international journal of critical infrastructure protection 37 (2022) 100526

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

Digital transformation of the maritime industry: A cybersecurity systemic approach

Evripidis P. Kechagias [a,*], Georgios Chatzistelios [a], Georgios A. Papadopoulos [a], Panagiotis Apostolou [b]

[a] National Technical University of Athens, School of Mechanical Engineering, Sector of Industrial Engineering and Operational Research, Zografos, 15780, Greece
[b] Hellenic Open University, School of Social Sciences, Patras, 26335, Greece

ARTICLE INFO

Keywords:
Cybersecurity
Maritime
Cyberattack
Information Technologies
Digital transformation
System

ABSTRACT

Information system solutions are increasingly being applied to the maritime industry, and eventually, all aspects of maritime operations will be aided by the digital transformation of the industry. The maritime industry is a sector driven by compliance and historically deals with security and safety matters at an international level. It has been recognized that safety and security in maritime heavily depend on cyber systems and cybersecurity implementation requirements have started to get integrated into maritime's regulatory context. This paper focuses on cybersecurity in the maritime industry, presenting an inside view of maritime cybersecurity aspects and offering a detailed case study analysis based on a real-world company's approach. The main objective of the paper is, therefore, to connect research with practice, presenting a maritime company's cybersecurity systemic approach with references to procedures and policies. The findings of the case study and the cyber security vessel audit survey that is performed show that the company was able to assess its current status, collect evidence and objectively determine security gaps, and achieve cyber risks mitigation. The gained knowledge will be used in the future to continuously improve the company's systems and move to a more predictive and proactive maturity level.

1. Introduction

World trade and economy depend on the maritime industry's reliability and sustainability. Maritime transport system (MTS) enables import and export of goods, supply in energy, trade, and transport of passengers and vehicles. The following statistics reflect the vital importance of shipping to societies and the global economy. According to the International Chamber of Shipping (ICS), a global trade association for shipowners and operators, the international shipping industry is responsible for 90% of world trade, while each year, 11 billion tons of goods are transported by over 50000 ships, crewed by over 1.5 million seafarers. The total value of the world shipping trade for 2019 is estimated above 14 trillion US Dollars [1].

The United Nations Conference on Trade and Development (UNCTAD) reports at the Annual Review of Maritime Transport for 2020 that the total world fleet consists of 98140 commercial ships of 100 gross tons and above, equivalent to a capacity of 2.06 billion deadweight tonnage (dwt). Especially during the pandemic, the shipping industry managed to support the global economy providing stability by ensuring the undisrupted delivery of critical supplies. Worth billions of dollars, tens of thousands of merchant's vessels are sailing the oceans at all times. However, at the start of 2020, the average age of the global fleet was 21.29 years in terms of the number of ships, while 41,85% of all ships currently at sea are older than 20 years old. Since there was no

Abbreviations: BIMCO, Baltic International Maritime Council; BYOD, Bring Your Own Device Policy; COSCO, China Ocean Shipping Company; CMA CGM, Compagnie Générale Transatlantique and Messageries Maritimes; CSO, Company Security Officer; CBT, Computer-Based Training; CyRiM, Cyber Risk Management; CSP, Cyber Security Plan; DCS, Data Collection System; ECDIS, Electronic Chart Display and Information System; ENC, Electronic Nautical Chart; ENISA, European Union Agency for Cybersecurity; ACLs, Firewalls and Access Control Lists; HSQE, Health, Safety, Quality and Environment; IMS, Integrated Management System; ICS, International Chamber of Shipping; IMSM, International Management Systems Marketing; IMO, International Maritime Organization; ISPS, International Ship and Port Facility Security; IDS, Intrusion Detection System; IPS, Intrusion Prevention System; MTS, Maritime Transport System; NIST, National Institute of Standards and Technology; UNCTAD, United Nations Conference on Trade and Development; WEF, World Economic Forum.

* Corresponding author.
E-mail address: eurikechagias@mail.ntua.gr (E.P. Kechagias).

https://doi.org/10.1016/j.ijcip.2022.100526
Received 16 September 2021; Received in revised form 2 March 2022; Accepted 26 March 2022
Available online 27 March 2022

cybersecurity by design providence at the time of their build, this statistic shows that most of these ships are now probably sailing with outdated and vulnerable operational technology (OT) infrastructure [2].

According to the same report, the volume of international marine trade was predicted to fall by 4.1% in 2020, mainly due to the coronavirus. Apart from the pandemic's impact on the industry, other factors also present a substantial risk for the industry. Climate-related challenges call for the industry to perform business in a more environmentally sustainable manner by reducing sulfur levels in marine fuel, such as the industry's commitment to decarbonize by 2050. Political instability and piracy also represent significant threats to the industry. Risks related to the advancement of technology in the sector also impose a threat for the industry. Cyber-threats have risen since modern ships today heavily rely on shore-based systems and onboard computers and software for carrying out daily tasks, operations, and satisfying the mariners' communications needs [2]. Allianz reports on Safety and Shipping Review 2020 that since the coronavirus pandemic began, maritime sector companies have faced an increase of 400% in attempted cyber-attacks [3].

Exploring the attributes of the maritime industry that make it particularly vulnerable to cyber incidents and attractive to cybercriminals, one would name the following [4]:

- The low visibility of the industry to the public makes it attractive to cybercriminals since cybercrimes targeting the maritime industry usually do not get mass media attention.
- Large money transfers are occurring for daily business.
- An extensive number of interconnected businesses and authorities in the industry share business-critical, data-sensitive, and commercially sensitive information.
- There is the involvement of multiple stakeholders in the operation of a ship which often results in a lack of accountability for securing it.
- Ships may be accessed and monitored by various shore parties. Various vendors may provide remote support to ship equipment (OT proprietary systems) or ship's software.
- Many legacy information technology (IT) and OT systems are still used. These systems run obsolete software that is no longer supported and cannot be secured. Automation systems may be comprised of multiple sub-systems from various vendors, integrated with no cybersecurity in mind.
- Use IT and OT systems that cannot be patched or updated due to type approval issues.
- The low awareness of the industry operators and the immature cyber risk management culture. Cybersecurity is a concept relatively new to shipping, not yet understood, and most maritime operators and managers have no training in related cyber risks.

The European Union Agency for Cybersecurity (ENISA) names low awareness as the first vulnerable point of the industry regarding Cybersecurity [5]. Since cyber-attacks affect the attacked organization's reputation, many incidents do not get to the media and do not get publicly known carried out an online questionnaire that experienced maritime professionals answered [6]. The lack of knowledge regarding cyber risks was reported to exceed 75% of the authors' maritime experts participating in the survey. The analysis of the results showed the lack of general knowledge in maritime Cybersecurity and the necessity to increase training levels in the maritime sector and the port interface connection with the supply chain. The authors also shed light on the alarming finding that the survey participants believe that solely the implementation of technological systems can address cyber threats without considering any responsibility of the operator or the administration [6].

Regarding the level of today's cybersecurity readiness, a shift in mindset is essential to direct more attention and resources toward Cybersecurity. Moreover, manufacturers need to improve the Cybersecurity of their products, as shipping systems currently remain vulnerable to cybercriminals [7]. On one side, we have globally complex supply chains, interconnected economies, and an emerging and rapidly changing cyber threat environment. On the other hand, an aging shipping infrastructure that is designed with no cybersecurity in mind. Undoubtedly in the last 20 years, technology has changed tremendously. Moreover, the fact that the vast majority of ships were built before Cybersecurity is a significant concern. During the last decade, many new technologies were adapted and implemented to existing infrastructure or are currently in the process of implementation, but still, ship managers and marine vendors are not yet fully aware of the cyber risks involved. This inevitably results in infrastructures of hardware and software vulnerable to modern cyber threats.

Historically cybersecurity was not a big issue for ships as the dependency on the digital systems was limited (compared to today), and ships were also considered isolated from the outside world therefore inaccessible by hackers. There was a perception that the whole ship environment was in an "air gap." An air gap describes the occasion "when one or more computers are physically isolated from unsecured computer networks, such as the public Internet or an unsecured local area network, for security purposes. Air gap computers are not connected by wire or wirelessly and (generally) cannot communicate directly with each other" This perception was not true. Although the vessel's data connectivity with its outside environment while sailing an ocean was not something permanent due to the high data usage cost and low bandwidth capabilities of that time satellite communication systems, it still allowed short-term intra-daily data connections, usually for e-mail exchange reasons. Therefore, the danger of receiving malicious emails and attachments has existed for many years now [8].

Advancements in communication capabilities allowed the vessels to frequently update their onboard software programs for route optimization, voyage planning, and reliable weather forecasting, to have continuous and efficient communications with ship managers naming the real-time exchange of data with the office side, the ability to resolve issues and support a case by remote connection or video communication or to use telemedicine to distribute health services remotely. They also allowed better communication and data exchange with national and port authorities to exchange forms and declarations and support continued reporting satisfying the various stakeholders' demands (e.g., charterers). Furthermore, these systems also satisfied the need to comply with the latest regulations implied for reporting fuel consumption and emissions, such as the Data Collection System (DCS) implied from the International Maritime Organization (IMO) or the Monitoring, Reporting, and Verification (MRV) implied from European Union. Another significant advancement is the transition from paper nautical charts to paperless navigation systems using electronic nautical charts (ENCs).

