brings challenges such as cybersecurity and legal considerations. These findings underscore the critical importance of addressing cybersecurity challenges in MASS operations to ensure resilience and security in the maritime industry. Solutions such as Quantum-Safe Cryptography, Adaptive Machine Learning and AI Defenses, Standardization of Cybersecurity

			Practices, Human Factors and Training comprehensively address cybersecurity challenges in Maritime Autonomous Surface Ships by emphasizing proactive defense, collaboration and adherence to regulatory standards to increase cybersecurity resilience in the maritime industry. aims to address (Tabish & Chaur-Luh, 2024).

3. MATERIAL AND METHODS

3.1 Purpose and Scope of the Research

The aim of the research is to analyse the cybersecurity awareness levels of Turkish seafarers and Turkish maritime industry employees. For this purpose, Turkish seafarers who are currently working on ships and people who have ended their working life on ships and who work in maritime industry companies or ports were interviewed and asked to answer a questionnaire consisting of 35 questions in total, 6 of which are demographic and 29 of which are 5-point likert type. As a result of the research, the cybersecurity awareness of Turkish maritime industry employees was analysed and recommendations were made on cybersecurity policies and trainings.

3.2 Methodology and Limitations of the Research

In this study, international and national reports, theses, articles and internet databases have been analysed and the details of interest are listed in the literature section. In the last section, a total of 403 maritime industry employees related to the subject were surveyed as a data collection tool. The survey form is presented in the appendix. The population of the research consists of Turkish seafarers and Turkish maritime industry employees.

The data obtained in this study were analysed with SPSS 25 package programme. Skewness and kurtosis coefficients were used to investigate whether the variables come from a normal distribution, and according to (Tabachnick & Fidell, 2013), if the skewness and kurtosis values are between -1.50 and +1.50, it is accepted that the variables come from a normal distribution.

Exploratory factor analysis was performed for construct validity. Confirmatory factor analysis was performed using AMOS package programme to strengthen the construct validity.

For reliability, the internal consistency coefficient Cronbach's Alpha test statistic was used and the reliability coefficient was determined as $0.00 \leq \alpha < 0.40$ (not reliable); $0.40 \leq \alpha < 0.60$ (low reliability); $0.60 \leq \alpha < 0.80$ (highly reliable) and $0.80 \leq \alpha < 1.00$ (highly reliable) (Kalaycı, 2008). Reliability results were given considering these results.

While analysing the differences between the groups, t and ANOVA tests were used since the variables came from normal distribution. In case of differences in the ANOVA test, differences were calculated with Tukey test by taking into account the assumption of homogeneity of variances. The Pearson correlation tests were utilised to examine the relationship between continuous variables. While interpreting the results, 0.05 was used as the significance level and it was stated that there was a significant difference in case of $p<0.05$ and there was no significant difference in case of $p>0.05$.

3.3 Importance of Research

Cybersecurity is one of the leading contemporary challenges for the entire maritime industry. In this context, cybersecurity, one of the most pressing issues facing the maritime industry today, is critical not only for ensuring system security, preventing accidents, loss of life and environmental damage, but also for national security and the global economy. Cyber-attacks cause the theft of important information, the creation of manipulations or serious financial damage to companies. In this regard, raising the level of awareness of employees together with giving the necessary investment and importance to this field are the necessary measures that can be taken. This research analyses the competencies of Turkish seafarers and Turkish maritime industry employees on cybersecurity awareness levels.

4. RESULTS AND DISCUSSION

4.1 Findings and Evaluation

The questionnaire subject to the research was completed with 403 people. The frequency information regarding the demographic information of the Turkish seafarers and Turkish maritime industry employees who participated in the research is summarised in Table 3.

Table 3. Frequency distribution table for socio-demographic characteristics

Variant	Category	n	%
Age	20 -	20	4,96
	21-30	119	29,53
	31-40	192	47,64
	41-50	53	13,15
	51+	19	4,71
Gender	Female	101	25,06
	Male	302	74,94
Maritime Industry Working Time	0-2 Years	98	24,32
	3-5 Years	65	16,13
	6-8 Years	65	16,13
	9-11 Years	68	16,87
	12-14 Years	43	10,67
	15 Years+	64	15,88
Level of Education	Maritime Course	47	11,66
	Associate degree	75	18,61
	Bachelor	201	49,88
	Postgraduate	47	11,66
	PhD graduate	21	5,21
	Others	12	2,98
Department in the Maritime Industry	Oceangoing Master	64	15,88
	Oceangoing Watchkeeping Off.	117	29,03
	Chief Engineer	19	4,71
	Engine Officer	48	11,91
	Crew	13	3,23
	Company Employee	96	23,82
	Port Management Employee	46	11,41
	Others	0	0,00
Type of Vessel Previously Employed	Tanker & Chemical	161	39,95
	Dry Cargo	131	32,51
	Container	81	20,10
	Ro-Ro	15	3,72
	LPG / LNG	15	3,72
	Others	0	0,00

The largest age group is between 31-40 years old (47.64%). This shows that most of the maritime sector workers are in this age range. The proportions of other age groups are lower, but the 21-30 age group (29.53%) also represents a large percentage. The majority of maritime sector employees are male (74.94 %). The rate of women is lower with 25.06 %. The majority of the employees have been working for less than 6 years (0-2 years: 24.32 % and 3-5 years: 16.13 %). However, the number of experienced employees is also quite high,

with 15.88 % of employees with more than 15 years of experience. The majority of employees have a bachelor's degree (49.88%). Associate degrees (18.61%) and master's degrees (11.66%) are also represented in a significant proportion. However, there are also employees with other levels of education, such as a maritime course (11.66 %) and a doctorate (5.21 %). Oceangoing Watchkeeping Off. (29.03 %) and Oceangoing Master (15.88 %) represent the most common percentage. Company employees (23.82%) also represent a significant percentage. Tankers (39.95%) and dry cargo (32.51%) are the most common vessel types worked. Other vessel types (container, Ro-Ro, LPG / LNG) are also represented at a significant rate.

Table 4. Frequency distribution table for cybersecurity awareness items

Variant	Do not agree		Rarely Agree		Partially Agree		Mostly Agree		Totally Agree	
	n	%	n	%	n	%	n	%	n	%
I have previously received training/course/certificate on information technology systems or cybersecurity.	218	54,09	94	23,33	52	12,90	21	5,21	18	4,47
The vessel / company / port management company I work for provides regular cybersecurity training.	203	50,37	104	25,81	46	11,41	24	5,96	26	6,45
I believe that cybersecurity trainings are important for seafarers and should be compulsory as per STCW.	40	9,93	78	19,35	89	22,08	93	23,08	103	25,56
In the vessel / company / port management company where I work; I believe that more training on cybersecurity should be provided.	47	11,66	86	21,34	117	29,03	116	28,78	37	9,18
In the vessel / company / port management company I work for; we have a plan that addresses the fight against cyber-attacks against possible cyber-attacks.	56	13,90	136	33,75	107	26,55	72	17,87	32	7,94
In the ship / company / port management company I work for; up-to-date information and training bulletins about cyber-attacks are sent regularly in order to increase the awareness of each employee and to know what to do.	75	18,61	40	9,93	99	24,57	117	29,03	72	17,87

I think that the trainings I have received are sufficient in fighting against cyber-attacks.	212	52,61	83	20,60	81	20,10	14	3,47	13	3,23
I am aware of cyber risks during daily use.	33	8,19	57	14,14	111	27,54	104	25,81	98	24,32
I know what a cyber attack is and how to protect against them.	48	11,91	31	7,69	195	48,39	78	19,35	51	12,66
I am aware of cyber-attacks on ships, maritime enterprises, ports and port enterprises with great impact and their consequences.	44	10,92	48	11,91	178	44,17	52	12,90	81	20,10
I know who is responsible for cybersecurity in the vessel / company / port management company I work for.	64	15,88	55	13,65	137	34,00	83	20,60	64	15,88
In the vessel / company / port management company where I work; I know what to do when my computer is infected with a virus.	58	14,39	90	22,33	112	27,79	99	24,57	44	10,92
I use the internet network of the vessel / company / port management company where I work for social media tools.	54	13,40	103	25,56	114	28,29	75	18,61	57	14,14
I open e-mails sent to my corporate or private e-mail without checking the sender; I click on the links.	42	10,42	96	23,82	74	18,36	134	33,25	57	14,14
At the vessel / company / port management company where I work; I do not open a device (flash memory, hard disk, etc.) that I plug into my corporate computers without scanning for viruses.	134	33,25	90	22,33	126	31,27	38	9,43	15	3,72

In the vessel / company / port management company I work for; if you have received an e-mail that your anti-virus is outdated and you are asked to open the attached file to update it, I open it without checking the sender.	69	17,12	84	20,84	126	31,27	91	22,58	33	8,19
If it is necessary to change the passwords of common use external connection equipment or wireless networks in the vessel / company / port management company where I work, I write the new passwords in visible places so that they are accessible.	202	50,12	81	20,10	85	21,09	16	3,97	19	4,71
In the vessel / company / port management company I work for; while creating written rules and policies regarding information security, the dangers and vulnerabilities that may occur in vital areas are taken into consideration.	26	6,45	18	4,47	40	9,93	109	27,05	210	52,11
The vessel / company / port management company I work for has written rules and policies on information security.	28	6,95	19	4,71	41	10,17	113	28,04	202	50,12
In the vessel / company / port management company I work for; protective measures have been taken against all kinds of dangers related to information technologies.	85	21,09	85	21,09	107	26,55	74	18,36	52	12,90
The vessel / company / port management company I work for has taken security measures regarding the use of portable computers or external storage devices.	53	13,15	128	31,76	116	28,78	63	15,63	43	10,67
We have internal security systems, drills and audits to prevent damage to our data in a possible cyber attack against the vessel / company / port management company I work for.	57	14,14	109	27,05	121	30,02	69	17,12	47	11,66
The vessel / company / port management company I work for has a procedure for regular updating of the software of various systems (e.g. transfer systems, ECDIS, information systems, etc.).	66	16,38	124	30,77	127	31,51	55	13,65	31	7,69

