Mersin University
Journal of Maritime Faculty

Mersin University Journal of Maritime Faculty (MEUJMAF)
Vol. 5, Issue 2, pp. 22-36, December 2023
e-ISSN 2687-6612, Türkiye
DOI: 10.47512/meujmaf.1370274
Review Article

THE ROLE OF CYBER SITUATIONAL AWARENESS OF HUMANS IN SOCIAL ENGINEERING CYBER ATTACKS ON THE MARITIME DOMAIN

Cihat AŞAN *[1]

[1] Piri Reis University, Maritime Faculty, Maritime Transportation and Management Department, Tuzla, Istanbul, Türkiye
ORCID ID 0000-0003-3674-6616
e-mail: casan@pirireis.edu.tr

* Corresponding Author
Received: 02/10/2023 Accepted: 12/12/2023

ABSTRACT
Through technological advancements, the expanding proportion of maritime transportation on a global scale is becoming faster, more automated, more digital, and ultimately more cyber-space. In particular, the Industrial Revolution 4.0 has brought real-time digital integration of stakeholders in the maritime industry, both on land and at sea, into cyberspace. However, the scope of life and property protection at sea has expanded with the participation of the cyber environment as well as the physical environment. The human factor plays a leading role in ensuring the security of both the physical and cyber environment. In parallel, the main target of hackers who try to gain profit by violating the security environment is the person who does not have sufficient situational awareness of cyber security and can be called the weakest link in the chain. In this study, as main goal, the role of the situational awareness of the employees in the past cyber-attacks on the maritime industry was examined, and a perspective on the measures to be taken was presented. To achieve this research goal, the study utilized the snowballing technique to access literature, which helped uncover additional relevant resources not initially detected. This was followed by a systematic analysis of the collected literature. An analysis of attacks conducted since 2010 revealed that 76% of them utilized social engineering methods, such as phishing, malware, and ransomware. These attackers appear to exploit the maritime industry's insufficient cybersecurity awareness among its employees and the lack of a comprehensive understanding of cybersecurity within the industry.

Keywords: *Maritime industry, Cyber security, Cyber-attack, Situational awareness*

1. INTRODUCTION

Throughout history, changes in production have shaped societies and lifestyles, creating new needs. This transformation is driven by economic demands, supply and demand dynamics, and international trade. These advancements have fostered and advanced capitalism, often labeled as the "industrial revolution" in academic discourse. Industry 4.0 represents the convergence of information technology and manufacturing, affecting multiple sectors, including the maritime industry.

Maritime transportation is an indispensable means of importing and exporting various commodities in the contemporary era. The advancement of technology has led to the progression of the technical structure of ships through the implementation of digitalization, integration, and automation systems. Developments that have been brought into the scene by Industry 4.0 have introduced concepts such as smart ports, intelligent vessels, and automated operations in maritime operations. Regarding the maritime domain in general, although all activities such as port administrations, management of ships, class organizations, ship agents, equipment manufacturers, ports, terminals, and logistic activities are based on the computer system, this technological change also includes negative aspects. Besides creating opportunities for maritime companies and commercial stakeholders, technological developments have also provided opportunities for crime actors by making the sector vulnerable to cyber-attacks (Fitton et al., 2015). With the rise of cyber-attacks, it is anticipated that in the future these attacks have the potential to seriously disrupt critical infrastructure. It is evident that the maritime industry conducts more cost-effective operations in line with technological advancements. However, the threat level posed by cybersecurity risks accompanying these technological advancements is crucial for security. In this context, a critical question arises: "What is the role of employees in the damage caused to the maritime industry by these emerging cybersecurity threats?"

Based on this research question study focused on human behaviors in cybersecurity. Hackers may employ social engineering techniques to obtain access to an organization's network by taking advantage of interpersonal relationships or social abilities (CISA-US, 2020). These human manipulations, which are utilized by hackers, have progressed from the stage where they try to convince company users to reveal their accounts to the stage where they use social networking sites to undertake reconnaissance to get relevant information about an enterprise (Algarni et al., 2013). As a part of this process, it is essential to recognize that cyber security is a human behavior issue, and not exclusively a matter for the Information Technology (IT) departments (Alcaide and Llave, 2020). This is supported by data that shows that human conduct, whether done purposefully or accidentally, is a common source of cyber mishaps (Futurenautics Maritime-KVH and Intelsat., 2018). Despite this, the primary factors that lead to cyber-attacks are incredibly nuanced, and in the context of maritime cyber security, people may be both an indispensable resource and a potential threat (Hareide et al., 2018).