Modern vessels nowadays rely heavily on the digitalization of systems and procedures. OT systems provide and transmit to shore parties various real-time information and data of the vessel's operation and status, such as bunker fuel consumption. A vessel is now a data center and IoT applications allow the connection of onboard sensors to shore, providing real-time transmissions. This enables remote diagnostics and configuration, enhances proactive maintenance, monitors vessel condition and performance, and promotes voyage optimization. The extended range of cyber systems that vessels are equipped with, means that ships are now complex computer-controlled platforms. The use of digital communications to connect marine systems to land applications means that ships are also part of the Internet-dominated world.

In the Futurenautics Crew Connectivity Survey in 2015, it was estimated that the average availability of Internet access across all fleet sectors stood at 43% [9]. The 2018 repeated survey estimated this characteristic at 75% —an increase of 32% since the previous survey [10]. In conclusion, these numbers reflect the high Internet penetration levels in all fleet sectors. These levels continue to rise, and Internet access is nowadays the most common form of crew connectivity available while at sea.

This paper gives an insight into the current status of cybersecurity

concerning Maritime, presents how a real-world organization manages it and adds to the development of overall awareness and knowledge on protecting shipping from mounting cyberthreats. After a brief introduction to the concepts of cybersecurity and cyberspace, this paper analyzes the importance, the characteristics, and the risk assessment of cybersecurity in the maritime industry. Concluding the aforementioned analysis, the main part of the paper unfolds. The main objective is to present a Maritime company cybersecurity systemic approach with references to procedures and policies. The first approach is the plan-do-check-act (PDCA) approach for continuous improvement. The second is to effectively manage the three pillars of security: procedures, the human factor, and technology. Moreover, to enhance the knowledge and understanding of the subject, a Cyber Security Vessel Audit Survey is presented along with its scope and findings.

2. Importance of cybersecurity and cyber risk management in the maritime industry

2.1. Importance of cybersecurity

IMO refers to Maritime cyber risk as a "measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised". Maritime cyber risk includes not only the cyberattack incidents but any incident that affect directly or indirectly the security properties of IT or OT systems [11].

Cyber risks are posed by cyber incidents that may include but are not limited to the following events [4]:

- An unintended system failure occurring during software maintenance and patching.
- A failure of a system due to software crashes or "bugs".
- Any crew interaction that could lead to loss of sensitive data or introduction of malware to shipboard systems
- Ransomware or denial of service incident.
- Loss or the manipulation of external sensor data, critical for the operation of a ship.
- Loss of availability of electronic navigational equipment or loss of integrity of navigation-related data.
- Loss of essential connectivity with the shore
- Loss of availability of OT systems, including propulsion, auxiliary systems, and other critical systems, as well as loss of integrity of data management and control

Cyber risk is an emerging and complex risk of global nature since connectivity can increase the magnitude of isolated cyber events into having global effects. Cybersecurity must become a primary concern for the maritime industry because cyber threats set the core of maritime safety at risk. When we talk about Cybersecurity in maritime, it is not only about protecting the information part of it that we do not see, but we need to focus on cyber because this will have some consequent physical effect and it needs to be well protected for that as well. A possible cyberattack on a ship might affect the ship's safety and its personnel, the company in terms of financial cost and reputation, the cargo, and possibly the environment in terms of pollution.

In some extreme cases, possible cyber-attacks on the cruise ship's navigation system, for example, could lead to property damage and even loss of life [12]. Current threat implications of marine-based cyber-attacks include business disruption, financial loss, damage to reputation, damage to goods and environment, incident response cost, fines, and/or legal issues [13]. Since such attacks impose such an essential risk for shipping companies, the importance of Cybersecurity has increased dramatically in recent years. Additionally, if a port facility's electronic or computer-based systems were to fail, malfunction, or be misused, this would result in economic, operational, physical, or reputational loss or damage or disruption of operations. Recent cyberattacks have shown that ships, maritime companies, ports, and maritime terminals are not immune from emerging cyber threats. In order to maintain safe and efficient operations, cyber risk should be managed like other significant threats, such as physical security, natural disasters, and industrial accidents. The magnitude of the threat depends on the actor's intention, opportunity, and capability. The threat factor, alongside the identified vulnerabilities of a target, constitutes the likelihood of a cyberattack. Finally, the overall risk level is the product of the likelihood of an attack and its impact.

Since the maritime industry, ships, and onshore, becomes more interconnected with the rest of the supply chain and more dependent on digitalization and automation, the cyber threat increases. Nowadays, vessels and their systems are part of online cyberspace. Cybercriminals are becoming more capable and sophisticated, and the Maritime industry should acknowledge that with integrated IT and OT onboard the vessels, cyberattacks on ships will become the norm, rather than an exception. Industry regulators and associations are ringing the danger bells for more to come and provide best practice guidance to address the cyber risks and enforce cybersecurity measures. As presented above, with the expansion of cyberspace, all components of risk have risen.

According to the Global Risks Report 2021 of the World Economic Forum (WEF) [14], 39% of the 650 respondents forecast that the risk of "cybersecurity failure" will become a critical threat to the world within the short term of 0–2 years. Furthermore, in the Allianz Annual Risk Barometer report [15], 40% of over 2700 risk management experts from 92 countries named cyber risk the third most considered business risk. The Cyber Risk Management (CyRiM) report [16], published by Lloyd's of London, investigated the impact of a cyberattack on the global economy, checking whether it impacted the systemic vulnerabilities across ports significantly and forced them to close. The report describes a cyber-attack from a hypothetical computer virus targeting and infecting port management software and reveals its effect on the global supply chain.

Some of the key findings and potential estimates of the attack are presented below:

- Economic damage to the global economy would range between $40.8 billion in the least severe scenario (6 ports affected) to $109.8 billion in the most severe scenario (15 ports affected)
- Various sectors would be affected by these losses, including Transportation/Aviation/Aerospace, Retail, Manufacturing, Business and Professional Services, Real Estate/Property/Construction, Pharmaceuticals, Defense/Military, IT, and many others
- Productivity losses would also affect each country that has bilateral trade with the attacked ports
- The insurance industry would have to pay claims estimated from $3.6 to $8.3 billion
- Due to high levels of underinsurance for cyber-attacks on the marine industry, 92% of the economic losses would be uninsured. The expansion of the cyber insurance market is both necessary and inevitable.

The various rapid technological developments allowed commercially operated ships to operate in autonomous mode (without crew). These are already being trialed in some sea areas and predicted to start operating on small voyages. Due to their need to connect to operational, management, and administrative systems onshore, autonomous ships are constantly exposed to the threat of cyber-attacks. An infiltration and infection of critical systems subsequently imply a threat for the ship itself, the cargo, and the environment. Vinnem and Utne (2018) outline the critical hazard that a hacked autonomous ship may even be used as a weapon and cause significant structural damage to the coast or offshore infrastructure (e.g., oil and gas platforms). For that reason, the design of autonomous ships must involve strict international requirements and a series of risk-reducing actions like, for example, a requirement to keep a

small crew onboard able to obtain local control [17]. The vulnerability of the maritime industry to cyber-attacks is stressed out by the fact that since September 2020, the largest four companies of the industry were hit. More specifically, Maersk and Compagnie Générale Transatlantique and Messageries Maritimes (CMA CGM) Group suffered ransomware attacks, while China Ocean Shipping Company (COSCO) Shipping and Mediterranean Shipping Company's (MSC) digital networks were also hit. All attacks took place within a short period of time, starting in 2017 with the Maersk ransomware attack [18].

In June 2017, the largest container ship and supply vessel operator, the Danish shipping company Maersk suffered the collateral damage of the attack of NotPetya ransomware. The NotPetya attack allegedly started as a Russian government cyberattack targeting the Ukrainian economy and was designed to be technically impossible for the victim to recover its files. While 80% of the infections with NotPetya were reported in Ukraine, incidents also took place in the US, UK, France, Italy, Germany, Poland, and Russia. Their total worldwide cost is estimated at $10 billion [19]. Particularly, at Maersk, it took only seven minutes to spread across the company's network and cause a major loss of data of 49000 laptops and 4000 servers and the disruption of operations for two weeks. The cost of the cyberattack to the company is estimated at over $300 billion [20]. However, it is true that while incidents happen all the time, small or large incidents are rarely reported. Cyberattacks occur at an even greater rate than everyone non-cyber professional is led to believe, but only a few shipping cyber incidents get public attention. Still, the threat imposed by cyberattacks on the maritime industry is verified by incidents of the last decade, as seen in Table. 1.

2.2. Cyber risk assessment

IMO defines cyber risk management as "the process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders."[22]. IMO emphasize that cyber is no different from other risks and encourages to focus on cyber risk through the objectives and functional requirements of the International Safety Management (ISM) code. This means that there is no need to necessarily cover all threats, but need to look at the risk that a given threat poses to operation, security, and safety and then manage it accordingly. Imo has also stressed that no two organizations are the same, and a fit-for-purpose delivery model should be used based on a company's performance, needs, and systems. In the end, the goals of cyber risk assessment are to support safe and secure shipping. In order to achieve these goals, the cyber risk assessment approach should be resilient and evolve as a natural extension of existing holistic control system practices.

Table 1
Selected maritime cyberattacks of the past decade (modified from [21]).