In the vessel / company / port management company I work for; operating systems, anti-virus software and other software on computers are regularly updated and audited in their original form.	192	47,64	90	22,33	91	22,58	13	3,23	17	4,22
In the vessel / company / port management company I work for, we have original and continuously updated network security protection programs.	44	10,92	67	16,63	188	46,65	54	13,40	50	12,41
In the vessel / company / port management company I work for; our data is regularly backed up to prevent damage in a possible cyber attack.	170	42,18	55	13,65	75	18,61	61	15,14	42	10,42
In the vessel / company / port management company I work for; each employee has access privileges and limits on the systems.	54	13,40	51	12,66	180	44,67	69	17,12	49	12,16
During the audits, an item related to cybersecurity was written for any system belonging to the vessel / company / port management company I work for.	91	22,58	113	28,04	124	30,77	46	11,41	29	7,20
In the last 12 months, the vessel / company / port management company I work for has been subjected to a cyber attack.	129	32,01	115	28,54	69	17,12	64	15,88	26	6,45

The frequency distribution table of cybersecurity awareness items shows the percentage and weight of the results of the items of the survey according to the answers given.

When we consider the education section among the classified survey questions; 54,09% of the employees disagree with the item "I have received training/course/certificate on information technology systems or cybersecurity" and 23,33% of the employees rarely agree. This shows that many maritime industry employees have not received training on this subject. "The ship/company/port management company I work for provides regular cybersecurity trainings": 50,37% of the employees strongly disagree and 25,81% rarely agree. This shows that many organisations do not provide regular cybersecurity training. "In the ship/company/port management company where I work; I believe there should be more training on cybersecurity": a total of 57,81% of maritime industry employees agree partially or mostly. This shows that many employees demand more training. "I think the trainings I have received on combating cyber-attacks are sufficient": 73.71% rarely or not at all agree. This shows that many maritime industry employees think that the existing trainings are insufficient.

When we consider the awareness section from the categorised survey questions; "I am aware of cyber risks during daily use": 52,35% of maritime industry employees partially or mostly agree. This shows that many maritime industry employees are aware of daily cyber risks. However, "I know who is responsible for cybersecurity in the ship/company/port management company I work for": 49,88% of maritime industry employees partially or mostly agree. This shows that many employees do not know who is responsible for cybersecurity. On the other hand, "In the ship/company/port management company where I work; I know what to do if my computer is infected with a virus": 37,49% of maritime industry employees fully or mostly agree. This shows that many employees do not know what to do in case of virus infection.

When we consider the user behavior section from the categorised survey questions; "I use the internet network of the ship/company/port management company I work for social media tools": 42,85% of the maritime industry employees partly or mostly agree. This shows that

many employees ignore cybersecurity risks when using social media. "I open emails that come to my corporate or private email without checking the sender; I click on links": 47,39% of maritime industry employees fully or mostly agree. This shows that many employees are careless about e-mail security. "If the passwords of the common use external connection equipment or wireless networks in the ship/company/port management company I work for need to be changed, I write the new passwords in visible places so that they are accessible": 71,21% of maritime industry employees rarely or never agree. This shows that many employees are careless about password security and completely ignore cybersecurity risks.

When we consider the rules and policies section from the categorised survey questions; "In the ship/company/port management company I work for; when creating written rules and policies on information security, hazards and vulnerabilities in vital areas are taken into account": 79,16% of maritime industry employees partially or mostly agree. This shows that the safety policies of many organisations cover vital areas. similarly, the existence of rules and policies in other items was reported by the employees. "In the ship/company/port management company where I work; protective measures have been taken against all kinds of hazards related to information technologies": 69,64% of maritime industry employees partially or mostly agree. This shows that many organisations have taken protective measures. "In the ship/company/port management company I work for; our data is backed up regularly to prevent damage in a possible cyber attack": 57,81% of maritime industry employees partially or mostly agree. This shows that many organisations also have a data backup policy.

When we consider the experiences section from the categorised survey questions; although in the rules and practices section, maritime industry employees state that there are sufficient rules and practices in the places where they work, in the experience section, it is seen that there are problems in implementing these rules and practices. "During the inspections, an article regarding cybersecurity was written for any system belonging to the ship/company/port management company I work for": 64.62% of maritime industry employees partially or mostly agree. This shows that although there are rules during inspections, there are gaps in cybersecurity in practice. “The ship/company/port management company I work for has been subject to a cyber attack in the last 12 months”:

60.55% of maritime industry employees partially or mostly agree. This shows that many businesses have been subject to cyber attacks recently, indicating that this situation is common.

Table 5. Cybersecurity awareness scale explanatory factor analysis and normality test result

Factor Name	Question Phrase	Factor Weights	Reliability	Factor Explanatory (%)
Education	m1	0,538	0,810	30,82
	m2	0,519		
	m3	0,619		
	m4	0,801		
	m5	0,677		
	m6	0,536		
	m7	0,528		
Awareness	m8	0,539	0,826	10,76
	m9	0,697		
	m10	0,592		
	m11	0,577		
	m12	0,744		
User Behavior	m13	0,805	0,901	8,18
	m14	0,659		
	m15	0,694		
	m16	0,652		
	m17	0,421		
Rules and Policies	m18	0,725	0,855	7,61
	m19	0,783		
	m20	0,600		
	m21	0,689		
	m22	0,785		
	m23	0,727		
	m24	0,556		
	m25	0,527		
Experiences	m26	0,671	0,836	5,76
	m27	0,523		
	m28	0,678		
	m29	0,739		
Total			0,910	63,13
KMO Validity				0,897
Barlett		Chi-Square		7433,92
		p		0,001*

The table 5, presents the results of an exploratory factor analysis conducted to assess the construct validity of a cybersecurity awareness scale used in a study of maritime industry employees. The table includes factor names, question phrases, factor weights, reliability coefficients, and the percentage of variance explained by each factor.

The primary purpose of conducting an exploratory factor analysis is to determine the construct validity of the cybersecurity awareness scale. Construct validity ensures that the scale accurately measures the concept it is intended to measure, which in this case is the cybersecurity awareness among maritime industry employees.

The construct validity of the scales used in the study was firstly evaluated by exploratory factor analysis. In order to test the suitability of the data set for factor analysis in the cybersecurity awareness scale, Kaiser-Meyer-Olkin (KMO) sampling adequacy and Barlett's sphericity test were applied. Since the KMO value was found to be 0.897, which is above the acceptable limit of 0.70, and the Barlett's sphericity test was above 0.50 and significant at 0.05 significance level, the data set was found suitable for factor analysis. The KMO coefficient signifies the appropriateness of the data for analysis. Given the absence of items under the factor, no statement was excluded from the analysis. Five factors, each possessing eigenvalues equal to or greater than 1, were extracted. The cumulative variance explained amounted to 63.13%, a notably high figure. This surpasses the widely accepted lower threshold of 60% deemed optimal for social sciences, thus affirming the construct validity of the model. Understanding how much of the total variance in responses is explained by each factor is critical. It indicates the importance of each factor in explaining differences in cybersecurity awareness. The factors were named as "Education", "Awareness", "User Behaviour", "Rules and Policies" and "Experience" respectively. Table 5 shows the factor analysis results of the cybersecurity awareness scale. The findings obtained from the exploratory factor analysis show that the model provides construct validity. The construct validity of the structure revealed by the explanatory factor analysis will be made stronger by confirmatory factor analysis.

For reliability, the internal consistency coefficient Cronbach's Alpha test statistic was used and the reliability coefficient was determined as $0.00 \leq \alpha < 0.40$ (not reliable); $0.40 \leq \alpha <$

0.60 (low reliability); $0.60 \leq \alpha < 0.80$ (highly reliable) and $0.80 \leq \alpha < 1.00$ (highly reliable) (Kalaycı, 2008). Reliability results were given by taking into consideration. It is seen that the scale levels are highly reliable.

In summary, the exploratory factor analysis and reliability tests were conducted to validate the cybersecurity awareness scale, ensure its reliability, understand its dimensionality, and confirm the suitability of the data for such analysis. These steps are crucial for ensuring that the scale is both accurate and reliable, thereby providing a solid foundation for further research and practical applications in improving cybersecurity awareness in the maritime industry.

Table 6. The result of confirmatory factor analysis of cybersecurity awareness scale

Index of Concordance	Realised Value	Comment
Chi-Square/df	2,654	Goodness of fit= <5
GFI	0,86	Goodness of fit =>.90
AGFI	0,873	Goodness of fit =>.85
NFI	0,902	Acceptable fit =>.95
IFI	0,936	Goodness of fit =>.90
CFI	0,936	Goodness of fit =>.95
RMSEA	0,07	Goodness of fit = <.08

Table 6 presents the results of the confirmatory factor analysis conducted on the cybersecurity awareness scale. The confirmatory factor analysis is used to verify the factor structure identified in the exploratory factor analysis and to assess the overall fit of the model.

The primary purpose of confirmatory factor analysisis to test whether the data fit a hypothesized measurement model. The confirmatory factor analysis is used to assess the construct validity of the cybersecurity awareness scale. Evaluating various goodness-of-fit indices helps in determining how well the model fits the observed data. Good fit indices suggest that the model adequately represents the data and that the underlying constructs are well-defined.