The main goal of this study is to demonstrate the role of employees' situational awareness of cyber security by conducting a state-of-the-art literature review of past cyber-attacks against the maritime domain. For this purpose, the resources of the resources were reached with the snowballing technique (Wohlin, 2014) so that the work was deepened by providing access to the resources that were not detected at the first stage, but which were related to the subject. Under the auspices of Okoli processes, a literature review was undertaken based on four primary steps: planning, selection, extraction, and implementation (Okoli, 2015). As a result of this review, findings have been presented, and while the role of cyber risk perception and situational awareness of humans in social engineering cyber-attacks on the maritime domain has been put forward as a conclusion, ideas for improving this awareness have been put forward as recommendations.

The conclusion stems from the analysis of cyberattacks conducted since 2010 in the maritime domain, revealing that 76% of them employed social engineering methods. Consequently, the primary outcome of the study indicates a substantial deficiency in employees' cybersecurity awareness, necessitating substantial and altruistic endeavors for improvement.

The major importance of the study is highlighting that the concept of cybersecurity in the maritime industry is not the responsibility of a specific group; especially, it underscores the significance of the human factor and how it represents both a crucial aspect and a weak link. In light of studies like this one, it is essential to conduct more comprehensive research to prioritize measures related to human behavior in cybersecurity.

2. LITERATURE REVIEW

Some research on cybersecurity has focused on examining situational awareness, which may include cognitive studies (D'Amico et al., 2005; Kokar and Endsley, 2012; Mahoney et al., 2010; McNeese et al., 2012). Other research has looked at behavioral elements to gain a better understanding of general cybersecurity awareness in organizations (Bada et al., 2019; Lebek et al., 2014; Pfleeger and Caputo, 2012).

The study of Farah et al., (2022), presents a taxonomy of cyber-attacks focusing on the maritime industry. has been provided and an analysis of cyber-security frameworks has been offered. In their study, Larsen and Lund, (2021) present a method for examining cyber risk perception through the use of acknowledged psychological models and give a current research overview of the topic in the context of the maritime realm.

To investigate the correlation between Cyber Curiosity and Situational Awareness, and their impact on cyber risk in organizations, Perez, (2019) created an interactive web-based site survey. The study was conducted with a total of 174 Information System (IS) users, comprising 120 maritime and 54 shoreside users. The information obtained was subjected to analysis to ascertain whether there exist any noteworthy variances in the degrees of Cyber Situational Awareness and Cyber Curiosity among IS users who operate in maritime and shoreside settings. Additionally, the study sought to examine how their respective positions within the established Cyber Risk classification scheme impact these constructs.

Mraković and Vojinović, (2019a) address some of the most significant challenges facing the maritime industry from the point of view of cyber security and offer some suggestions for resolving or mitigating those challenges.

Due to the growing awareness among hackers of the cyber vulnerabilities present in the maritime domain, and with their assessment of the inadequacy of existing risk assessment tools in addressing the distinct character of maritime cyber threats, Tam and Jones, (2019) put forward a model-based framework for risk assessment. This framework combines both cyber and maritime factors to better assess the risks faced by the maritime industry.

Bolat and Kayışoğlu, (2019) investigated cybersecurity awareness in the maritime industry, utilizing the Turkish Maritime Sector as a case study. Employing Structural Equation Modeling the study emphasizes the significant role of education in enhancing cybersecurity awareness. It also highlights the impact of cybersecurity incidents on both awareness and behavior, establishing a noteworthy correlation between maritime cybersecurity awareness and the adoption of secure user behavior. Importantly, the study suggests that factors such as rules, policies, and information sharing have limited influence on cybersecurity awareness and the development of secure employee behavior.