Date	Victim
2010	Gulf of Mexico Offshore Drilling Rigs
Aug 2011	Iranian Shipping Line
2011-2013	Port of Antwerp
2012	Australian Customs and Border Protection Service agency
2012-2014	Danish Port Authority
Apr 2016	Ships in South Korea
Jun 2017	AP Moller Maersk
Jun 2017	Ships in Novorossiysk
Nov 2017	Clarksons
Jul 2018	Cosco US
Sep 2018	Ports of Barcelona & San Diego
Jan 2018	GPS and AIS interference in Eastern Mediterranean
Oct 2018	Austal
Jun–Aug 2019	GPS and communications interference in the Strait of Hormuz
Q1 and Q2 2020	Toll Group
Apr 2020	MSC Group
May 2020	Iranian Port Facility
Aug 2020	Carnival Corporation

Cyber risk frameworks assist organizations in addressing cybersecurity by providing the methodology, principles, and best practices that ensure the incorporation of essential elements of protection and resilience into an enterprise. National Institute of Standards and Technology (NIST) developed a cybersecurity framework to protect the critical sectors and infrastructure and consists of five core elements or activities [23], Identify, Protect, Detect, Respond, Recover, which are divided into 22 categories that can be used to create a cyber security plan. These activities are relevant also in the context of maritime services security and IMO adopted these elements and provided these five core activities as high-level recommendations that all form part of successful cyber risk assessment [22]. Baltic and International Maritime Council (BIMCO) and a coalition of industry bodies published such an approach of Maritime cyber risk assessment comprising of the following steps [4]:

- Identify threats
- Identify vulnerabilities
- Assess risk exposure
- Develop protection and detection measures
- Develop protection and detection measures
- Establish response plans
- Respond to and recover from cybersecurity incidents.

3. Case study–How a shipping company can integrate a cyber security systemic approach

3.1. Company background

The ship Management Company that is examined specializes in the management and operation of oil tankers and bulk carriers. The vessels are owned by individual companies and are registered mostly under the Greek Flag. All vessels are managed from a central Head Office which occupies approximately 100 people. Fleet consists of more than 30 vessels, and the fleet's deadweight capacity is close to 4 million deadweight tones, with an average age of about seven (7) years old. The ships' crew is multinational, mainly consisting of Greek officers and international crew members.

3.2. Cybersecurity as part of the integrated management system

As a basic principle, Cyber Security management must be based on the assumption that there will always be a way to compromise any digital environment, even when it is among the most adequately secured. Cybersecurity management includes everything an organization does to develop and continuously improve cybersecurity services and procedures to protect its IT and OT systems and detect and timely respond to security breaches from any malicious adversary. Specifically in Maritime, Cybersecurity policies need to be implemented into existing operational procedures, communicated and audited within a continuous process of improvement that fits the already established management systems of safety and security, Occupational Health & Safety, Quality, Environmental, and Energy Performance which is the Integrated Management System (IMS).

Integrated Management System describes a system of policies, procedures, and instructions for the safe operation of ships and crews and the avoidance of damage to the environment and property. Its contents indicate conformity with the requirements of the International Safety Management Code and the associated amendments. The scope and application of the Integrated Management System include all the Ship Management services and apply to all company's departments ashore and all vessels under management. The company maintains documented information within the Integrated Management System to support the company's processes. It retains documented information and records to ensure that the processes are being carried out as planned. With the adoption of IMO regulatory context of MSC.428(98), cybersecurity is now part of IMS as a continuing effort to protect the company's assets,

systems, data, and operations and secure compliance with regulators' requirements of the ISM and International Ship and Port Facility Security (ISPS) codes.

3.3. PDCA approach

A main systematic for management systems is the Plan – Do – Check – Act cycle, also known as the Deming cycle, a four-step management model for continuous improvement of products, people, and processes. The company applies the International Organization for Standardization (ISO) 90001 quality management system, follows the plan–do–check–act cycle in a process-oriented approach, and focuses on risk-based thinking for each procedure implemented throughout the organization. The objective of the PDCA cycle is to achieve planned results and maintain a continual improvement of the system.

The four stages of PDCA are [24]:

- Plan: Address risks and opportunities, make plans and procedures to accomplish target and objectives determined after sorting out any issues identified.
- Do: Perform actual work based on what was planned.
- Check: Verify and evaluate whether the initial objectives were accomplished in accordance with the plans or not. Identify any issues with the process.
- Act: Improve the process and performance based on the result of an evaluation.

A PDCA management cycle should also include Cybersecurity processes. As the cyber risk continuously changes, an ongoing control procedure is needed to confirm that checklists and policies/procedures and barriers are still effective, maintained, and kept up to date. Through the PDCA approach and its continuous improvement cycles, the company's cybersecurity maturity and resilience increase over time by moving from a reactive to a more predictive and proactive maturity level [25]. The basic steps for each PDCA stage specifically for cybersecurity are now presented below:

3.3.1. Plan

Identify cybersecurity objectives

A company should examine its current cybersecurity status/level and define what it wants to achieve. In this step, cybersecurity objectives for both the office side and vessel side are identified. The company in focus has identified its cybersecurity objectives and has included them in its IMS section of the cybersecurity policy statement, which we present later in this study.

1 Make an inventory of systems & software

If a company does not know what it has, it will not know how to protect it. According to the company's IMS procedure manuals, all IT and OT hardware and software are recorded on the relevant office and shipboard forms and reviewed according to the company's policy.

1 Execute cyber risk assessment

A company should prepare an assessment methodology to identify possible hazards in its operations/activities, estimate and evaluate risks and establish appropriate controls to minimize the risk levels. The company in focus has created a Risk Assessment (RA) Library where it is sharing the mitigating measures and experiences concerning the various identified risks. Therefore, before a job/operation, the RA library index should be reviewed. If a job/operation is included, there is no need to carry out a new RA. If not, then a new RA must be issued.

1 Set Key Performance Indicators (KPIs) for cybersecurity.

There is a need for a company to set cybersecurity metrics and keep tracking them because they help understand how effective the cybersecurity efforts have been and whether they have improved or declined over time. Some relevant examples of KPIs to monitor are the number of items for which a risk assessment has been performed, the ratio of people who have received cybersecurity training, the number of cyber incidents that have occurred, the mean time to detect or to respond to incidents, the security ratings of the company's systems and many others.

3.3.2. Do

1 Establish cybersecurity policy & procedures

A company needs to establish dedicated cybersecurity procedures & policy but also integrate cybersecurity into existing operational procedures as needed. In this manner, the company in focus has established cybersecurity manuals, such as the "Cyber Security Policy" and "Cyber security Plan" that define and describe the policies, procedures, guidelines, and work instructions that must be followed to ensure compliance with cyber security statutory requirements and accomplish identified cyber security objectives. Moreover, it has integrated cybersecurity into existing manuals such as training, risk assessment, management of change, drills-exercises, and others.

1 Define roles & responsibilities

Roles, responsibilities, accountabilities, and delegating authorities must be clearly defined for each job description/procedure/operation that an IMS manual describes. They are also presented collectively on organization charts or matrixes of responsibilities.

1 Execute cybersecurity training

Having acknowledged the importance of the human factor in cybersecurity, a company should develop company-wide cybersecurity awareness training and competence-building programs for the personnel. The training program of the company in focus is further presented in this study as part of the human factor pillar approach.

1 Report cyber events & incidents

The company has established official forms and checklists for cyber event reporting. Moreover, the company's systems are 24/7 monitored by a Security Operations Center (SOC) reporting cybersecurity incidents. An incident response team is available 24/7 to be contacted and handle reports from the SOC or those coming directly from a vessel.

3.3.3. Check

1 Evaluate the effectiveness of reaching objectives

In this step, a company investigates whether the objectives are achieved or not. It reviews its objectives and targets and evaluates its performance against the target's key performance indicators (KPIs).

1 Analyze cyber incidents& event reports

A company investigates if the cyber incident reporting is followed as it should and if they get actual learning outcomes from past incidents. A company should investigate all reported cyber incidents by utilizing relevant IMS-established forms and procedures. An investigation must result in a better understanding of the threats the company and its ships are facing and to new lessons learned. Cybersecurity risks and threats are also reviewed as necessary.

1 Execute internal audits of cybersecurity

A company should establish a process for performing objective audits to determine if cybersecurity has been effectively implemented and maintained. An audit can be executed either internally or externally. By performing audits, the administration receives reports on the status of cybersecurity measures and consequently understands what needs to be done. An insight into an accomplished cybersecurity survey/audit is presented later in this study.

3.3.4. Act

1 Execute corrective & preventive actions

Lessons learned and information derived from the "Check" phase can improve the company's approach to cybersecurity. Having acquired a better understanding, the company eventually determines the appropriate corrective actions needed to eliminate the causes of cyber incidents and avoid recurrence. After the identification of new or changed technical and procedural controls, then these are updated and utilized accordingly. The procedure requires that the proposed actions shall be taken through a risk assessment before the implementation.

1 Strive for continuous improvement

The company should investigate whether it strives towards continuous improvement or not, evaluate if it fills the gaps identified and if risks are successfully mitigated. The Company has established procedures that can be followed by company personnel (both shipboard and office personnel) when they wish to make suggestions for improvement or advise the shore administration of proposed changes. Periodic formal administration review meetings occur to determine and improve the efficiency of the Integrated Management System and ensure sustainability, adequacy, and effectiveness of Cyber Security measures.