The fit index values are given in Table 6. According to the confirmatory factor analysis results obtained with AMOS, it is seen that there is a good fit between the chi-square test and the model (p<0,05). The x2/df obtained as a result of the fits between the covariance matrix of the sample and the estimated covariance matrix of the model shows good fit with 2,654, Goodness of fit index value (GFI) shows good fit with 0,860, Adjusted goodness of fit index (AGFI) shows good fit with 0,873, Normed Fit Index (NFI) showed acceptable fit with 0.902, Incremental Fit Index (IFI) showed good fit with 0.936, Comparative Fit Index (CFI) showed good fit with 0.936 and Root Mean Square Error of Approximation (RMSEA) showed good fit with 0.07.

In summary, the confirmatory factor analysis was conducted to validate the factor structure identified in the exploratory factor analysis, assess the construct validity, and determine the overall fit of the model. The fit indices presented in Table 6 indicate that the model provides a good fit to the data, thereby confirming the reliability and validity of the cybersecurity awareness scale for maritime industry employees. This validation is essential for developing effective training programs and interventions aimed at improving cybersecurity awareness in the maritime sector.

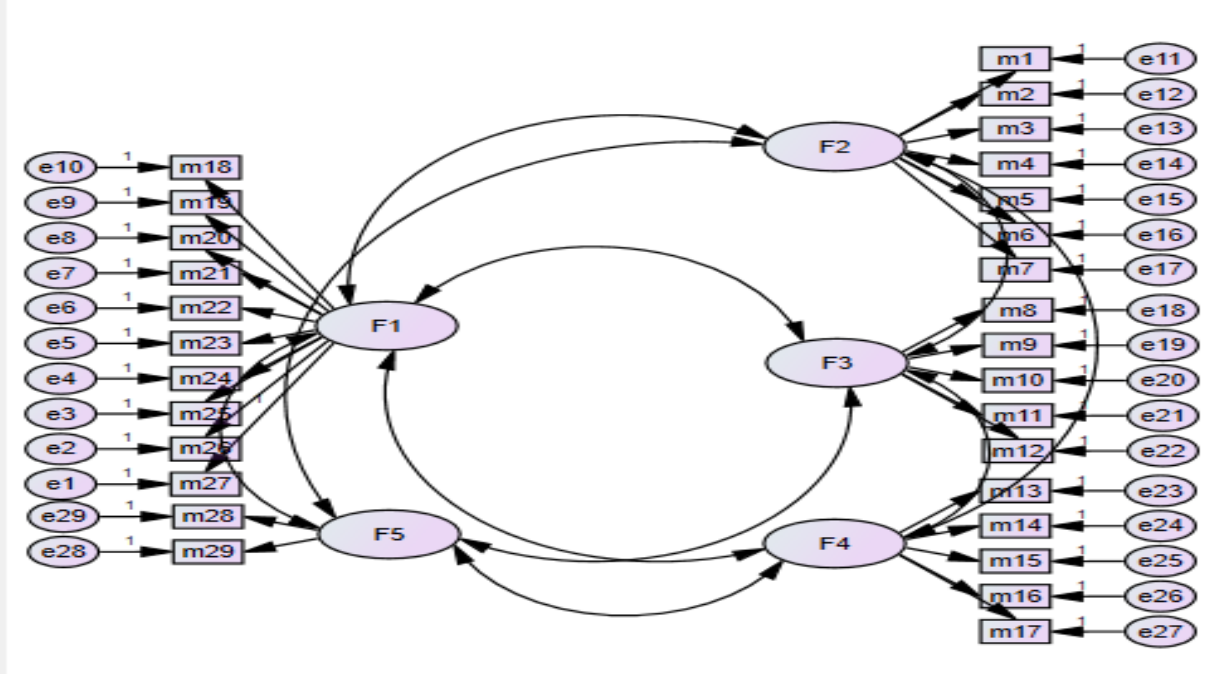

Figure 8: Cyber security safe path diagram

Table 7. Frequency distribution and normality test results of cybersecurity awareness scale

Variant	Average	Min.	Max.	SD	Skewness	Kurtosis
Education	17,86	7,00	32,00	4,58	0,415	0,359
Awareness	15,79	5,00	25,00	4,76	-0,140	-0,075
User Behavior	13,16	5,00	25,00	3,99	0,124	0,051
Rules and Policies	29,68	10,00	50,00	6,53	-0,157	1,378
Experiences	4,89	2,00	10,00	2,22	0,505	-0,616
Cyber Security Awareness Level	81,38	29,00	135,00	18,58	0,156	0,687

Table 7 presents the descriptive statistics and normality test results for the cybersecurity awareness scale, including its sub-factors: Education, Awareness, User Behavior, Rules and Policies, Experiences, and overall Cyber Security Awareness Level. The table provides the average (mean), minimum (Min.), maximum (Max.), standard deviation (SD), skewness, and kurtosis for each variant.

The questionnaire was designed as a 5-point Likert type; 1: Do not agree at all, 2: Rarely agree, 3: Partially agree, 4: Mostly agree, 5: Totally agree. In statistical analysis applications, skewness and kurtosis measures basically give us information about the general distribution of our data, their conformity to normal distribution and outliers. As the median and average approach each other, the skewness approaches zero. If the average is smaller than the median value, there is a negative skewness, and if it is larger, there is a positive skewness. In kurtosis, if the kurtosis value is positive, the curve is steeper and if it is negative, it is flatter (Kalaycı, 2008). The entire scale was analysed and skewness and kurtosis values should be distributed between -1.5 and +1.5. The results presented in Table 5 are within this range and show that the scale is generally normally distributed.

The average education level was found to be 17.86. The minimum education level is 7 and the maximum is 32. The standard deviation is 4.58, which shows how variable this distribution is. The skewness and kurtosis values of 0.415 and 0.359, respectively, indicate that this distribution is relatively non-normal.

The average of awareness is 15.79 and the standard deviation is 4.76. The minimum and maximum values are 5 and 25, respectively. Skewness -0,140 and kurtosis -0,075 values show that this distribution is somewhat negatively skewed and kurtosis.

The average user behaviour level is 13.16 and the standard deviation is 3.99. The minimum and maximum values are 5 and 25 respectively. The values of skewness 0.124 and kurtosis 0.051 indicate that this distribution is relatively normal.

The average level of rules and policies is 29.68 with a standard deviation of 6.53. The minimum and maximum values are 10 and 50 respectively. The values of skewness -0.157 and kurtosis 1.378 indicate that this distribution is negatively skewed and highly kurtotic.

The average experience level is 4.89 and the standard deviation is 2.22. The minimum and maximum values are 2 and 10 respectively. Skewness 0.505 and kurtosis -0.616 values show that this distribution is positively skewed and negatively kurtotic.

The average cybersecurity awareness level is 81.38 and the standard deviation is 18.58. The minimum and maximum values are 29 and 135, respectively. Skewness 0,156 and kurtosis 0,687 show that this distribution is positively skewed and highly skewed.

The analysis presented in Table 7 is a crucial step in validating the cybersecurity awareness scale and ensuring the robustness of subsequent statistical analyses. The descriptive statistics and normality tests confirm that the data is generally well-distributed, with minor deviations from normality, thus supporting the reliability and validity of the scale. This lays a strong foundation for further investigations into the factors influencing cybersecurity awareness among maritime industry employees and informs the development of targeted training programs.

Table 8. Comparison of cybersecurity awareness scale levels with age groups

Variant	Category	Age		ANOVA		
		Ave.	SD	F	p	Difference
Education	20 – (1)	17,30	4,69	0,341	0,851	-
	21-30 (2)	17,65	4,62			
	31-40 (3)	18,10	4,14			
	41-50 (4)	17,89	5,71			
	51+ (5)	17,32	5,29			
Awareness	20 – (1)	15,10	4,52	0,893	0,468	-
	21-30 (2)	15,70	5,11			
	31-40 (3)	16,19	4,48			
	41-50 (4)	15,13	5,06			
	51+ (5)	14,84	4,57			
User Behavior	20 – (1)	12,25	4,04	1,069	0,371	-
	21-30 (2)	13,45	4,30			
	31-40 (3)	13,34	3,77			
	41-50 (4)	12,40	4,05			
	51+ (5)	12,68	3,84			
Rules and Policies	20 – (1)	27,95	6,46	2,118	0,078	-
	21-30 (2)	29,10	6,91			
	31-40 (3)	30,46	6,17			
	41-50 (4)	28,28	7,10			
	51+ (5)	31,05	5,05			
Experiences	20 – (1)	4,30	1,89	1,479	0,208	-
	21-30 (2)	4,59	2,23			
	31-40 (3)	5,12	2,22			
	41-50 (4)	5,00	2,25			
	51+ (5)	4,74	2,21			
Cyber Security Awareness Level	20 – (1)	76,90	18,63	1,116	0,348	-
	21-30 (2)	80,48	19,29			
	31-40 (3)	83,22	17,29			
	41-50 (4)	78,70	21,44			
	51+ (5)	80,63	17,71			

**p<0,05; F=ANOVA Test, Difference=Tukey Test*

Table 8 presents the results of an ANOVA analysis comparing cybersecurity awareness scale levels across different age groups. The table includes various categories such as Education, Awareness, User Behavior, Rules and Policies, Experiences, and overall Cyber Security Awareness Level. The age groups examined are 20 and below, 21-30, 31-40, 41-50, and 51 and above.