3. METHODOLOGY

With the progression of technology, the proliferation of Industry 4.0 in the Maritime domain has entailed the emergence of cyber security concerns. The exploitation of the vulnerabilities inherent in human behavior, commonly referred to as social engineering, is a significant factor in the success of cyber-attacks. The absence of cognizance about social engineering attacks can make an organization more susceptible to cyber-attacks. To fulfill the objective of the study, the literature was initially accessed utilizing the snowballing technique (Wohlin, 2014), thereby allowing for a greater understanding of the topic at hand by providing access to resources that were not initially detected, yet still associated with the subject. The literature was subjected to a systematic analysis utilizing the Okoli processes, as outlined in Figure 1.

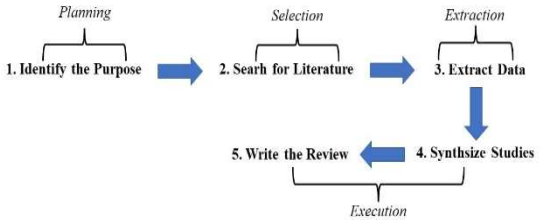

Fig. 1. Methodology for constructing the literature review (Okoli, 2015)

During the 'Planning' stage, the purpose and scope of the scan were established as cyberattacks that had been perpetrated directly against the maritime sector since 2010, with successful results and significant consequences. In the "Selection" phase, the literature relevant to this purpose was identified through reports and existing studies. In the "Extraction" phase, the targets of the listed cyber-attacks were scrutinized, and during the "Execution" phase, the evaluation of which of these targets were executed through ransomware/malware exploiting the situational awareness deficiency of the staff within the ambit of social engineering was completed.

4. CYBER RISKS IN THE MARITIME DOMAIN

The Industrial Revolutions played a pivotal role in driving industrialization, accelerating economic growth, and causing significant shifts in societal structures. Presently, modern industrial production technologies continue to bring about revolutionary changes, with a growing impact on the global economy. We are now in the era of Industry 4.0, often termed the fourth industrial revolution or the digitization period. In the maritime industry, Industry 4.0 technologies are actively employed to enhance the efficiency, safety, and sustainability of ships and their operations. This transformation involves the integration of advanced technologies into ship design, construction, and operation, resulting in a more efficient, secure, and sustainable maritime sector. However, the challenge of safeguarding against cyber threats has emerged as a significant obstacle for companies adopting the Industry 4.0 framework to maintain their competitive edge.

The management of cybersecurity within Industry 4.0 is a pertinent and evolving subject in contemporary academic literature. While various methodological solutions have been proposed to address cybersecurity concerns in the context of Industry 4.0, there is a gap in these solutions, as they do not adequately establish links between critical assets requiring protection against cyber-attacks and the subsequent impacts on business operations, nor do they provide a measurable metric for assessing these effects. (Corallo et al., 2020).

With Industry 4.0, the concept of risk management against cyber threats has also found its place on the agenda. "Cyber risk" refers to the potential harm stemming from the manipulation of cyberspace by adversaries, involving threat assessment, vulnerability evaluation, and an understanding of the consequences. In contrast to "cyber-attacks," which are specific offensive actions, "cyber risk" takes a more holistic view, encompassing the broader landscape of vulnerabilities, threats, and potential impacts, along with measures to manage and respond to digital threats. This manipulation may target various components of cyberspace, including computer systems, services, embedded processors/controllers, and data that is either while in stored or in process. When examining the cyber threats that merchant vessels face, it is advantageous to classify their systems into two distinct categories: Onboard Operational Technology (OT) systems are cyber-physical systems that interact with their environment by controlling physical components and processes. This includes handling cargo frameworks, bridge facilities, propulsion and machinery executives, and power management systems. IT systems, on the other hand, refer to a range of functions such as data management, access control, passenger management, networking, executive and crew assistance, communication, and ship-to-shore connections. In sum, merchant ships and their management must be aware of the risks posed by both OT systems and IT systems. (Refsdal et al., 2015), (IMO, 2017).