In these meetings:

- performance data are presented and compared to appropriate benchmarks to determine priorities and goals for improvement
- results of the internal audit program are presented, results are discussed, and areas, where improvement is required are identified.
- data and the effectiveness of the improvement projects are discussed, and new improvement targets and projects are suggested
- data demonstrating the progress towards the achievement of continual improvement goals are presented, and current and completed improvement of cyber security are reviewed

3.4. Risk assessment

As part of the above PDCA process and as a major key element of any effective risk assessment system, risk assessment process of the company in focus will now be presented based on the ISO risk assessment process. Risk assessment is the process for identifying hazards and assessing the risk posed by each, and reviewing the acceptability of this risk based on comparison with risk criteria. The company has prepared and documented in IMS, a risk matrix assessment methodology on board and ashore as a tool for analyzing risk scenarios, identifying possible hazards in its operations/activities, and evaluating and establishing appropriate controls to minimize risk.

3.4.1. Identification of cyber threats and vulnerabilities

Cyber Threat (Hazards) Identification is the first step related to cyber risk Assessment. It defines the activities that their risks are studied, and it serves to identify "what could go wrong" with these activities. This step identifies actual or potential incidents, hazards, or scenarios using a systematic approach and deploys a detailed hypothetical risk scenario describing the sequence of events leading to the incident. The key objectives of "Cyber Threat (Hazard) Identification" are to build a complete list of potential threats (both intentional and unintentional) and to build knowledge and awareness based on past incidents and other work issues. For the scope of Cyber Security Risk Assessment, the list of IT & OT Hardware and Software in Office and Vessels is evaluated to determine the Cyber Risk per asset.

3.4.2. Cyber risk estimation

Cyber Risk Estimation considers both the cyber hazard effects (i.e., the severity of consequences) and the occurrence likelihood of the cyber hazard. The severity scale of the consequences is based on criteria that correspond to Confidentiality, Integrity & Availability of cybersecurity properties, as seen in Table. 2.

Frequency (or Probability) Determination is used to estimate how likely the various incidents or hazards will occur (i.e., the probability of occurrence). The Risk Matrix of the company defines five probability levels based on the frequency at which the hypothetical scenario is likely to occur. The occurrence likelihood scale is displayed in Table. 3.

Risk (R) is a function of the severity of the possible Consequences (C) for a hazard and the Frequency/ Probability of occurrence (F) of that particular hazard. Therefore, it is customary to use the product of the two to calculate the risk (R):

$$\text{Risk (R)} = \text{Frequency (F)} \times \text{Consequence (C)}$$

Under existing control measures, once the cyber hazards for a system or process have been identified and the frequency associated with these events have been estimated, relative risks associated with the events are evaluated. The Risk Matrix can be used as a mechanism for assigning risk and making risk acceptance decisions using a risk categorization approach. Each cell in the Risk Matrix corresponds to a specific combination of frequency and consequence and can be assigned a priority number [26]. Below Risk Matrix (Table. 4) provides a traceable framework to rank hazards in order of significance, screen out insignificant ones, or evaluate the need for risk reduction.

3.4.3. Cyber risk evaluation

The RA team shall evaluate the level of risk as estimated by the RA process and categorize their possible combinations to be High, Medium, or Low risk within the Risk Matrix [27]. Once the risk level has been determined, the response can be defined in Table. 5 "Risk Categories". Higher risk levels require a greater level of response. The Company uses this table as a guideline to assess the level of Risk by using risk criteria.

3.4.4. Risk reduction/ New control measures

The most important step in the RA process is identifying risk control measures as improvements to the design or operation of the Cyber asset applied to enhance the security level and mitigate the initially evaluated Cyber Risk.

Table 2
Consequence categories and severity levels.

	Consequences	Criteria
5	Catastrophic/ Hazardous effect	Critical violations of confidentiality/integrity/ availability; critical asset/data/resource unavailable; major violations of procedures / process / policies; Problem known/unknown but cannot be controlled
4	Critical/Major effect	Major violations of confidentiality/integrity/ availability; critical asset/data/resource unavailable; major violations of procedures / process / policies; Problem known and can be controlled
3	Moderate effect	Minor violations of confidentiality/integrity/ availability; non-critical asset/data/resource unavailable; major violations of procedures / process / policies
2	Minor effect	Minor violations of confidentiality/integrity/ availability; minor effect on availability of asset/ data/resource available; minor violations of procedures / process / policies
1	no effect	No effect; confidentiality/integrity/availability not endangered; asset/data/resource available; minor violations of procedures / process / policies

Table 3
Frequency description.

Frequency classes	Quantification	
5	Frequent - Possibility of repeated incidents	More often than once per voyage.
4	Probable - Possibility of isolated incidents	Once per year - The mishap scenario has occurred in the past and/or is expected to occur in the future.
3	Occasional - Possibility of occurring sometime	Once per 5 years - The mishap scenario might occur. It would not be too surprising if it did.
2	Remote - Not likely to occur	Once per 10 years - The mishap scenario is considered unlikely. It could happen, but it would be surprising if it did.
1	Very unlikely - Practically impossible	Once per 30 years or more.

Available risk reduction options include [25]:

- Avoidance – Circumvent the risk by changing the course of action.
- Reduction:
  - Prevention steps that reduce the probability of scenario incidents and failures through better design, procedures, training, or other actions.
  - Mitigation steps, which reduce the severity of incidents or the effect of failures.
  - Measures that reduce both probability and severity/consequences of incidents.
- Acceptance – Accept the risk and take the chance of the negative impact.
- Transfer – Risk outsourcing and sharing via third parties

The effort required to implement a risk-reducing measure in terms of cost, time, difficulty, and necessary resources needs to be considered against the benefits that are likely to be achieved. Following the selection of the appropriate new control measures, the risk ranking process should be repeated to evaluate if the risk is reduced to a lower Category (e.g., from High to Medium). The process should be repeated to reach the lowest possible Category.

3.4.5. Follow up

In this step, implementation of the new control measures is followed up and recorded. More specifically, in this step, the office team:

- Conducts follow-up evaluations of the controls to ensure they remain in place and have the desired effect.
- Monitors for changes or alternative ways to conduct the work, which may require further Risk Assessment.
- Takes corrective action when necessary.
- Identifies any required IMS amendments/improvements.

4. The three pillars of the cyber security approach

The company addresses its Cyber Security program through three main pillars/elements: the procedures, the human factor, and the technology. The primary tool to manage all these components is the International Management Systems Marketing (IMSM) which, for the needs of this study, was examined to identify the parts relevant to cybersecurity management. The three elements need to be coordinated, but they also need to be integrated to work well together. Effective maritime cybersecurity requires both technology and behavioral controls (procedures). The company sets the cybersecurity policy and procedures through its administrative documentation (IMS), and the people and technical controls implement them.

The three pillars of cybersecurity are presented below in more detail:

4.1. Human factor

The human factor may be the most significant vulnerability to cybersecurity, and cyber incidents are mainly caused due to lack of training or awareness. i.e., an employee who inadvertently or not, performed an action that allowed an exploit to occur. The vast majority of cybersecurity incidents are related to the human element. TrendMicro's research showed that 91% of targeted attacks involve phishing emails because users continue to fall prey to them [28]. Moreover, it is commonly argued by experts that humans are the weakest link in cybersecurity. This happens because organizations usually invest resources in cybersecurity unilaterally in technology, but they omit to do the same for the human element.

Through increased and sophisticated phishing and social engineering attacks, attackers can bypass most technical controls by simply targeting

Table 5
Risk categories.

Risk categories	Cyber security	
Low	Acceptable (1-3)	A limited adverse effect.The cyber security risk is negligible and no risk reduction is required.
Medium	Tolerable (4-9)	A substantial adverse effect means.The cyber security risk must be reduced to a level as is reasonably practicable
High	Intolerable (>9)	A severe or catastrophic adverse effect. The cyber security risk cannot be justified and must be reduced by additional measures.

Table 4
Risk assessment matrix.

Severtity	Consequences	Probability				
		1	2	3	4	5
	Cyber Security Properties	Very unlikely Practically impossible	Remote Not likely to occur	Occasional Possibility of occurring sometime	Probable Possibility of isolated incidents	Frequent Possibility of repeated incidents
		Once per 30 years or more	Once per 10 years. The scenario is considered unlikely. It could happen, but it would be surprising if it did	Once per 5 years. The scenario might occur. It would not be too surprising if it did	Once per year. The scenario has occurred in the past and/or is expected to occur in the future	More often than once per voyage
1	Non or minor CIA effect	L(1)	L(2)	L(3)	M(4)	M(5)
2	Moderate CIA effect	L(2)	M(4)	M(6)	M(8)	H(10)
3	Major CIA effect	L(3)	M(6)	M(9)	H(12)	H(15)
4	Critical CIA effect	M(4)	M(8)	H(12)	H(16)	H(20)

the human layer. For this reason, any Company should not only set the cybersecurity requirements and policies but most importantly must find a way to efficiently communicate them to personnel and make sure they are applied. To sum up, this pillar concerns both onboard & shore personnel and has the scope of building Cyber Security awareness, skills, and competencies to manage the potential cyber risks, communicating how certain behaviors can be exploited, and training people to respond to cybersecurity breaches adequately.