The analysis aims to investigate whether there are significant differences in cybersecurity awareness levels across different age groups. This is important to identify potential gaps in awareness and tailor cybersecurity education and training programs accordingly. By understanding the variations in awareness, user behavior, and experiences among different age demographics, policymakers and educators can develop targeted interventions to improve overall cybersecurity preparedness and resilience. The use of ANOVA allows for the examination of multiple groups simultaneously to determine if any of the observed differences are statistically significant.

The ANOVA test for each variable shows that there is no statistically significant difference between education, awareness, user behaviour, rules and policies, experience and cybersecurity awareness levels according to age categories. This shows that age does not have a determining effect on these variables.

While the analysis did not reveal significant differences in cybersecurity awareness across age groups, it achieved the objective of clarifying that age alone may not be a critical factor in cybersecurity awareness. This insight is valuable for guiding future research and shaping cybersecurity education and policy initiatives to consider a broader range of influencing factors. The uniformity in awareness levels also suggests that broad, inclusive educational strategies may be effective in enhancing cybersecurity awareness across the population.

Table 9. Comparison of cybersecurity awareness scale levels with gender

Variant	Gender				t test	
	Female		Male			
	Ave.	SD	Ave.	SD	t	p
Education	17,36	4,15	18,03	4,72	-1,285	0,199
Awareness	15,50	4,64	15,88	4,80	-0,711	0,477
User Behavior	13,90	4,05	12,92	3,94	2,156	**0,032***
Rules and Policies	29,39	6,58	29,77	6,52	-0,518	0,605
Experiences	4,77	2,28	4,93	2,20	-0,606	0,545
Cyber Security Awareness Level	80,91	18,14	81,54	18,75	-0,293	0,771

**p<0,05; t= Independent Sample t-test*

Table 9 presents the results of an independent sample t-test comparing cybersecurity awareness scale levels between female and male participants across various categories, including Education, Awareness, User Behavior, Rules and Policies, Experiences, and overall Cyber Security Awareness Level.

The analysis aimed to determine whether there are statistically significant differences in cybersecurity awareness levels between female and male participants. This analysis sought to achieve several objectives.

There was no statistically significant difference between female and male in terms of educational level (p=0,199). There was no statistically significant difference between female and male in terms of awareness level (p=0,477). A statistically significant difference was found between female and male in terms of user behaviour level (p=0,032). This shows that user behaviour scores may vary depending on gender. No statistically significant difference was found between female and male in terms of their level of rules and policies (p=0,605). There was no statistically significant difference between female and male in terms of

experience level (p=0,545). There was no statistically significant difference between female and male in terms of cybersecurity awareness level (p=0,771). The analysis revealed a significant difference in the user behavior category, with females scoring higher than males. This suggests that females might exhibit better cybersecurity behaviors than males.

The analysis aimed to identify gender-based differences in cybersecurity awareness to inform targeted interventions and improve cybersecurity strategies. While a significant difference was found in user behavior, with females exhibiting better behaviors, no significant differences were observed in other categories. These findings suggest that, except for user behavior, cybersecurity awareness levels are generally similar across genders, indicating that broad-based cybersecurity education and training programs may be effective for both female and male participants.

Table 10. Comparison of cybersecurity awareness scale levels with working time in maritime industry

Variant	Category	Maritime Industry Working Time		ANOVA		
		Ave.	SD	F	p	Difference
Education	0-2 Years (1)	17,47	4,98	1,487	0,193	-
	3-5 Years (2)	16,98	3,39			
	6-8 Years (3)	18,46	3,63			
	9-11 Years (4)	18,26	5,22			
	12-14 Years (5)	18,95	5,22			
	15 Years+ (6)	17,59	4,61			
Awareness	0-2 Years (1)	15,19	5,33	1,573	0,167	-
	3-5 Years (2)	15,29	3,89			
	6-8 Years (3)	16,23	4,50			
	9-11 Years (4)	15,99	5,03			
	12-14 Years (5)	17,35	4,83			
	15 Years+ (6)	15,48	4,39			
User Behavior	0-2 Years (1)	12,91	4,54	0,968	0,437	-
	3-5 Years (2)	13,05	3,23			
	6-8 Years (3)	13,57	3,89			
	9-11 Years (4)	12,94	4,00			
	12-14 Years (5)	14,21	4,12			
	15 Years+ (6)	12,80	3,77			
Rules and Policies	0-2 Years (1)	28,37	7,03	1,715	0,13	-
	3-5 Years (2)	29,12	5,09			
	6-8 Years (3)	30,49	6,68			
	9-11 Years (4)	30,34	6,71			
	12-14 Years (5)	31,21	6,33			
	15 Years+ (6)	29,69	6,62			
Experiences	0-2 Years (1)	4,34	2,22	3,021	**0,011***	1<5
	3-5 Years (2)	4,68	1,84			
	6-8 Years (3)	5,15	2,39			
	9-11 Years (4)	5,31	2,50			
	12-14 Years (5)	5,60	2,16			
	15 Years+ (6)	4,75	1,94			
Cyber Security Awareness Level	0-2 Years (1)	78,28	19,94	2,012	0,076	-
	3-5 Years (2)	79,12	13,72			
	6-8 Years (3)	83,91	18,19			
	9-11 Years (4)	82,84	20,22			
	12-14 Years (5)	87,33	19,61			
	15 Years+ (6)	80,31	17,79			

**p<0,05; F=ANOVA Test, Difference =Tukey Test*

This table presents the results of an ANOVA test comparing cybersecurity awareness across different working time categories in the maritime industry. The categories examined are Education, Awareness, User Behavior, Rules and Policies, Experiences, and Cyber Security Awareness Level. Each category is subdivided into different working time groups, and the

analysis evaluates the mean scores (Ave.), standard deviations (SD), F-values, p-values, and significant differences between groups.

The primary purpose of conducting this ANOVA analysis was to determine whether there are significant differences in cybersecurity awareness levels across different working time categories within the maritime industry. The goal was to identify if the duration of working experience impacts the awareness and behavior related to cybersecurity.

There was no statistically significant difference between the averages of education level according to the duration of working in the maritime industry (p=0,193). No statistically significant difference was found between the averages according to the duration of working in the maritime industry in terms of awareness level (p=0,167). No statistically significant difference was found between the averages according to the duration of employment in the maritime industry in terms of user behaviour levels (p=0,437). There is a slight difference between the levels according to the duration of working in the maritime industry in terms of rules and policies, but this difference is not statistically significant (p=0,13). There is a statistically significant difference between the levels of experience according to the duration of working in the maritime industry (p=0,011). According to the results of Tukey test, it is stated that there is a significant difference between group 1 and group 5. In terms of cybersecurity awareness level, there is a slight difference between the averages according to the duration of working in the maritime industry, but this is not statistically significant (p=0,076).

In summary, the analysis provides valuable insights into how working time correlates with various aspects of cybersecurity awareness in the maritime industry. While most categories showed no significant differences, the significant finding in the Experiences category highlights the need for targeted interventions for new employees to enhance their cybersecurity experiences.

Table 11. Comparison of cybersecurity awareness scale levels with education levels

Variant	Category	Education Level		ANOVA		
		Ave.	SD	F	p	Difference
Education	Maritime Course (1)	17,23	5,36	1,192	0,312	-
	Associate degree (2)	18,35	4,64			
	Bachelor (3)	17,63	4,45			
	Postgraduate (4)	18,70	3,91			
	PhD graduate (5)	18,76	5,00			
	Others (6)	16,33	4,85			
Awareness	Maritime Course (1)	15,77	5,89	0,911	0,475	-
	Associate degree (2)	16,32	4,10			
	Bachelor (3)	15,44	4,90			
	Postgraduate (4)	16,15	4,15			
	PhD graduate (5)	17,10	3,66			
	Others (6)	14,67	4,98			
User Behavior	Maritime Course (1)	12,81	4,58	1,403	0,222	-
	Associate degree (2)	13,99	3,76			
	Bachelor (3)	12,81	3,95			
	Postgraduate (4)	13,55	3,87			
	PhD graduate (5)	14,00	4,09			
	Others (6)	12,42	3,48			
Rules and Policies	Maritime Course (1)	29,00	7,78	1,425	0,214	-
	Associate degree (2)	30,91	6,61			
	Bachelor (3)	29,30	6,34			
	Postgraduate (4)	29,79	6,14			
	PhD graduate (5)	31,52	4,85			
	Others (6)	27,33	7,05			
Experiences	Maritime Course (1)	4,81	2,29	0,761	0,579	-
	Associate degree (2)	5,08	2,36			
	Bachelor (3)	4,78	2,18			
	Postgraduate (4)	4,79	2,25			
	PhD graduate (5)	5,67	2,03			
	Others (6)	4,92	2,11			
Cyber Security Awareness Level	Maritime Course (1)	79,62	23,47	1,481	0,198	-
	Associate degree (2)	84,64	17,37			
	Bachelor (3)	79,95	18,22			
	Postgraduate (4)	82,98	16,67			
	PhD graduate (5)	87,05	15,83			
	Others (6)	75,67	19,92			

**p<0,05; F=ANOVA Test, Difference =Tukey Test*

This table displays the results of an ANOVA test that compares cybersecurity awareness across different education levels in the maritime industry. The categories analyzed are

Education, Awareness, User Behavior, Rules and Policies, Experiences, and Cyber Security Awareness Level. Each category is further subdivided based on education levels, and the table provides mean scores (Ave.), standard deviations (SD), F-values, p-values, and significant differences between groups.

The purpose of conducting this ANOVA analysis was to investigate whether there are significant differences in cybersecurity awareness levels across various education levels within the maritime industry. This analysis aimed to determine if the level of education influences individuals' cybersecurity awareness and behaviors.