In particular, the scope of such risks will increase in the possibility of the spread of passenger and cargo transportation without a ship crew (autonomous. ships) in the coming years. To engage in maritime activities that

involve such as Global Positioning Systems (GPS), autonomous technology, physical safety sensors, digital certificates, cargo tracking, electronic navigational components, automatic identification systems, and record keeping it is imperative to utilize secure computers and an encrypted internet connection. All of these systems are vulnerable to cyberattacks whenever they are connected to the internet. To give an example of the damages that can occur with various malware attacks; damage to sensitive cargoes, cargo hijacking, delay, loss, damage, damage to transportation facilities (port, marina, etc.), the collision of ships, accident of port operators, alteration or destruction of information in the bill of ladings and cargo manifests, seizure of trade secrets, commercial reputation injury, etc. Because data has value like capital in cyberspace, data protection is also important. In addition to company data, personal data is also at risk from cyber dangers. Although the results of cyber-attacks are generally economic damage, they have a high potential to harm people and the environment. Accidents that may result in injury or death may occur due to the steering of ships for malicious purposes, or the deactivation or steering of machinery. Again, as a result of malicious cyber interventions environmental damage is inevitable via physical damage such as collision or grounding and the leakage of the ship's fuel or harmful chemicals and cargoes.

4.1. Types of Cyber Attacks

According to the studies that are cited in the following paragraphs, the most significant maritime cyber challenges present themselves in the following forms:

4.1.1. Spear-phishing: It is the most prevalent cyber incident type. Among the most common attacks is spear-phishing, which uses emails containing suspicious links to obtain unauthorized access. (Clark, 2018; Mraković and Vojinović, 2019c). There are two primary classifications of attacks: social engineering and malware-based. Social engineering relies on exploiting human curiosity or carrying out illicit activities (Jensen, 2015), while malware-based attacks utilize malicious software (Gupta et al., 2017). With regards to social engineering, attackers endeavor to cause harm using electronic mail which might appear innocuous upon first assessment, or by means of bogus websites. Conversely, malware phishing employs malicious programs that are installed on the user's computer. Maritime vessels are commonly subjected to this type of security threat by way of electronic mail. E-mail communication typically includes a hyperlink to a false website, where the individual may unknowingly enter confidential information, for example, their username and password, due to either a lack of attention or understanding. Typically, when personnel are overworked and inattentive to the information contained within emails or the associated hyperlinks, this occurs. Despite the prevalence of spear-phishing attacks, port managers are reticent to report incidences, due to the sensitivity of the maritime sector, as breaches can have adverse implications not only for the confidentiality of individuals but also for the economic ties between nations. (Mraković and Vojinović, 2019c).

4.1.2. Ransomware: Malicious software of this type is commonly referred to as malware. It is often the case that an e-mail that appears innocuous can create significant disruption. Ransomware is typically presented in the form of Portable Document Format (PDF) or compressed (ZIP) files, which are attached to electronic mail messages. The initiation of the malware may lead to a denial of access to documents or the system as a consequence of opening these files, posing a danger to the system. The resolution would involve reimbursing ransom to successfully regain access to files or systems. (Mraković and Vojinović, 2019c).

4.1.3. Distributed Denial of Service (DDoS): DDoS attacks are regarded as criminal. The port IT systems have been rendered inaccessible due to the inundation of the network with an excessive amount of traffic, thus obstructing access to its sites. (Kessler and Uk, n.d.).

4.1.4. Port Scanning: Attackers ascertain the most susceptible network ports by utilizing the traditional approach of scanning. The objective is to ascertain the condition of services, determine the best method to gain access to databases, and recognize which users are cognizant of services. At the most sophisticated level, the perpetrator utilizes IP fragmentation to perplex the firewall, thus allowing the packet filters to be circumvented. Another approach is based on interrogating a port at the Transport Layer of the Open Systems Interconnection (OSI) Model, to scan IP addresses through a trial of multiple protocols and other ports. The test models employed by a hacker are created randomly (Hindy et al., 2021).

4.1.5. Supply chain: Attacks on the supply chain can be focused on exploiting the weakest element within the entirety of the end-to-end network to create disruption (Lam and Bai, 2016). The successful facilitation of global shipping and transportation of cargo from origin to concluding destination relies upon essential processes and stakeholders for container tracking, confirmation, and intercontinental permissions. An illustrative instance of a deleterious effect of an attack is the alteration of the destination of a container, which necessitates expertise in the supply chain and the susceptibilities within it, to adjust critical data. (Mraković and Vojinović, 2019c).