The company has various procedures and activities relative to training and awareness of the human factor:

- Has assigned responsible personnel — both ashore and onboard — to execute relevant tasks. It has established competence requirements per responsible position and developed a training program, as per the competencies required for each position/responsibility. Any identified training needs are reported to the company's training manager through personnel efficiency reports by each department director and by the Master or Chief Engineer. Identified training needs are considered during the preparation of the annual training plan and budget of shipboard personnel.
- All ships have been provided with cybersecurity e-learning software for crew members. The crew must complete the seminars of the computer-based training (CBT) modules. Each month the training records of each member and the score of each completed module are sent to head office. The monthly reports are reviewed by the training manager, who identifies potential areas of improvement.
- The Master also organizes on-board formal familiarization training to cover, among all the security issues, also the cyber-security subject. The Master schedules at least once per month training seminars during which cybersecurity material is presented. A designated form ("Record of Onboard Seminars") is used to monitor and record the onboard training programs such as the seminars and lectures.
- An onboarding process is obligatory to seafarers during which seafarers are instructed to review and acknowledge the organization's cybersecurity policy. By acknowledging that they have read the organization's policies as a new hire, they are then accountable to adhere to the corporate policy of the organization. Familiarization of Cyber Security policy is given to all vessel and office personnel and conducted by IT Dept. A designated form is used to maintain the training records of ashore seminars, forums, and lectures.
- In-House Seminars: Shore-based seminars are carried out for all Officers. Officers carry out an in-House Seminar at least every two years. The content of the seminar includes Cyber Security training. Attendance is monitored to ensure that all Officers attend shore-based seminars as appropriate. For foreign officers and crew (e.g. Ukrainians, Filipino), an "In House Seminar" is delivered once per year at their countries by department managers and other experienced members.
- Company-wide regular Cyber Security Training: All personnel within the Company receive regular cybersecurity training seminars from certified third parties to improve their awareness and skills. Certain staff members (IT Staff) receive additional and specialized training according to their duties.
- Company responsible departments (IT and Health, Safety, Quality and Environment (HSQE)) frequently provide training material such as Digital Video Discs (DVDs) or send emails and memorandums containing awareness emails and updates about cybersecurity incidents and threats.
- A Cyber Security Campaign a constantly active procedure, and enforced before each audit.
- Software Usage Training Policy. For all company's software assets installed in IT systems, usage training is provided by the responsible department to both shore side employees and seafarers. For OT systems, training is often provided by official vendors of software/hardware, or seafarers are familiarized using the manufacturer's manual.
- Training by visiting Superintendents. During their onboard attendances, designated office personnel relative to cybersecurity (from IT Dept, HSQE, or Vetting Dept) conduct cybersecurity surveys and cybersecurity training to the Crew.
- Cybersecurity Drills. Carrying out a cybersecurity drill is a learning experience, and its purpose is to familiarize and train office and vessel personnel with the existing contingency plans, enabling them to respond to emergencies. Drills are carried out realistically to develop personnel confidence & competency, and the results of the drills are recorded and evaluated through a designated form.

4.2. Infrastructure and technical controls

These are the technical system security measures that need to be scaled to satisfy the specific company cybersecurity requirements without compromising the efficiency and workability of business functions. They provide solid barriers against attacks arising either from insiders or from outsiders.

Email technical infrastructure

About the email technical infrastructure and from a high-level perspective:

- The company's onshore and vessel email accounts are protected through anti-spamming, antivirus, and antimalware central systems implemented in three levels: network perimeter, email server, and email client.
- E-mail accounts are secured by the application of appropriate passwords and multi-factor authentication.
- The system provides application and Uniform Resource Locator (URL) filtering, Hypertext Transfer Protocol Secure (HTTP) proxy filtering on perimeter configured to allow specific categories or "whitelisted" sites while blocking others according to the company's policy.

Corporatenetwork

The major technical controls that the company has implemented for the Corporate Network are:

- Physical security
- Network segregation
- Firewalls and Access Control Lists (ACLs)
- Multi-Factor Authentication (MFA)
- Intrusion prevention systems (IPS)
- Endpoint Security Protection (0-day malware, behavior analysis)
- Intrusion detection systems (IDS)
- Secure software design and configuration.
- Providing software updates and patches
- Vulnerability scanning and patching
- Data Loss Prevention (DLP) systems: Detects potential data breaches and data ex-filtration transmissions and prevents them.
- Data Encryption measures
- Central logging server - Security Information and Event Management (SIEM)
- Security Operations Center - Managed Detection Service
- Sandblast appliance (intercepting and filtering inbound files and inspecting URLs linked to files within emails by running them in a virtual environment) with real-time threat extraction (delivers clean and reconstructed versions of potentially malicious files that are received by email or downloaded from the web)
- Backups: All servers, physical and virtual, are supported with regular, continuous incremental backup images. Access to the backup set is feasible only from the backup server. Additional application-based backups are performed for email and database Servers. Script file backups are used for the personal workstation files of each user.

Remote working laptops

The major technical controls that the company has implemented for the remote working corporate laptops are:

- Virtual Private Network (VPN)
- Sandblast agent
- Hard disk drive Encryption
- Member of domain – Enforcement of domain policy
- Endpoint Protection (0-day malware, behavior analysis)
- Host Intrusion Prevention System (IPS)
- Firewall
- Endpoint Detection and Response
- Multi-Factor Authentication (MFA)
- Umbrella roaming client: protect users from connections to malicious destinations and command-and-control callbacks at the Domain Name System (DNS) and Internet Protocol (IP) layers, no matter where the device connects to the internet.
- Data loss prevention (DLP)

4.3. Procedures and policy

This pillar includes all administrative controls and documentation related to cyber security implementation. The main elements are the policies, procedures, and guidelines that describe organizational processes, define personnel responsibilities and business practices following the organization's specific operations and security objectives. This pillar typically includes the management systems, the governance framework, policies and procedures to reflect cyber security best practices, audit regimes, etc. The central system that contains every company's official documentation regarding the company's procedures and policies is the IMS manual (IMSM).

The documentation that the IMS of the company refers to Cyber Security includes these main sections:

- Cyber Security Policy Statement
- Cyber Security Plan
- Procedure Manuals

4.3.1. Cyber security policy statement

In the Cyber Security Policy Statement, the company declares its commitment to ensuring Cyber Security, by establishing and maintaining the required office and vessel Cyber Security protection measures, to:

- Safeguard the confidentiality, integrity, and availability of Information, Information Systems, and IT / OT equipment.
- Promote the Safety and Security of persons and property within the Organization, both onboard and ashore.

Cyber Security statement also declares the company's commitment and the general requirement and responsibilities for the company's personnel such as:

- Employees to comply with the requirements as described in the Cyber Security Plan (CSP) document and be familiar with their relevant cybersecurity duties and responsibilities.
- Managing director and senior managers to provide all necessary resources onboard and ashore to support the organization's cybersecurity objectives as described in CSP.
- The Company Security Officer (CSO) and IT Manager are responsible for obtaining, managing, reviewing, and sharing cybersecurity-related information for vessels and shore-based locations.
- The Master onboard as the ultimate authority onboard is responsible for taking decisions regarding Cyber Security incidents or threats to maintain safety and security onboard.

Cyber Security statement finally present the Company's cybersecurity objectives and the basic methods that will be achieved, such as:

- Monitoring and implementing regulatory requirements and industry best practices.
- Assigning responsible personnel — both ashore and on board — to execute relevant tasks.
- Performing comprehensive continuous training of all company Personnel.
- Promoting Cyber Security awareness amongst all company Personnel.
- Conducting regular documented reviews and internal audits of cybersecurity policies, procedures, and technical Infrastructure.

4.3.2. Cyber security plan

To document the necessary measures for shore staff and seagoing personnel and deal with cybersecurity, the company has established the CSP. CSP describes the necessary steps to safeguard the company and the vessels under administration from current and emerging cyber threats and vulnerabilities.

More specifically, the cybersecurity plan is a comprehensive document which:

- Define the cybersecurity objectives
- Define required and prohibited actions
- Define duties and responsibilities
- Identify threats and vulnerabilities onboard and ashore
- Describe activity phases of cyber risk exposure assessment
- Present the adopted protection measures for cybersecurity control
- Present the contingency and incident response plan and the cybersecurity incident analysis procedure

4.3.3. Procedure manual "Information Technology and data control"

The scope of this procedure is to describe Information Technology activities and data controls within the company. This procedure sets relevant responsibilities for the company users (managing director, IT manager, IT staff, information system users) and provides instructions and requirements for various IT procedures such as establishing user accounts and passwords, hardware and software usage, antivirus systems usage, backup execution, training, and others.

4.3.4. Procedure manual "Software Management"

The purpose of this procedure is to define the actions that need to be followed to maintain an effective Software Management System to control and protect the company's software assets, whether installed at the office premises or on board the vessels. The procedure covers software installed in Information Technology systems and Operational Technology systems. It covers relevant responsibilities and procedures related to the lifecycle of the software and the decisions that need to be acquired, such as software inventory, updates/upgrades, backup process, usage training, management of Change, software acquisition, testing, and deployment.

4.3.5. Forms

To perform, support, and monitor the activities described in the procedure manuals, various mandatory forms are utilized and required to be maintained up to date. Some important and most indicative procedure forms will be briefly presented in this section. All Information Technology and Operational Technology shipboard and shore systems must be recorded. The IT Manager and the Marine Department, in collaboration with the vessels, must create and maintain a hardware and software inventory for IT and OT shipboard systems. An update process must monitor all software and hardware changes.