The analysis found no significant differences in cybersecurity education, awareness, user behavior, rules and policies, experiences, and overall cybersecurity awareness level across different education levels. Despite variations in average scores among the education levels, none of the categories showed statistically significant differences.

In summary, the analysis indicates that education level does not significantly impact cybersecurity awareness and behaviors in the maritime industry.

Table 12. Comparison of cybersecurity awareness scale levels with the departments worked in maritime industry

Variant	Category	Department Worked in		ANOVA		
		Ave.	SD	F	p	Difference
Education	Oceangoing Master (1)	18,25	5,50	0,747	0,612	-
	Oceangoing Watchkeeping Off. (2)	17,47	4,44			
	Chief Engineer (3)	19,21	3,98			
	Engine Officer (4)	18,06	3,53			
	Crew (5)	17,15	6,23			
	Company Employee (6)	18,11	4,71			
	Port Management Employee (7)	17,24	4,01			
Awareness	Oceangoing Master (1)	16,22	5,08	1,338	0,239	-
	Oceangoing Watchkeeping Off. (2)	15,52	4,71			
	Chief Engineer (3)	16,74	4,38			
	Engine Officer (4)	14,46	4,48			
	Crew (5)	14,38	6,27			
	Company Employee (6)	16,20	4,52			
	Port Management Employee (7)	16,39	4,76			
User Behavior	Oceangoing Master (1)	13,25	4,29	0,287	0,943	-
	Oceangoing Watchkeeping Off. (2)	13,08	4,02			
	Chief Engineer (3)	13,74	3,41			
	Engine Officer (4)	12,79	3,81			
	Crew (5)	12,31	4,42			
	Company Employee (6)	13,35	4,17			
	Port Management Employee (7)	13,26	3,48			
Rules and Policies	Oceangoing Master (1)	29,88	6,09	1,411	0,209	-
	Oceangoing Watchkeeping Off. (2)	28,90	7,12			
	Chief Engineer (3)	31,00	6,57			
	Engine Officer (4)	29,44	5,61			
	Crew (5)	26,85	9,23			
	Company Employee (6)	30,89	6,04			
	Port Management Employee (7)	29,37	6,34			
Experiences	Oceangoing Master (1)	5,33	2,23	0,729	0,626	-
	Oceangoing Watchkeeping Off. (2)	4,78	2,31			
	Chief Engineer (3)	5,00	1,97			
	Engine Officer (4)	4,52	2,15			
	Crew (5)	5,15	2,34			
	Company Employee (6)	4,84	2,24			
	Port Management Employee (7)	4,91	2,09			
Cyber Security Awareness Level	Oceangoing Master (1)	82,92	20,11	0,878	0,511	-
	Oceangoing Watchkeeping Off. (2)	79,74	19,16			
	Chief Engineer (3)	85,68	17,01			
	Engine Officer (4)	79,27	16,25			
	Crew (5)	75,85	27,10			
	Company Employee (6)	83,40	17,53			
	Port Management Employee (7)	81,17	17,14			

**p<0,05; F=ANOVA Test, Difference=Tukey Test*

This table presents the results of an ANOVA test comparing cybersecurity awareness across different departments within the maritime industry. The categories examined include Education, Awareness, User Behavior, Rules and Policies, Experiences, and Cyber Security Awareness Level. Each category is analyzed based on the department, and the table provides mean scores (Ave.), standard deviations (SD), F-values, p-values, and significant differences between groups.

The primary purpose of conducting this ANOVA analysis was to determine whether there are significant differences in cybersecurity awareness levels across different departments within the maritime industry. This analysis aimed to understand how the specific department in which an individual works influences their awareness and behavior related to cybersecurity.

The analysis found no significant differences in cybersecurity education, awareness, user behavior, rules and policies, experiences, and overall cybersecurity awareness level across different departments. Despite variations in average scores among the departments, none of the categories showed statistically significant differences.

In summary, the analysis indicates that the department in which an individual works does not significantly impact cybersecurity awareness and behaviors in the maritime industry.

Table 13. Comparison of cybersecurity awareness scale levels with the most recent ship type

Variant	Category	Type of Vessel Last Employed		ANOVA		
		Ave.	SD	F	p	Difference
Education	Tanker&Chem (1)	17,60	4,07	0,383	0,821	-
	Dry Cargo (2)	18,10	4,98			
	Container (3)	17,78	4,94			
	Ro-Ro (4)	18,33	3,99			
	LPG / LNG (5)	18,67	5,05			
Awareness	Tanker&Chem (1)	15,35	4,52	1,406	0,231	-
	Dry Cargo (2)	15,84	4,68			
	Container (3)	16,09	5,25			
	Ro-Ro (4)	16,00	4,61			
	LPG / LNG (5)	18,20	4,97			
User Behavior	Tanker&Chem (1)	13,09	3,75	0,291	0,884	-
	Dry Cargo (2)	13,02	3,87			
	Container (3)	13,56	4,59			
	Ro-Ro (4)	12,80	4,04			
	LPG / LNG (5)	13,40	4,26			
Rules and Policies	Tanker&Chem (1)	29,65	5,47	0,294	0,882	-
	Dry Cargo (2)	29,72	6,53			
	Container (3)	29,99	7,80			
	Ro-Ro (4)	28,00	8,37			
	LPG / LNG (5)	29,60	8,00			
Experiences	Tanker&Chem (1)	4,81	2,12	0,709	0,586	-
	Dry Cargo (2)	5,00	2,32			
	Container (3)	4,72	2,35			
	Ro-Ro (4)	4,87	1,96			
	LPG / LNG (5)	5,67	1,99			
Cyber Security Awareness Level	Tanker&Chem (1)	80,50	16,37	0,337	0,853	-
	Dry Cargo (2)	81,68	18,90			
	Container (3)	82,12	21,58			
	Ro-Ro (4)	80,00	19,01			
	LPG / LNG (5)	85,53	21,74			

**p<0,05; F=ANOVA Test, Difference=Tukey Test*

This table presents the results of an ANOVA test comparing cybersecurity awareness across different types of vessels recently employed by personnel in the maritime industry. The categories analyzed include Education, Awareness, User Behavior, Rules and Policies,

Experiences, and Cyber Security Awareness Level. Each category is analyzed based on the type of vessel, and the table provides mean scores (Ave.), standard deviations (SD), F-values, p-values, and significant differences between groups.

The primary purpose of conducting this ANOVA analysis was to determine whether there are significant differences in cybersecurity awareness levels across different types of vessels recently employed by personnel within the maritime industry. This analysis aimed to understand how the type of vessel influences individuals' cybersecurity awareness and behaviors.

The analysis found no significant differences in cybersecurity education, awareness, user behavior, rules and policies, experiences, and overall cybersecurity awareness level across different vessel types. Despite variations in average scores among the vessel types, none of the categories showed statistically significant differences. The lack of significant differences across vessel types implies a need for uniform cybersecurity training and awareness programs that can be effective regardless of the specific vessel type.

The results of this analysis emphasize the importance of comprehensive and inclusive cybersecurity programs that address the needs of all personnel in the maritime industry, ensuring that cybersecurity awareness is maintained at a high level across all types of vessels.

Table 14. Relationship among scale levels

		Education	Awareness	User Behavior	Rules and Policies	Experiences	Cyber Security Awareness Level
Education	r	1					
	p						
	N	403					
Awareness	r	,602**	1				
	p	**0,001***					
	N	403	403				
User Behavior	r	,545**	,759**	1			
	p	**0,001***	**0,001***				
	N	403	403	403			
Rules and Policies	r	,536**	,696**	,645**	1		
	p	**0,001***	**0,001***	**0,001***			
	N	403	403	403	403		
Experiences	r	,601**	,653**	,555**	,633**	1	
	p	**0,001***	**0,001***	**0,001***	**0,001***		
	N	403	403	403	403	403	
Cyber Security Awareness Level	r	,778**	,890**	,836**	,876**	,777**	1
	p	**0,001***	**0,001***	**0,001***	**0,001***	**0,001***	
	N	403	403	403	403	403	403

*p<0,05; ** Correlation Coefficient

This table presents the correlation coefficients (r) and significance levels (p) for the relationships between different aspects of cybersecurity awareness: Education, Awareness, User Behavior, Rules and Policies, Experiences, and Cyber Security Awareness Level. The table includes data from 403 respondents.

The primary purpose of conducting this correlation analysis was to determine the strength and significance of the relationships among various aspects of cybersecurity awareness within the maritime industry. This analysis aimed to uncover how different dimensions of cybersecurity awareness are interrelated and to identify the most influential factors contributing to overall cybersecurity awareness.

The analysis revealed significant correlations between all aspects of cybersecurity awareness, indicating that improvements in one area are likely to positively impact others.

There is a positive and medium relationship (r=0,602) between education level and awareness (p<0,001). This result is interpreted as awareness is positively affected as the level of education increases. There is a positive and medium relationship (r=0,545) between education level and user behaviour (p<0,001). Likewise, as the level of education increases, user behaviour increases positively. A positive and medium relationship (r=0,536) was found between education level and rules and policies (p<0,001). The effect of increasing education level on rules and policies is positive. A positive and medium relationship (r=0,601) was found between education level and experience (p<0,001). The increase in the education level positively affects the experience of the individuals. A positive and high (r=0,778) relationship was found between education level and cybersecurity awareness level (p<0,001). This result shows that the higher the level of education, the higher the level of cybersecurity awareness.

Similarly, there are strong and positive relationships between cybersecurity awareness level and other variables (r values between 0.777 and 0.890 and p values <0.001). As the education and awareness levels of individuals increase, their cybersecurity awareness levels also show a strong increase. The more positive the user behaviours are, the more positively the cybersecurity awareness level is positively affected. The existence of rules and policies also strongly and positively affects cybersecurity awareness. The experiences of people in their professions also strongly increase their cybersecurity awareness.