4.1.6. Man in the middle (MITM/MIM): This kind of malware exploits weaknesses in the SSL/TSL protocol, which facilitates communication between two networks (Čekerevac et al., 2017; Mallik et al., 2019). In such circumstances, the downloading of significant data takes place while users rarely can detect it.

4.1.7. Data theft: In many cases, it is not detected until after an extended period or is not acknowledged at all. Unauthorized data duplication or downloading is occurring. Engagement in criminal endeavors through the utilization of ransomware and malware, with illicit access leading to both data theft and data erasure to disguise evidence or inflict immense damage to corporate entities. (Borazjani, 2017).

4.2. Human Factor in Cyber Security

The end user plays a crucial part in cybersecurity by helping to guard against, identify, and counteract cyberattacks. Cybersecurity is a user-centric notion that necessitates the implementation of secure behavior to protect against online vulnerabilities and assaults. Users' awareness of the importance of cyber security to their personal and professional lives has emerged as a major obstacle to the continued success of digital information exchange. End users are workers, so they should be made aware of the importance of their role in maintaining the safety of the cyber-physical system and safeguarding the data that passes through it. Cyberattacks can occur due to human error, such as the use of weak passwords, the opening of unfamiliar e-mail files, or the disregarding of dangers brought about by wireless networks and mobile devices at work. Therefore, education is the first line of protection. (NSI, 2017). In addition, fostering a culture of cybersecurity consciousness and encouraging a proactive approach to threat identification and reporting should be integrated into the overall strategy to address the human factor. This involves promoting vigilance, clear reporting channels for suspicious activities, and ongoing awareness campaigns to ensure that cybersecurity remains a collective responsibility within the organization.

Because the human component has become such an essential concern to ensure cybersecurity, the businesses that are directly connected to the human element may be exposed to a significantly higher level of risk than the other sectors. Given these circumstances, the maritime transportation industry becomes a major hub from the point of view of cybersecurity. This is due to the fact that 90% of maritime accidents have happened due to human-related mistakes. When incidents and penetration tests involving cybersecurity in the maritime industry are evaluated, it is clear that a dearth of knowledge and an inability to adopt safe behavior are significant contributors to the frequency of cybersecurity incidents. It is clear from looking at responsible individuals who are involved in connected cyberspace that they are unaware of the security procedures aimed at the system (ENISA, 2011b; S. de Vleeschhouwer, 2017).

Consequently, maritime transportation is an area with a high level of cybersecurity risk and a low level of cybersecurity awareness. This approach was also supported by the European Network and Information Security Agency, which outlined seven significant gaps in maritime cybersecurity: “Low awareness and focus, the complex structure of Maritime systems, absence of holistic management approach in a national and international context in the maritime field, inadequacies related to the security of cyberspace in maritime regulations, no holistic understanding of cybersecurity, lack of economic incentives and initiatives for work to increase the cybersecurity in the maritime sector, lack of incentives to motivate work” (ENISA, 2011b).

4.3. Cyber-attack incidents in the maritime domain

4.3.1. Year 2010:

Malware on the offshore rig: Malicious computer software overpowered a drilling rig while it was at sea after departing from its South Korean construction location to Brazil. The blowout preventer, a crucial piece of safety equipment, was controlled by computers that were corrupted by the malware because it had expanded so widely throughout the rig's systems[1]. This was one of several rigs that experienced similar issues after their construction. Even computers on offshore oil platforms that are not linked to the Internet and were not designed to communicate with the Web have been infected by malware. Users who engage with the computers while inadvertently transporting problematic files cause issues frequently. Links in malicious emails or malicious webpages can contain links that download those files onto a computer, where they can then attach to USB devices or propagate over a network. Source: (Shauk, 2013)