More specifically:

- "Office IT Infrastructure Inventory" form is used to record installed hardware in the office.
- "Office IT Software Register" form is used to record installed software in the office.
- "Vessel IT Infrastructure Inventory" form is used to record installed IT hardware onboard the vessels.
- "Vessel OT Infrastructure Inventory" form is used to record installed OT systems onboard the vessels.
- "Vessel IT/OT Software Register" form is used to record installed software onboard the vessels.
- "IT/OT Software Update Form" is used during a software update where specific test procedures and compatibility checks must be performed to ensure integration with existing systems. For monitoring and keeping records of procedure, this form has to be recorded, updated, and reviewed. Software updates fix bugs or add enhancements, and the company ensures that all its software assets are updated with the latest applicably compatible updates.
- "Software Evaluation" form is used to evaluate and test a software program before the actual use on corporate systems. All new software should be tested for correct operation and compatibility with the current infrastructure. It is strictly forbidden to use any software that the responsible departments have not previously checked and approved.
- "Cyber Security Incident Investigation" form is utilized when an assessment/investigation for a cyber security incident is conducted.
- "Antivirus Update / Scan Form" is used onboard to keep records of computer antivirus updates and execution of antivirus scans.
- "PC Inspection Form" is used to accurately record results of diagnostic programs that run on all PCs by the I.T. Dept.
- "I.T. Training Form" is used to identify the training needs of each user and maintain training records of conducted software, policy, and cyber security training for office and crew users.
- "Back up Monitoring Form" is used for backup records monitoring.
- "Password Change Monitoring Form" is used for password change monitoring.

4.3.6. Policies

Procedure manuals and CSP manual further contain the more specific policies such as the hiring and termination policies, separation of duties, data classification, account disablement policy, access rights, business contingency plan or incident response plan, handling of third parties, etc. Some of these policies are briefly presented and include the:

- Personal computer policy: Defines the proper and expected use of the personal computer provided by the company. Example: Under no circumstances should the user change the settings which the I.T. Manager has made.
- Backup policy: Describes the procedures and policies that are defined for backup of production systems. Example: According to the inventory, a backup is kept for every software installed onboard or within the Company.
- Email Policy: Defines the proper and expected usage of the email exchange activity. Example: Email to be used only for Company's business-related purposes. Personal communication is not permitted.
- Third-party access policy: Define the requirements of how the company should interact with third-party service providers and vendors. Indicative example: If the company's partners would like to gain access to the company's network, IT Manager should be informed and access should be provided only under supervision and controlled permissions.
- Software installation policy: Describes the requirements that Company sets regarding software installation on the Company's systems. Indicative example: no installation or use of new software is allowed without the permission and supervision of the IT Manager.
- User accounts Control and User Access Management Policy: Describes the requirements that Company sets regarding how the user accounts and privileges (i.e, rights and permissions) are established, managed, and deleted. Indicative example: Each office user is associated with a unique username and is allocated access rights and permissions based on standard role-based profiles and by the tasks he/she is expected to perform.
- Password policy: Describe the methods for the secure management of passwords. Indicative examples of this policy are: password complexity requirements are enforced to establish secure passwords, passwords are locked after several failed attempts, The passwords of the office and vessel users are managed and periodically changed according to the company procedure.
- Removable media policy: Defines expected usage of removable media (universal serial bus (USB) sticks, compact disks (CDs)/DVDs) on the Company's systems. Indicative contents of this policy are: The use of unauthorized removable media devices on the company's systems is prohibited. Especially for Vessels, all USB ports on IT and OT equipment should be blocked with protection covers.
- Bring Your Own Device Policy (BYOD): This policy defines the accepted practices, responsibilities, and procedures for the use of personally owned mobile devices, including Mobile phones, External hard disks, USBs, tablets, and laptops. Indicative example: Charging personal phones in Vessel's equipment through USB ports is strictly prohibited.

4.4. Cyber security campaign

Although the Integrated Management System (IMS) documentation satisfies the requirements for appropriately addressing "Cyber Risks", of most importance is how it is efficiently communicated. Adding to everything mentioned above, one of the most effective and immediate methods of improving cybersecurity awareness on board and ensuring regulatory compliance is the cybersecurity campaign. By cybersecurity campaign, we refer to the continuous effort and plan to promote straightforward instructions and requirements and periodically remind them through memos and email notifications to all company's personnel, especially to onboard crew. Master and his crew are frequently requested to review and confirm compliance.

The campaign is made up of the following parts:

1. Bring Your Own Device Policy. To be printed and posted inside every cabin, including those used by visitors or company's representatives and smoking rooms.
2. Cyber Security Response Plan. To be printed and posted in public places (Smoking rooms, CCR, ECR, Bridge).
3. Immediate action to be taken after a cybersecurity incident. To be printed and placed along with the Cyber response plan.
4. Identifying Cyber Security breaches and symptoms. To be printed and posted and posted in public places.
5. Guidance on the use of personal devices onboard. To be printed and posted in public places and every cabin, including those used by visitors or company's representatives.
6. Required Actions (DOs) and Prohibited Actions (DONTs). A copy to be given to every crew member and visitor on board. Also, to be posted in every cabin, including those used by visitors or company's representatives. Make a seminar about this to all crew members.
7. Dedicated USB blockers and USB sticks to use onboard. Master is requested to ensure that the vessel is equipped with an adequate number of USB port blockers to lock USB systems, especially on OT systems on board, and that the vessel is equipped with an adequate number of USB sticks to be dedicated on specific IT or OT devices.
8. Enable USB software access control. Restrict unknown USB devices (non-vessel dedicated USB sticks) to have access to critical computers (Navtor/RadioRoom/Bridge) and allow only

dedicated sticks (e.g., Navstick) as per the "EndPoint Antivirus USB Control" document.

9 Refer to Fleet Circular "Antivirus Updates" to verify that the antivirus is updated on all vessel computers.

10 Print Cyber Security Posters and post them within the accommodation at specific indicated places.

11 Review Cyber Security video training material that the company has sent. It is specifically aimed at a non-technical audience and focused on best practice behavior. There are videos of various subjects, e.g., How to Be Cyber Aware At Sea, Passwords, Personal Devices, Phishing, Safe Browsing, Sextortion, Social media, and others.

12 Review Fleet/Interoffice Circular "Instructions regarding Computer Data Security Onboard Vessels." This circular contains guidelines and best practices to be followed to protect the vessel's computer data from any malicious or accidental interference.

13 Review Fleet Circular with subject "Vessels' Computer Data Backup Instructions.".

Backup is the only defense against hardware failures and virus influences.". Backup Monitoring Form" should be completed weekly to maintain records for the backup procedure and be available to be presented to auditors if requested.

14 Review of Fleet Circular with the subject: "Disaster / Recovery instructions for operation & maintenance of vessel IT systems in abnormal / emergency conditions.". This circular deals with the operation and maintenance of vessel IT systems in abnormal or emergency conditions. The following instructions for disaster/ recovery of IT systems onboard must be followed in case of IT equipment damage or malfunction.

5. Performing a cyber security vessel audit survey

5.1. Assessment scope

A cybersecurity audit survey is the systematic, independent, and documented process for collecting evidence and objectively determining whether or not cybersecurity measures are appropriately implemented in an organization.

More specifically, is used:

- to assess conformity with regulatory requirements as well as the company's requirements regarding cybersecurity
- to identify gaps and potential opportunities for improvement
- to set the security profile and requirements.

The company wanted to assess the current status of their vessels regarding Cyber Security preparation (policies, procedures, processes) and the cyber awareness of the crew. The company performed an onboard assessment covering the company's cybersecurity policies, procedures, and related processes, the ISM documentation, and the crew's behavior, focusing on the IT and OT systems in use against regulatory and company requirements. A list of findings and recommendations were identified and documented during the assessment.

5.2. Assessment regime

The company assessed the vessel's IT/OT environment by visual inspection of various locations combined with extensive interviews/ questions/discussion with the crew to assess both infrastructures and crew awareness on-board.

The following locations were included in the scope:

- Bridge
- Master and Crew cabins
- Engine control room
- Cargo control room,
- Recreational areas.

The assessment regime consisted of:

- Interviews with Master, Engineers, Officers, and IT administrators in charge of onboard IT and OT systems.
- Inspection of network cabinets, computers, USB ports, printers, network connections, and other equipment.
- Inspection of OT workstations and their ports in the engine control room and cargo control room.
- Visual inspection of notices posted to check if confidential information is exposed.
- Inspection of PC's event logs (for any security incidents), installed software (check for software not expected, e.g., games), virus scanner existence, reports, and update status.

5.3. Review of policies and procedures

The review of policies and procedures is presented in this section. More specifically, this review presents the general concept that was reviewed, the particular requirements of ISM, the respective references, any indicative questions addressed to Captain and crew officers, and finally, the comments and recommendations for any gaps identified.

Review of remote access policy and procedure.

- Requirement: A list of systems requiring remote access is maintained and regularly updated.
- References: ISM A 3.5.1
- Questions: Is there a list of systems that may require remote access? Is there is a list of approved vendors for remote access? Do the 3d parties connect by themselves, or is access provided by the company? Is there a list of authorized contacts (names and telephone numbers) of 3d parties support? How do you verify the authenticity of the support? Logs must be kept of who, when, and for which purpose executed the remote access
- Comment: A list of systems requiring remote access was not presented on the vessel.
- Recommendation: Create a list of approved remote accesses to the vessel. This list should contain systems requiring remote access and third-party contacts (including names, emails, and phones).