In summary, the analysis highlights the interconnectedness of various aspects of cybersecurity awareness. It suggests that a comprehensive approach targeting multiple dimensions particularly Awareness, User Behavior, and Education could be most effective in enhancing overall cybersecurity awareness within the maritime industry. The findings underscore the need for integrated strategies that address these interrelated components to improve cybersecurity practices holistically.

Table 15. Suggestions for increasing the cybersecurity awareness level of maritime industry employees

Suggestions	f	%
Education programmes can be planned for taking the necessary security measures and using the necessary applications.	74	18,36
Courses or certificate programmes on cyber security can be implemented in the relevant departments of universities.	70	17,36
Legal penalties or applications related to cybersecurity at maritime can be increased.	11	2,72
A harmless link attack can be organised by the authorities in the companies to raise awareness.	19	4,71
Compatible virus protection programmes can be installed on every technological device used on board ships.	14	3,47
Access authorisation to computers and internet-connected devices on board ships can be restricted.	9	2,23
Corporate e-mail addresses can be banned for personal use.	11	2,72
If cyber incidents experienced in the maritime industry are shared, it can be preventative for possible incidents.	18	4,46
Maritime industry employees can be raised awareness to take necessary precautions.	54	13,39
If current brochures are regularly published in a remarkable way, maritime industry employees can be informed about cybersecurity.	42	10,42
The importance of cyber training and company policy should be explained to the staff and officers by the office staff before joining the ships.	81	20,09

This table provides a list of suggestions to enhance cybersecurity awareness among maritime industry employees, along with the frequency (f) and percentage (%) of respondents who endorsed each suggestion.

The purpose of conducting this analysis was to gather and prioritize actionable suggestions from maritime industry employees to enhance cybersecurity awareness within the industry. By identifying the most endorsed suggestions, the aim was to provide a strategic framework for implementing effective cybersecurity training and policy measures.

At the end of the survey, maritime industry employees were asked for their suggestions for increasing the level of awareness. When these suggestions are analysed, it is seen that many suggestions converge on common points, although their priority ranking is different from each other. As a result of the study, it is seen that the suggestions for increasing the level of cybersecurity awareness are frequently shared by the maritime industry employees (f=81, %=20,09) regarding the importance of cyber training and company policy to the personnel and officers by the office staff before joining the ships. It can be said that many problems related to cybersecurity are caused by the lack of training of maritime industry employees on the subject. It is observed that the second most frequently shared result by the maritime industry employees is the suggestion that trainings should be planned to increase the level of cybersecurity awareness, to take the necessary security measures and to use the necessary applications (f=74, %=18,36). Likewise, the percentage of employees who suggested that training programmes should be implemented in universities is also quite high (f=70, %=17,36).

When other suggestions of maritime industry employees to increase the level of cybersecurity are analysed;

"Legal penalties or practices can be increased." The percentage of employees who gave the following suggestion is 2.72. This can be interpreted as legal sanctions will necessarily raise awareness.

"A harmless link attack can be organised." The percentage of employees giving suggestions is 4.71. This suggestion suggests that the dangers related to cybersecurity are caused by carelessness and ignorance, and that it is necessary to have awareness to prevent cyber attacks.

"Compatible virus protection programmes can be installed." The percentage of employees who gave such a suggestion is 3.47. This suggestion shows that employees think that they will not have a problem with cybersecurity when appropriate virus programmes are installed.

"Access authorisation can be restricted." The percentage of employees who gave the suggestion is 2.23. This suggestion shows that employees think that they will not have a problem with cybersecurity if they have access authorisation.

"E-mail addresses can be banned for personal use." The percentage of employees who gave the suggestion is 2.72. This suggestion, similar to the suggestion of access authorisation, shows that employees think that they will not have a problem with cybersecurity by providing some restrictions.

"Cyber incidents can be preventive if shared." The percentage of employees who gave such a suggestion is 4.46. This suggestion points to the power of sharing. Employees think that the higher the level of sharing, the higher the level of awareness of people.

"Employees can be made aware." The percentage of employees who gave the following suggestion is 13.39. This suggestion states that possible cybersecurity problems are caused by lack of awareness. It suggests that raising awareness of employees is possible through training.

"Regular brochures can be published." The percentage of employees who gave such a suggestion is 10.42. This suggestion shows that possible cybersecurity problems are caused by lack of information.

The maritime industry employees who expressed their opinions state that they think that the problems that have occurred or are likely to occur related to cybersecurity will decrease in the entire maritime industry when these suggestions are taken into consideration.The results of the recommendations show that; a large part of the maritime industry employees emphasise the importance of training in parallel with the analysis results of the survey. It is possible to say that cybersecurity training is the leading and most important force in preventing cyber attacks. By implementing these suggestions, the maritime industry can enhance its overall cybersecurity posture and better protect its assets and operations.

5. CONCLUSION

Global maritime transport is the most important cornerstone for the smooth flow of economic activities in the world and the uninterrupted continuation of international trade. The digitalisation of high-tech systems, which are becoming increasingly important in the maritime sector, brings the problem of cyber to the sector. The concept of cybersecurity stands out as an important issue for the maritime industry not only in terms of ensuring system security, preventing accidents, loss of life and environmental damage, but also in terms of national security and economy.

In this study, within the framework of cybersecurity approaches, cybersecurity issues and current threat dynamics in the maritime industry are considered and analysed. The cybersecurity awareness levels of Turkish maritime industry employees were evaluated in terms of different variables. In this research, which aims to measure the cyber awareness levels of maritime industry employees and to increase awareness according to the results obtained, the socio-demographic characteristics and cybersecurity awareness levels of the employees were tried to be determined with the help of a questionnaire. The issues related to cybersecurity and its importance, previous cyber-attacks, cybersecurity applications and digitalisation have been comprehensively explained in the previous sections and the survey results obtained have been statistically tested.

Results related to the survey;

-When the frequency distribution of the survey participants is analysed; the number of employees between the ages of 31-40 constitutes the largest segment. Male participating in the survey are 3 times denser than female. The working time of the survey participants in the maritime industry is distributed in a similar range. Half of the participants have a bachelor's degree from the relevant departments of universities. Most of the participants are working as Oceangoing Watchkeeping Officers The ship types they are working on are tankers and cargo ships with equal density.

-When the frequency table of the survey questions is analysed, it is seen that the participants intensively gave similar answers to some questions. Participants who stated that they did not receive training on cybersecurity within the company or individually constitute the largest segment.

-The findings obtained from the explanatory factor analysis of the cybersecurity awareness scale show that the model provides construct validity. It is seen that the scale levels are highly reliable.

-The results of the frequency distribution of the cybersecurity awareness scale of the tested questionnaire show that; when the cybersecurity awareness scale of the maritime industry employees is evaluated, it is concluded that they score below the average in the awareness, user behavior and experience sub-factors of the scale to determine the level of ensuring cybersecurity, and slightly above the average in the education, rules and policies sub-factors. The conclusion drawn from the whole scale and all sub-factors is that the cybersecurity awareness of maritime industry employees is inadequate.

-Although it was concluded that the level of maritime industry employees' provision of cybersecurity did not show a significant difference according to their age, the cybersecurity provision status according to age groups was found to be higher than the other age groups, especially in the 31-40 age range, in the whole scale and most of the sub-factors. It is seen that the level of ensuring personal cyber gradually decreases in the age groups after and before the 31-40 age group maritime industry employees.

- It has been determined that the level of cybersecurity of maritime industry employees does not show a significant difference in total according to their years of employment, but since the calculated value is very close to the limit value, it can be interpreted that there is a low level of awareness in general. However, there is a significant difference with the experience factor among the sub-factor values; those with 0-2 years of experience and those with 12-14 years of experience constitute this difference.

- It has been determined that the level of cyber of maritime industry employees does not show a significant difference according to their level of education, the department they work in and the type of ship they last worked on.

-When the relationship between the scale levels is analysed; when education, one of the sub-factors, is compared with the other sub-factors, it is seen that the awareness of maritime industry employees increases as the level of education increases. In addition, as the education level of maritime industry employees increases, it is determined that user behaviours, compliance process with rules and policies, and experience are positively affected. The increase in other sub-factors also positively affect each other.

-The result obtained from the analysis of the suggestions for increasing the level of cybersecurity awareness directed to the maritime industry employees is that the majority of the employees made suggestions to increase the level of education. It has been concluded that maritime industry employees are of the opinion that cybersecurity problems experienced in the society will decrease when these suggestions are acted upon.

Cybersecurity can only be ensured in a system and network when cybersecurity is handled in all its dimensions. Considering that the weakest link is the last users, it would be appropriate to focus on cyber awareness training considering the results of this study.

In the maritime sector, last users are the most important building blocks in ensuring the security of the systems and protecting the information they process. If users are not educated on cyber issues or do not take precautions, they are open to cyber threats. It may cause virus infections on the devices it uses, and may unintentionally serve cyber attackers with the threat it creates. Even if technically necessary security standards are fulfilled, risks continue if there are unconscious users. At this point, as seen from the results of the survey, it is necessary to emphasise the importance of training to close the cybersecurity awareness gap of maritime industry employees.