Hacking of a Greek shipping company: A Greek shipping company was the target of multiple successful piracy assaults in the Gulf of Aden over two years. This was because local pirates employed hackers to gain access to the company's headquarters and identify the ships that were the most susceptible to attack, as well as route itineraries. Hackers were able to access the information technology systems of the business by using the wireless equipment that had been installed in the company's buildings. (Kapalidis, 2020)

4.3.2. Year 2011:

IRISL: The servers of the Iranian Shipping Corporation IRISL (Islamic Republic of Iran Shipping Lines) were compromised as a result of a cyber-attack, resulting in the loss of data pertaining to rates, loading, dispatch, and location. Consequently, the location of numerous cargo containers remained unknown, and an undisclosed quantity of financial losses resulted. Sources: (Kapalidis, 2020; Torbati and Saul, 2012)

4.3.3. Year 2011-2013:

Port of Antwerp: A criminal organization utilized the port of Antwerp to transport large quantities of narcotics from South America disguised as bananas. To accomplish this, the organization employed a group of Belgian hackers who compromised the management systems of two

[1] According to Michael Van Gemert, who manages systems and controls for Lloyd's Register Drilling Integrity Services, an offshore inspection company that was informed about the incident, the rig encountered malware and had to be shut down for several days during its journey from Korea to Latin America in 2010.

terminals in the port. The infiltration allowed the criminal organization to locate every container prior to the arrival of the actual client to collect it. Sources: (Kapalidis, 2020; Nguyen, 2018; Walker and Spencer, n.d.)

Saudi Aramco, Oil and Gas Operator: During the month of Ramadan in 2012, the main Saudi Arabian state-owned oil and gas corporation, Saudi Aramco, which supplies 10% of the world's oil, suffered a cyberattack. A company employee opened a phishing mail containing an infected link. According to Aramco's vice president of corporate planning, Abdullah al-Saadan, the primary objective of this attack was to prevent the flow of oil and gas to both domestic and international markets. Due to this attack, the company failed to send or receive financial transfers or contracts, as well as process payments, compelling it to cease operations and close its internal corporate. Moreover, the negative effect resulting from the attack had a significant impact on the company's supply chain, particularly in maritime transportation. As a result, it became clear that cyberattacks could have far-reaching consequences beyond the immediate financial damage they cause. Sources: (Reuters, 2012)

Danish Maritime Authority: In 2012, the Danish Maritime Authority was targeted by malware encoded in a PDF file. Before being found in 2014, the virus had expanded throughout the Maritime Authority's network and into Danish government organizations. A large majority of cyberattacks are the result of human activity. Authorized users make poor password decisions, click on harmful links, open email files containing malevolent code, misplace their computers, tablets, and phones, and have their usernames and passwords collected by a growing number of phishing scammers. Source: (Linton, 2016)

4.3.4. Year 2015:

Mobile Offshore Drilling Unit (MODU): In 2015, the US Coast Guard reported a case in which offshore oil employees carried infected laptops and USB drives aboard a MODU. The accidentally transmitted malware disrupted computer networks by downloading adult and unlawful music files directly. The malware disabled the dynamic positioning and thruster signals, causing the MODU to drift away from the well site. As stated by Nguyen, (2018):

"This incident is another example of a non-existent 'cyberculture'. The incident highlights the disastrous effects that such an attack on an offshore critical infrastructure, or a ship, could have on the environment. A case that affected both the human factor and the infrastructure and illustrated the necessity for effective cyber training for maritime professionals, once again".

Sources: (Athens Group Services, 2019; Kapalidis, 2020; Nguyen, 2018)

4.3.5. Year 2016:

South Korean fishing boats: After GPS signals were disrupted, which also made it difficult to locate fishing nets at sea, hundreds of South Korean fishing vessels were forced to return in early 2016. South Korean authorities said this was due to the jamming of GPS signals. The occurrence has been attributed to North Korea, but there was no evidence to support this claim. Source: (Kim and Saul, 2016)

4.3.6. Year 2017:

Clarksons incident: Clarksons is one of the largest shipbrokers in the globe. According to the company's official press release, unauthorized access was attained through a solitary, isolated user account in November 2017. Following the stealing of sensitive information, the stock value decreased by 5% immediately. It demonstrates the significance of developing "cyberculture" for the most vital pillar of cyber resilience, the human element. It highlights the need for effective cybersecurity training for all maritime professionals. Companies should revise their access and administration rights by the "need-to-know" principle, limiting them to only the necessary personnel and closely monitoring them all. Sources: (Nguyen, 2018), (Kapalidis, 2020)