Review of data retention policy

- Requirement: Policy to delete documents, data, and media before disposal exists and is applied for the vessel.
- References: ISM 11.2.3
- Comment: There is no policy to delete documents, data, and media before disposal.
- Recommendation: Create and implement Data Retention Policy where should be defined how long the Company needs to hold on to specific data, the period to clean this data, and who will do that action. The company should only retain data for as long as it is needed.

Review of drills

- Requirement: Cybersecurity drills and exercises must be executed (at least annually) and recorded to verify the effectiveness of cybersecurity reporting, response, and recovery measures.
- References: ISM 1.4.5, 8.2, 8.3, A 3.5.4
- Questions: Are there records of cybersecurity drills performed?
- Comment: No cybersecurity drills have been executed for this vessel.
- Recommendation: Execute cybersecurity drills between the vessel, the office, and related third parties.

Review of backup policy and procedure of critical IT systems.

- Requirement: Backups on IT systems (and, where applicable, OT systems) on board are executed regularly (at least weekly), and information is stored on disconnected storage media.
- References: ISM 10.4, A 3.5.5
- Questions: Which are the systems to follow backup procedures, and how is backup executed? What is the data retention policy? What is the procedure to update the Electronic Chart Display and Information System (ECDIS)? Records were requested to prove the execution of backups.
- Comment: Backups of IT systems are executed as per the company procedure. ECDIS system backup should be executed every month, but there was observed that last month's backup was missed.
- Recommendation: To ensure adequate backup of the operating system of ECDIS emergency computer, add the description of this process into the procedure and create a list of last executed backups. This list should be updated after every backup and communicated to the office.

Review of incident reporting scheme.

- Requirement: Cybersecurity event or incident reporting scheme, including a reporting form and procedure, is utilized and implemented on the vessel.
- References: ISM 8.1, 8.3, 9.1, A 3.5.3
- Comment: Evidence provided. Cyber Security event and incident reporting scheme exists, is printed and is clearly visible in several locations onboard.

Review of cyber response plan and disaster recovery plan.

- Requirement: Dedicated cybersecurity response and recovery plan exist on the vessel and include instructions on how to react in case of an incident.
- References: ISM 1.4.4, 1.4.5, 8.1, 8.3, 9.2, A 3.5.4
- Questions: Do you have a disaster recovery plan for the vessel IT systems? Is there a Cyber Response Plan? Who do you inform in case you suspect something suspicious? In case of an incident, which steps will be followed? If/ when to conduct an impact assessment, who needs to be informed during and after the incident? Who should record what happens during the incident?
- Comment: Evidence provided, but some information is missing.
- Recommendation: Implement response scenarios in case of failure of specific critical systems, e.g. address procedural steps for the recovery of loss of stability and loading computers or the recovery of loss of VSAT communication.

Review of crew cybersecurity training

- Requirement: Cybersecurity training is implemented for new crew members. Records of the crew who attended cybersecurity training are kept.
- References: ISM 1.2.2.3, 6.3, 6.4, A 3.7
- Questions: Is there a cybersecurity training program? Are there records of cybersecurity familiarization or seminars?
- Comment: Evidence provided

Review of Cybersecurity awareness

- Requirement: Cybersecurity awareness of crew is established. Crew and officers are aware of potential cybersecurity threats and how to report any incidents or events. Cybersecurity roles and responsibilities of the crew and onshore staff are well defined and understood.
- References: ISM 2.2, 6.5, 6.6, 8.1, A 3.5.3, A 3.7
- Questions: In a scenario of a received email message urging to click provided link or log in somewhere to download a file, what would your actions be, and what should you be aware of when looking into an email? What is phishing? Even if you click something suspicious, what should you do? What is allowed and what not to post on Facebook and other social media? Is there an official policy on how to behave on social media?
- Comment: Evidence provided. Crew awareness is good, and crew staff knows their responsibilities

Review of cybersecurity policy onboard exposition

- Requirement: Cyber Security Policy is available at all locations and known to all personnel ashore and onboard. Cybersecurity awareness is included in safety instructions for visitors on board.
- References: ISM 2.2, 11.2.1, A 3.7, 13.2.4
- Comment: CS Policy available on board. Distributed also via internal circulars and main awareness posters were printed in several locations onboard.

Review of inventory of systems/software

- Requirement: Inventory of installed IT and OT systems and software exists and is updated following changes to the hardware and software.
- References: ISM A 3.5.1
- Questions: Is there an inventory of OT systems installed onboard? Is there an inventory (showing designated IP addresses) of IT systems and computers installed onboard? What is the process/schedule to update it? Is the list of software onboard documented?
- Comment: Inventory of main installed software and related computers exists, but updating this inventory is done regularly once a year and does not follow the change management process to the hardware and software.
- Recommendation: Improve the process to update installed IT and OT systems inventory after changes to the hardware and software were executed. This allows having updated and accurate inventory.

Review of IT/OT systems physical aspects

- Requirement: On-board networks, including wiring, patch panels, and network elements, are physically protected. On-board critical IT/OT infrastructure components are installed in racks, or closed cabinets and cabinets are locked.
- References: ISM A.2.5.1, A 3.5.2, 10.3
- Questions: Where are the critical IT systems located? Is the rack physically locked? Who has the key for the rack? Who has access to these systems? Are the cables, systems, and components labeled to be easily identified when relying on instructions to do something?
- Comment: Evidence provided

Review of IT security software and Antivirus protection

- Requirement: Anti-malware software is installed and active on all computers onboard and updated regularly. Anti-malware scans are required before connecting to privileged or safety-critical systems. Tools for the detection and analysis of cybersecurity events and incidents are utilized.

Questions: Which security software is implemented to protect the IT systems? What is the procedure to update antimalware/antivirus onboard? How do you update the standalone computers? Records of the antivirus update form and scan results were requested to present.

- References: ISM 8.1, 8.3, 10.1, A 3.5.2, A 3.5.3
- Comment: Evidence provided.

Review of USB control.

- Requirement: Policies and procedures to securely deal with removable media devices are applied on the vessel. Training for employees and crew on how to securely handle removable media devices is performed.
- References: ISM 7, A 2.1.6, A 3.5.2, A 3.7
- Questions: How is USB control managed and USB risk mitigated? Do you have a "bring your own device policy"?
- Comment: Evidence provided. General cybersecurity training for the crew is provided every month, but specific training on how to securely handle mobile devices has not been executed.
- Recommendation: Include specific training on how to securely handle mobile devices into the training plan for the crew.

Review of Criticality of systems.

- Requirement: There is knowledge of which systems failure may result in hazardous situations.
- References: ISM 10.3, A 3.5.1
- Questions: Which systems are critical? Is the criticality of systems documented? Need to be clearly visible which systems may lead to hazardous situations in case of failure of software or equipment of the computer.
- Comment: Inventory of main installed softwareand related computers exist, but software has not been ranked by criticality. Therefore, it was not possible to understand which system may cause hazardous situations.
- Recommendation: Include criticality of software.

Review of software and hardware management.

- Requirement: Obsolescence management procedure, incl. updating/upgrading of software, hardware and networks components exists and is applied for the vessel.
- References: ISM 10.1, A 3.5.2
- Questions: Is there a software and hardware management procedure to cover shipboard systems?
- Comment: Software Management Procedure exists, but how to update/upgrade of hardware and networks components are missing. 2 computers with obsolete OS were found with no plan to be replaced.
- Recommendation: Create and implement a procedure for Obsolescence Management for Hardware and Software as part of the already created Software Management Procedure. This plan should contain the replacement of already obsolete systems which are difficult to patch and also systems that will be obsolete in near future.

Review of Management of Change (MOC).

- References: ISM 7, 10.1, A 3.5.2
- Requirement: The Management of Change procedure exists and is applied for the vessel.
- Comment: Evidence provided

Requirement: Process to manage security patches for all onboard IT and OT ensuring that security-relevant updates are installed in a timely manner is implemented.

- References: ISM 10.1, A 2.5.1, A 3.5.2
- Comment: Evidence provided

Requirement: Cyber risk assessment process exists and is executed regularly (at least annually) or in case of changes to IT and OT systems and networks.

- References: ISM 1.2.2.2, A 3.4, A 3.5.2
- Comment: A cyber risk assessment process exist but was executed on a generic fleet perspective.
- Recommendation: Check that the generic threats, systems, and vulnerabilities are relevant for this particular vessel. Issue an updated risk assessment for the specific vessel and update it on a scheduled regular basis.

Review of IT and OT systems connectivity

- How are OT systems onboard protected? Is there any interconnection between IT and OT networks? Does segregation of networks exist? Can these systems be reached from networks? Provide the diagram of the vessel network topology.

5.4. Major positive findings

Positive findings during the assessment include:

- The vessel Cyber Security preparedness levels are very good and well above average for tanker operators.
- There are solid and practical measures to mitigate risks from external USB devices, e.g., all ports were locked for all systems with access to the network.
- IT systems in cabins were labeled, and the crew knows which system belongs to which cable and equipment.
- Overall, cybersecurity awareness of master, officers, and crew was very good and demonstrated competence in handling daily risks and threats.
- The Cyber Security company policy was evident in multiple locations, and the crew was aware.
- No confidential information was publicly available or undisclosed

5.5. Major gaps and recommendations

Very few gaps were identified through the assessment.