Training the labor force of the future starts in schools; a strong structure can be established by providing education from the basics as a priority. To promote the sustainable management of the maritime sector and to develop the skills and competences that will increase the awareness of cybersecurity, which is one of the leading maritime problems emerging with the development of technological integration, priority awareness on cybersecurity can be created by adding courses to the maritime education departments of universities. With the trainings that can support this awareness, it can be made possible for a maritime industry employee who is faced with a cyber-attack to consciously respond to this attack or prevent the cyber threat. If the trainings are visually supported with course resources and videos, their retention will increase. In addition to all these, academic and administrative staff should also receive this training. In order to test the awareness of students after these courses and training programmes added to the curriculum and to see the feedback, surveys can be applied, and harmless attacks can be carried out at an indefinite time. The courses and training programmes to be implemented should help to understand the risks and take precautions.

When designed as a training programme to be applied to maritime industry employees, the primary objective should be to reach all human resources working in the maritime industry by using a hierarchical structure. Considering the hierarchical structure, all users in the maritime industry chain should be raised awareness through trainings and awareness programmes. It will be more efficient to customise the trainings in accordance with the task of the maritime industry employees. This system will help employees to gain awareness in a way that they can apply what they know and understand the seriousness of the situation. With regular meetings and brochures that can be prepared, trainings can be detailed according to the employees and content in the missing parts, and the existing information and missing parts can be dynamically memorised.

The fact that cyber awareness is a dynamic process shows that the appropriate training model should be selected for this dynamic process. While building the basis of a secure maritime industry, new training programmes to be organised and implemented for the formation of cyber awareness are of vital importance for a cyber-secure maritime industry.

5.1 Recommendations for Future Research

In light of our findings, further research could be beneficial to expand and rigorously test the theory developed herein. Future studies could extend this research by focusing on:

1. Investigating cybersecurity and cybersecurity awareness among system users within the scope of MSW as the future system.
2. Exploring the role and application of cybersecurity in projects involving increased use of automation systems on ships and MASS (Maritime Autonomous Surface Ships) projects.
3. Modeling and developing educational programs within the scope of cybersecurity at sea.
4. Examining the technical aspects of cybersecurity for IT department employees in the maritime sector.

6. REFERENCES

Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean and Coastal Management*.

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network*, 123-138.

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the ma aritime sector. *ELSEVIER*, 547-554.

Alop, A. (2019). The Main Challenges and Barriers to the Successful "Smart Shipping" . *The International Journal on Marine Navigation and Safety of Sea Transportation*, 521-528.

Amro, A., & Gkioulos, V. (2023). Evaluation of a Cyber Risk Assessment Approach for Cyber-Physical Systems: Maritime and Energy Use Cases. *MDPI*.

Androjna, A., Brcko, T., Pavic, I., & Greidan, H. (2020). Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering*.

Arora, A., & Antoniadou, E. (2020). *Maritime Cyber Risk Management Guidelines.* The Standard Club.

Bacasdoon, J., & Bolmsten, J. (2022). A Multiple Case Study of METI Cybersecurity Education and Training: A Basis for the Development of a Guiding Framework for Educational Approaches. *The International Journal on Marine Navigation and Safety of Sea Transportation*, 319-334.

Basulo-Riberio, J., Primentel, C., & Teixeira, L. (2024). 5th International Conference on Industry 4.0 and Smart Manufacturing. *What is known about smart ports around the world? A benchmarking study* (pp. 1748-1758). Procedia Computer Science.

BIMCO, CSA, INTERCARGO, INTERTANKO, ICS, IUMI, . . . WSC. (2021). *The Guidelines on Cyber Security Onboard Ships Version 4.* BIMCO; CSA; INTERCARGO; INTERTANKO; ICS; IUMI; OCIMF; Sybass; WSC.

Caprolu, M., Pietro, R. D., Raponi, S., Sciancalepore, S., & Tedeschi, P. (2020). Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. *IEEE Communications Magazine*, 90-96.

Chen, X., Ma, D., & Liu, W. R. (2024). Application of Artificial Intelligence in Maritime Transportation. *Journal of Marine Science and Engineering*.

Cho, S., Orye, E., Visky, G., & Prates, V. (2022). *Cybersecurity Considerations in Autonomous Ships.* Tallinn: CCDCOE: NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE.

Crowdstrike. (2022, Feb 13). *10 Most Common Types of Cyber Attacks*. Retrieved from Crowdstrike Web Site: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

DanubePortsNetwork. (2019). Smart Port Model. *Smart Port Model*. Vienna: Interreg Danube Transnational Programme.

DCSA. (2021, Nov 16). *DCSA publishes complete framework of Just-in-Time Standards for main port call activities* . Retrieved from DCSA Web Site: https://dcsa.org/newsroom/resources/dcsa-publishes-complete-framework-of-just-in-time-standards-for-main-port-call-activities/

Diaz, R., Ungo, R., Smith, K., Haghnegahdar, L., Singh, B., & Phuong, T. (2024). Applications of AI /ML in Maritime Cyber Supply Chains. *Procedia Computer Science*, 3247-3257.

Diaza, R., Smitha, K., Bertagnab, S., & Buccib, V. (2023). Digital Transformation, Applications, and Vulnerabilities in Maritime and Digital Transformation, Applications, and Vulnerabiliti. *Procedia Computer Science*, 1396-1405.

DNV. (2023). *Maritime Cyber Priority 2023* . DNV.

ENISA. (2022, Oct 21). *Maritime Sector Sails through rough 'Cybersecurity' Seas*. Retrieved from ENISA Web Site: https://www.enisa.europa.eu/news/maritime-sector-sails-through-rough-cybersecurity-seas

ENISA. (2023). *Cybersecurity of AI and Standardisation* . European Union Agency for Cybersecurity.

Erstad, E., Hopcraft, R., Harish, A. V., & Tam, K. (2023). A human-centred design approach for the development and conducting of maritime cyber resilience training. *WMU Journal of Maritime Affairs*.

Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022, Jan 6). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information*.

Hinrichs, R. J., Popovsky, V. M., & Endicott-Popovsky, B. (2023). Bringing the Industry Partner to the Cybersecurity Education Table as an Active Participant. *2023 Journal of The Colloquium for Information Systems Security Education*.

Hopcraft, R., Harish, A., Tam, K., & Jones, K. (2023). Raising the Standard of Maritime Voyage Data Recorder Security. *Journal of Marine Science and Engineering*.

Hopcraft, R., Tam, K., Misas, J. D., Moara-Nkwe, K., & Jones, K. (2022, Aug 18). Developing a maritime cyber safety culture: Improving safety of operations. *Maritime Technology and Research*.

IBM. (2023). *What is SIEM?* Retrieved from IBM Web Site: https://www.ibm.com/topics/siem

Ilcev, D. S. (2022). Software Solutions for GMDSS Network and Equipment . *The International Journal on Marine Navigation and Safety of Sea Transportation*, 463-472.

IMO. (2019). *Brief History of IMO*. Retrieved from IMO Web Site: https://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx

IMO. (2022, June 7). *IMO Guidelines on Maritime Cyber Risk Management.* Retrieved from IMO Web Site: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

IMO. (2023). *Maritime Cyber Risk*. Retrieved from IMO Web Site: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

Kalaycı, Ş. (2008). *Spss Uygulamalı Çok Değişkenli İstatistik Teknikleri.* Ankara: Asil Yayın Dağıtım.

Karim, S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*.

Kayişoğlu, G., & Bolat, P. (2022). Denizcilikte Siber Güvenlik Ridk Yönetimi. In A. MERT, B. R. KURTDARCAN, B. Ş. ŞEKER, B. E. BAL, F. BOLAT, G. KAYİŞOĞLU, . . . T. YALÇIN, *Deniz Hukuku ve Güvenliği* (pp. 209-237). Ankara.

Kim, M.-K., Kim, J.-H., & Yang, H. (2023). Optimal Route Generation and Route-Following Control for Autonomous Vessel. *Journal of Marine Science and Engineering*.

Kuhn, K., Bicakci, S., & Shaikh, S. ,. (2021). COVID-19 digitization in maritime: understanding cyber risks. *WMU Journal of Maritime Affairs*, 193-214.

Li, X., Oh, P., Zhou, Y., & Yuen, K. F. (2023). Operational risk identification of maritime surface autonomous ship: A network analysis approach. *Transport Policy*, 1-14.

Mednikarov, B., Tsonev, Y., & Lazarov, A. (2020). Analysis of Cybersecurity Issues in the Maritime Industry. *Information&Security*, 27-43.

Melnyk, O., Onyshchenko, S., Pavlova, N., Kravchenko, O., & Borovyk, S. (2022). Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. *IJCSNS International Journal of Computer Science and Network Security*, 135-140.

MissionSecure. (2021). *Complying with the IMO 2021 Cybersecurity Regulations.* MissionSecure.

Mohammed, A. S., Reinecke, P., Burnap, P., Rana, O., & Anthi, E. (2022). Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber Physical Systems (ICPS) Perspective. *A PREPRINT*.

NIST. (2023). *Intrusion detection and prevention system (IDPS)*. Retrieved from NIST Web Site: https://csrc.nist.gov/glossary/term/intrusion_detection_and_prevention_system

OAS. (2021). *MARITIME CYBERSECURITY IN THE WESTERN HEMISPHERE An Introduction and Guidelines.* . OAS.

Onishchenko, O., Shumilova, K., Volyanskyy, S., Volyanskaya, Y., & Volianskyi, Y. (2022). Ensuring Cyber Resilience of Ship Information Systems. *The International Journal on Marine Navigation and Safety of Sea Transportation*, 43-50.

Ozdemir, P., Sevim, A., & Albayrak, T. (2023). Closing the gap between present and future through education: MINE-EMI project. *Case Studies on Transport Policy*.

Scanlan, J., Hopcraft, R., Cowburn, R., Trovåg, J. M., & Lützhöft, M. (2021). Maritime Education for a Digital Industry. In T. R. ACADEMY, *NECESSE ErgoShip 2021 – Maritime artikler* (pp. 23-33). MONOGRAPHIC SERIES.