Maller Maersk: A significant maritime firm, A.P. Moller-Maersk, experienced a significant business interruption cyber incident in June 2017. The notPetya malware was brought to the company's terminal in Ukraine by a claimed state-drive assault. NotPetya caused global disruptions that persisted for weeks. According to the Chief Information Security Officer of Maersk, the event began with the infection of a single user's workstation and spread rapidly within seven minutes (Parizo, 2019; Progoulakis et al., 2021). As many as 76 of the company's port facilities around the world were affected by the virus, including important ones like Rotterdam, Los Angeles, Mumbai, and Auckland.

Sources: (Cimpanu, 2018b; Maritime Executive, 2020c; Mcquade, 2018; Nguyen, 2018)

Subcontractors of the US Navy: Hackers from China are suspected of obtaining information from companies that provide services to the United States Navy. In addition, it is believed that 27 Universities in the United States have been targeted in an operation to acquire research data associated with maritime technology. Sources: (Lubold and Volz, 2018; Volz, 2019).

4.3.7. Year 2018:

Port of Barcelona: The Port of Barcelona reports a cyberattack in 2018, which turned out to be a "Ryuk" ransomware infection. Only internal IT systems were harmed by the attack, not ship traffic. When ransomware got into a computer, it messed up the camera and access control systems and caused important process control tracking systems to stop working. A malicious email sent to a worker at the marine center was the point of entry. "Once an employee clicked on the malicious link in the email, the ransomware allowed a threat actor to access important enterprise IT network files and encrypt them, making it impossible for the facility to access important files," the agency said. Sources: (Cimpanu, 2019; Safety4sea, 2018)

Port of San Diego: Five days after the aforementioned occurrence in Barcelona, the Port of San Diego reports serious disruptions to its IT systems. This was another Ryuk ransomware infection, and its effects are limited to the port's local operations. It was subsequently disclosed that both incidents were caused by the same Ryuk ransomware. Sources: (Cimpanu, 2019; Safety4sea, 2018)

Gold Galleon: A monetarily driven Nigerian threat organization known as "Gold Galleon" is engaged in business email compromise (BEC) and business email spoofing (BES) scams. The Group stole at least $3.9 million US dollars from marine shipping companies and their clients between June 2017 and January 2018. BEC is a type of social engineering plan in which threat actors obtain entry to a company's email account. The attackers typically use spear phishing emails with malicious payloads attached to capture the email passwords of people in charge of business operations. Sources: (Secureworks, 2018)

COSCO: A cyberattack was launched against China Ocean Shipping Company, also known as COSCO, which resulted in significant disruptions in the network operations of their US office. For a period of five days, correspondence via email and the network telephone was disrupted. Emails sent within the company suggest that the incident was caused by an infestation with ransomware. Sources: (Cimpanu, 2019; Interpol, 2020)

SAIPEM attack: Saipem, an Italian subsea engineering and energy services company, disclosed that it had detected a hacking attempt on its Middle Eastern server systems. About 400 of Saipem's servers, predominantly those located in Middle Eastern nations, were affected by the attack, but not the company's primary servers in Europe, according to company officials. The suspected origin of the hacking endeavor is India. The company had backups of all the afflicted data, so no information was lost irreversibly. Saipem has found no evidence to suggest that any data was taken. Source: (The Maritime Executive, 2020)

GPS jamming: In northern Norway, there have been numerous reports of GPS interference throughout the course of 2018 and 2019. The disturbance has had some effect on maritime traffic, but fortunately, the situation could have been much worse had it not been prevented. Sources: (Meland et al., 2021; The Norwegian National Security Authority (NSM), 2020)

4.3.8. Year 2019:

Large ship en route to New York: In February 2019, a large ship that was sailing towards New York City reported a serious cyber-attack on its onboard network to the US Coast Guard. An incident-response team led by the Coast Guard found out that the ship's systems had been infected with malware, causing severe damage to their functionality. A warning was issued to commercial vessels urging them to improve their cybersecurity by splitting shipboard networks, enforcing per-user passwords and tasks, implementing fundamental security measures, and patching regularly. Source: (Lemos, 2019)