- There was no list of remote accesses to the vessel. Therefore, the crew was not able to say which systems require remote access, for which purpose, and if this remote access was approved or not. A list should be created containing the systems requiring remote access and the respective third-party contacts (including names, emails, and phones).
- No cybersecurity drills have been executed for this vessel. Therefore, the crew has not been able to prove their cyber resilience in practice. Drills help test cybersecurity resilience and crew awareness across IT and OT environments by simulated cybersecurity exercises. These drills should occur regularly following a reasonable time plan.

6. Conclusions

Ships are part of cyberspace, and shipboard IT and OT systems convergence is an ongoing process. The complexity of ships is constantly increasing, with more software and automation, more internet connectivity, and more interconnection between systems onboard. It will extend entirely to reach a level of fully autonomous ships. Consequently, the attack surface of the vessel has increased, meaning that each of the shipboard cyber-systems may hinder cyber vulnerabilities either due to inadequate design or inadequate configuration. Additionally, malicious actors have various motives to target maritime, while advancements in attack capabilities and sophistication techniques increase risk. Malicious actors usually target the human factor. Hence it is a priority to raise the maritime sector's cybersecurity awareness. This study reveals that cyber threats are real and that maritime companies need to get over outdated misconceptions and practices. Executive-level support for cybersecurity is required to give enough resources to implement cybersecurity. The level of risk is innately very high because when these systems are impacted, the ship's safety is at risk, and consequently, the risk is life, property, environment, and all of the above. Since the level of risk is so

high, it is essential to identify and manage it accordingly, as well as restrain and minimize its negative impacts.

Nevertheless, maritime stakeholders need to see the digitalization and automation of the industry as an opportunity. Cybersecurity resiliency is the key for safely realizing the benefits of digital shipping and doing operations better. Most companies are looking to remote operation, reduce costs of their operations, optimize performance, take advantage of a better logistics chain, reduce maintenance and provide better and more efficient services. The companies that will resist digital evolution will lag behind the competition. Those who will embrace it may gain a competitive advantage. Since the 1st of January 2021, Cybersecurity is also a regulatory requirement for the industry and part of safety administration activities. Management companies and their vessels will be subjected to audits by class society inspectors and port state controls to prove that they successfully address cyber risks. The company should follow a cybersecurity framework/management system to effectively deal with people, procedures, and technology. The risk management approach should be resilient and evolve as a natural extension of existing management system practices. There is no 'one size fits all solution. Although common traits do exist, since no two organizations are the same, a custom fit-for-purpose delivery model should be used based on an individual company's performance, needs, procedures, and systems.

Companies should establish continual improvement programs through the Integrated Management System. The two major critical elements of any effective cyber risk assessment system are the risk assessment and the audit survey. The risk assessment process allows the company to identify possible hazards in its operations/activities, estimate and evaluate risks posed by each risk, and establish appropriate controls to minimize the risk levels. The cybersecurity audit survey process allows the company to assess the current status, collect evidence and objectively determine whether or not cybersecurity measures are appropriately implemented or not. Both processes are vital to monitor the gaps identified and to mitigate cyber risks. Eventually, they allow the company to continuously improve its systems and move to a more predictive and proactive maturity level. Maritime industry bodies, associations, regulators, and stakeholders should agree on a continuous collective effort to improve cybersecurity by discussing open gaps and taking appropriate measures. Pressure should be put on shipboard systems vendors to provide cybersecurity certified systems, and cybersecurity by design requirements must be enforced to ship new buildings to reduce cybersecurity risks.

CRediT authorship contribution statement

Evripidis P. Kechagias: Conceptualization, Methodology, Writing – original draft, Writing – review & editing. **Georgios Chatzistelios:** Methodology, Data curation, Formal analysis, Investigation. **Georgios A. Papadopoulos:** Project administration, Software, Supervision, Validation, Visualization. **Panagiotis Apostolou:** Conceptualization, Writing – original draft.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] ICS, Shipping and World Trade: Driving Prosperity, International Chamber of Shipping. (2021). https://www.ics-shipping.org/shipping-fact/shipping-and-world-trade-driving-prosperity/(accessed September 15, 2021).
[2] UNCTAD, Review of Maritime Transport 2020, United Nations Conference on Trade and Development. (2020). https://unctad.org/webflyer/review-maritime-transport-2020 (accessed September 15, 2021).
[3] Allianz, Safety and Shipping Review, Munich, Germany, 2020. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2020.pdf (accessed September 15, 2021).
[4] BIMCO, The Guidelines on Cyber Security Onboard Ships, Bagsværd, Denmark, 2020. https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (accessed September 15, 2021).
[5] D. Cimpean, J. Meire, V. Bouckaert, S. vande Casteele, A. Pelle, L. Hellebooge, Cyber Security Aspects in the Maritime Sector, Hraklion, Greece, 2011. https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1 (accessed September 15, 2021).
[6] J.I. Alcaide, R.G. Llave, Critical infrastructures cybersecurity and the maritime sector, Transp. Res. Procedia 45 (2020), https://doi.org/10.1016/j.trpro.2020.03.058.
[7] A. Androjna, T. Brcko, I. Pavic, H. Greidanus, Assessing cyber challenges of maritime navigation, J. Mar. Sci. Eng. 8 (2020) 1–21, https://doi.org/10.3390/jmse8100776.
[8] L. Ayala, Cybersecurity Lexicon, 1st ed., Apress, New York, USA, 2016.
[9] Futurenautics, Crew Connectivity Survey Report 2015, Futurenautics Ltd. (2015). https://www.futurenautics.com/product/2015-crew-connectivity-survey-report/(accessed September 15, 2021).
[10] Futurenautics, Crew Connectivity Survey Report 2018, Futurenautics Ltd. (2018). http://www.navarino.co.uk/wp-content/uploads/2018/04/Crew_Connectivity_2018_Survey_Report.pdf (accessed September 15, 2021).
[11] IMO, Maritime Cyber Risk, International Maritime Organization. (2019). https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (accessed September 15, 2021).
[12] MARSH, Global Marine Practice The Risk of Cyber-Attack To the Maritime Sector, Marsh & McLennan Companies. (2014). https://www.ahcusa.org/uploads/2/1/9/8/21985670/the_risk_of_cyber-attack_to_the_maritime_sector-07-2014.pdf (accessed September 15, 2021).
[13] K. Tam, K.D. Jones, M. Papadaki, Threats and Impacts in Maritime Cyber Security, Engineering & Technology Reference. 1 (2012). 10.1049/etr.2015.0123.
[14] WEF, The Global Risks Report 2021, Geneva, Switzerland, 2021. https://www.weforum.org/reports/the-global-risks-report-2021 (accessed September 15, 2021).
[15] Allianz, Allianz Risk Barometer Identifying Hte Major Business Risks for 2021, Munich, Germany, 2021. https://www.assiteca.it/wp-content/uploads/2021/01/Allianz-Risk-Barometer-2021.pdf (accessed September 15, 2021).
[16] J. Daffron, Shen Attack Cyber Risk Scenario: up to $110 billion at risk from maritime malware attack, Cambridge Centre for Risk Studies. (2019). https://risk-studies-viewpoint.blog.jbs.cam.ac.uk/2019/10/30/shen-attack-cyber-risk-scenario-up-to-110-billion-at-risk-from-maritime-malware-attack/(accessed September 15, 2021).
[17] J.-E. Vinnem, I.B. Utne, Safe Societies in a Changing World : Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway., Taylor & Francis Group, London UK, 2018. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2586644/10.1201_9781351174664-188.pdf?sequence=2&isAllowed=y (accessed September 15, 2021).
[18] C. Cimpanu, All four of the world's largest shipping companies have now been hit by cyber-attacks, ZDNet. (2020). https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/(accessed September 15, 2021).
[19] A. Sheperd, What is NotPetya?, ITPro. (2021). https://www.itpro.co.uk/malware/34381/what-is-notpetya (accessed September 15, 2021).
[20] C. Pownall, The Context and Impact of Maerk's NotPetya cyber attack, London, UK, 2019. https://charliepownall.com/maersk-notpetya-cyberattack-timeline/(accessed September 15, 2021).
[21] P. Kapalidis, Cybersecurity at Sea, in: 2020. 10.1007/978-3-030-34630-0_8.
[22] IMO, Guidelines on Cyber Risk Mangement, London, UK, 2017. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf. (accessed September 15, 2021).
[23] M. Barrett, Framework for improving critical infrastructure cybersecurity, in: Proceedings of the Annual ISA Analysis Division Symposium, 2018.
[24] IPA, Cybersecurity Management Guidelines Ver 1.1., Tokyo, Japan, 2016. https://www.yumpu.com/en/document/view/56523440/cybersecurity-management-guidelines-ver-11 (accessed September 15, 2021).
[25] DNV, Cyber security resilience management for ships and mobile offshore units in operation, Høvik, Norway, 2016. https://www.gard.no/Content/21865536/DNVGL-RP-0496.pdf (accessed September 15, 2021).
[26] ABS, Guidance notes on Risk Assessment Applications for the Marine and Offshore Industries, Spring, USA, 2020. Guidance notes on Risk Assessment Applications for the Marine and Offshore Industries (accessed September 15, 2021).
[27] INSB, International Naval Surveys Bureau Class, INSB Class. (2010). https://insb.gr (accessed September 15, 2021).
[28] Trend Micro, Spear-phishing email : most favored APT attack bait, Trend Micro Incorporated. (2012). https://documents.trendmicro.com/assets/wp/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf (accessed September 15, 2021).