Shea, S. (2023). *SOAR (security orchestration, automation and response)*. Retrieved from TeachTarget Security Web Site: https://www.techtarget.com/searchsecurity/definition/SOAR

Silverajan, B., Ocak, M., & Nagel, B. (2018). Cybersecurity Attacks and Defences for Unmanned Smart Ships. *IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics* (pp. 15-20). IEEE.

Solmaz, M. S. (2023). The 28th INTERNATIONAL MARITIME LECTURERS‘ ASSOCIATION CONFERENCE (IMLA 28). *Determination of Cyber Risks and Cber Security Measures in Smart Ports* (pp. 113-121). Varna: Nikola Vaptsarov Naval Academy.

Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2024). Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. *Applied Ocean Research*.

Svilicic, B., Kamahara, J., Celic, J., & Bolmsten, J. (2019). Assessing ship cyber risks: a framework and case study of ECDIS security. *WMU Journal of Maritime Affairs*, 509–520.

Svilicic, B., Kristić, M., Žuškin, S., & Brčić, D. (2020). Paperless ship navigation: cyber security weaknesses. *Journal of Transportation Security*, 203-214.

Svilicic, B., Rudan, G., Jugovic, A., & Zec, D. (2019). A Study on Cyber Security Threats in a Shipboard Integrated Navigational System . *Journal of Marine Science and Engineering*.

Tabachnick, B., & Fidell, L. (2013). *Using Multivariate Statistics.* New York: Pearson.

Tabish, N., & Chaur-Luh, T. (2024). Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives. *IEEE VEHICULAR TECHNOLOGY SOCIETY SECTION*, 17114-17136.

Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs* , 129-163.

Tam, Kimberly; MoaraNkwe, Kemedi; Jones, Kevin, D. (2021). The use of cyber ranges in the maritime context: Assessing maritime- cyber risks, raising awareness, and providing training. *Maritime Technology and Research*, 16-30.

Thomas, M. L. (2022). Maritime Hacking Using Land-Based Skills. *2022 14th International Conference on Cyber Conflict* (pp. 249-263). Tallinn: NATO CCDCOE Publications.

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T.-E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. *Maritime Economics & Logistics*, 208–227.

Zarzuelo, I. P. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transport Policy*, 1-4.

APPENDIX A

EVALUATION OF THE CYBERSECURITY AWARENESS LEVELS OF TURKISH SEAFARERS AND TURKISH MARITIME INDUSTRY EMPLOYEES

1.Age?

☐ 20 and under ☐ 21-30 ☐ 31-40 ☐ 41-50 ☐ 50 and up

2.Gender?

☐ Female ☐ Male

3. How long have you been working in the maritime industry?

☐ 0-2 years ☐ 3-5 years ☐ 6-8 years ☐ 9-11 years ☐ 12-14 years
☐ 15 and more years

4. What is your educational background?

☐ Maritime Course (TÜDEV etc.) ☐ Associate degree ☐ Bachelor
☐ Postgraduate ☐ PhD graduate ☐ Other

5. What is your role in the department you work in?

☐ Oceangoing Master ☐ Oceangoing Watchkeeping Off. ☐ Chief Engineer
☐ Engine Officer ☐ Crew ☐ Company Employee ☐ Port Management Employee ☐ Other

6. What was the last ship type you worked on? (If you are a company employee, the type of fleet the company has)

☐ Tanker & Chemical ☐ Dry Cargo ☐ Container ☐ Ro-Ro ☐LPG/LNG
☐Other

Please complete the following statements by choosing the option that suits you best.

1: Do Not Agree / Not Applicable at All

2: Rarely Agree / Rarely Applied

3: Partially Agree / Partially Applicable

4: Mostly Agree / Mostly Applicable

5: Totally Agree / Fully Applicable

	1	2	3	4	5
7- I have received training/course/certificate on information technology systems or cybersecurity.	☐	☐	☐	☐	☐
8- In the vessel / company / port management company I work for; regular cybersecurity training is provided.	☐	☐	☐	☐	☐
9- I am aware of cyber risks during daily use.	☐	☐	☐	☐	☐
10- I know what a cyber attack is and how to protect against these attacks.	☐	☐	☐	☐	☐
11- I have knowledge of cyber-attacks on vessels, maritime companies, ports and port management companies with major impacts and their consequences.	☐	☐	☐	☐	☐
12- I use the internet network on the vessel I work on or the internet of the company or port management company for social media tools.	☐	☐	☐	☐	☐
13- I open my corporate or private e-mails without checking the sender; I click on the links.	☐	☐	☐	☐	☐
14- In the vessel / company / port management company I work for; I do not open a device (flash memory, hard disk, etc.) that I plug into my corporate computers without scanning for viruses.	☐	☐	☐	☐	☐
15- In the vessel/ company / port management company I work for; while creating written rules and policies regarding information security, dangers and vulnerabilities that may occur in vital areas have been taken into consideration.	☐	☐	☐	☐	☐
16- The vessel / company / port management company I work for has written rules and policies regarding information security.	☐	☐	☐	☐	☐

17- I know who is responsible for cybersecurity in the vessel / company / port management company I work for.	☐	☐	☐	☐	☐
18- In the vessel / company / port management company where I work; protective measures have been taken against all kinds of dangers related to information technologies.	☐	☐	☐	☐	☐
19- In the ship / company / port management company I work for; security measures have been taken regarding the use of portable computers or external storage devices.	☐	☐	☐	☐	☐
20- In the ship / company / port management company I work for; I know what to do when my computer is infected with a virus.	☐	☐	☐	☐	☐
21- During the inspection, an item related to cybersecurity was written for any system belonging to the vessel / company / port management company I work for.	☐	☐	☐	☐	☐
22- We have internal security systems, drills and audits in place to ensure that our data is not damaged in a possible cyber attack against the vessel / company / port management company I work for.	☐	☐	☐	☐	☐
23- In the last 12 months, the vessel / company / port management company I work for has been subjected to a cyber attack.	☐	☐	☐	☐	☐
24- I believe that cybersecurity trainings are important for seafarers and should be mandatory as per STCW.	☐	☐	☐	☐	☐
25- I believe that more training on cybersecurity should be provided in the vessel / company / port management company where I work.	☐	☐	☐	☐	☐
26- In the vessel / company / port management company I work for; there is a procedure for regular updating of software for various systems (e.g. Transfer systems, ECDIS, information technology and automation systems, etc.).	☐	☐	☐	☐	☐

27- In the vessel / company / port management company where I work; operating systems, anti-virus software and other software on computers are regularly updated and audited in their original form.	☐	☐	☐	☐	☐
28- In the vessel / company / port management company I work for; we have original and constantly updated network security protection programs.	☐	☐	☐	☐	☐
29- In the vessel / company / port management company I work for; we have a plan that addresses the fight against cyber attacks against possible cyber attacks.	☐	☐	☐	☐	☐
30- In the vessel / company / port management company I work for; if you receive an e-mail that your anti-virus is out of date and you are asked to open the attached file to update it, I open it without checking the sender.	☐	☐	☐	☐	☐
31- In the vessel / company / port management company I work for; our data is regularly backed up to prevent damage in a possible cyber attack.	☐	☐	☐	☐	☐
32- In the vessel / company / port management company where I work; if it is necessary to change the passwords of the connection equipment or wireless networks outside the common use, I write the new passwords in visible places so that they are accessible.	☐	☐	☐	☐	☐
33- In the vessel / company / port management company I work for; each employee has access privileges and limits on systems.	☐	☐	☐	☐	☐
34- In the vessel / company / port management company I work for; up-to-date information and training bulletins about cyber-attacks are sent regularly to increase the awareness of each employee and to know what to do.	☐	☐	☐	☐	☐
35- I think that the trainings I have received are sufficient in fighting against cyber-attacks.	☐	☐	☐	☐	☐

Additional Question: What are your suggestions for increasing the level of cybersecurity awareness?

CURRICULUM VITAE

HANDE YILMAZ	
EDUCATION	
Postgraduate	Piri Reis University – İstanbul – Maritime Business and Economics (%100 Scholarship)– 09/2021 – Continue (Thesis Term)
2nd University	İstanbul University – İstanbul – International Trade and Logistics – 09/2020 – Continue
University	Istanbul University – Istanbul – Econometrics – 09/2007 – 06/2012
High School	Bahçelievler Anatolian High School – İstanbul – 09/2003 – 06/2007
WORK EXPERIENCE	
08/2018 – Continue	ORTAKLAR DEMİR METAL ÇELİK MAK. SAN. VE TİC. LTD. ŞTİ. Rank: Senior Operation and Accounting Specialist
09/2016 –07/2018	BANYAN KİMYA TEKSTİL SAN. TİC. LTD. ŞTİ. Rank: Senior Operation and Accounting Specialist
08/2014 – 09/2016	BANYAN KİMYA TEKSTİL SAN. TİC. LTD. ŞTİ. Rank: Operation and Accounting Specialist
LANGUAGE SKILLS	
English	Reading: Advanced, Writing: Advanced, Speaking: Advanced
German	Reading: Pre-Intermediate, Writing: Pre-Intermediate, Speaking: Pre-Intermediate
Spanish	Reading: Beginner, Writing: Beginner, Speaking: Beginner
PUBLICATIONS	
08/2023	IMLA 2023 Conference – Research On Cybersecurity Issues And Current Threat Dynamics In The Maritime Industry
03/2023	Deniz İşletmeciliği Ve Yönetiminde Güncel Yaklaşimlar – Denizde Siber Güvenlik Uygulamalarinda Güncel Yaklaşimlar