Undisclosed port in the USA: The Ryuk ransomware has attacked a port in the United States that has not been identified. Because of the infection, CCTV cameras, access control systems, and essential process monitoring were rendered inoperable. The infection was spread through an attachment in a phishing email. Source: (Cimpanu, 2019)

James Fisher & Sons (JFS): A maritime services provider JFS, located in the United Kingdom, has announced that it has become the target of a cyber-attack and has made the decision to temporarily disable its digital systems as a preventative measure. The irony of the situation is that the official revelation of the data compromise has caused a 7% drop in the price of the company's shares. Officials from the JFS have stated, under the condition of confidentiality, that the assault was a ransomware variation that prevented access to the files. Source: (Goud, 2019)

Undisclosed US pipeline operator: Due to being infected with Ryuk ransomware, a natural gas compression facility belonging to an unnamed US pipeline provider is forced to go offline for two days. Phishing emails were used in the assault, and both IT and operational technology systems were compromised as a result. Sources: (Buurma and Sebenius, 2020; Dragos, 2020)

A tanker in Finland: Ransomware compromises the administration computer of a tanker that is located in the vicinity of the harbor of Naantali in Finland. Additionally, the archival drive is formatted. It has been determined that the Remote Desktop Protocol (RDP), a USB device, or an email

attachment are all potential entry points for an attack. Four months later, in the vicinity of the same harbor, the same vessel becomes infested once more. Source:(Meland et al., 2021).

Hermes 2.1.: Two vessels belonging to the same proprietor have been infiltrated by the Hermes 2.1 ransomware. The intrusion was propagated through a Word document with macro capabilities embedded in an email, resulting in the compromise of multiple computers on the administrative networks. Source:(Meland et al., 2021).

4.3.9. Year 2020:

A vessel near Tynemouth: A maritime vessel anchored in the vicinity of Tynemouth, England, has been subject to a Ryuk ransomware attack, resulting in the encryption of its ship server and several client PCs. The IT service provider dispatched two specialists who determined that all data had been encrypted and irretrievably lost. A complete reinstallation was required to reinstate the systems. Source:(Meland et al., 2021).

Sodinokibi: Around the middle of the year 2020, the ransomware cyberattack known as Sodinokibi spreads throughout the administrative networks of three ships carrying the American flag. In addition to encrypting data, this malware also carries the risk of committing information theft (also known as "ransomtheft"). Source: (Meland et al., 2021).

MSC: MSC, a US-based gas pipeline operator and shipping company has experienced two separate malware incidents, with the latter forcing the closure of the shipowner's Geneva headquarters for five days. Sources: (Grinter, 2020; Maritime Executive, 2020c)

Shahid Rajaee port: The Iranian port of Shahid Rajaee, which is the newest of two major shipping ports in the city of Bandar Abbas on the Strait of Hormuz, suddenly stopped working for no apparent reason. All of the computers that control the flow of ships, trucks, and goods crashed at the same time. This caused huge delays on the rivers and roads that lead to the center. Israel is accused of breaching into the Iranian port of Shahid Rajaee, which stopped all shipping and goods for a long time. Sources: (Grinter, 2020; Warrick Joby and Nakashima, 2020).

Vard Group: Recently, the Norwegian shipbuilding company Vard Group AS encountered a ransomware attack at the Langsten shipyard. In light of the cyber-attack sustained by the servers at Langsten Shipyard, the company implemented all necessary measures for the resolution of the problem. It has been notified to numerous personnel that the interruptions could result in temporary unemployment because of suspended shipbuilding. Source: (Goud, 2020; Safety4sea, 2020b).

Carnival Corporation & plc: The cruise operator Carnival Corporation & plc has been subjected to two ransomware cyber-attacks between 2019 and 2020, likely resulting in the compromise of the personal data of customers and employees. Source: (Maritime Executive, 2020a).

Transport Malta: The Maltese transport authority experienced a debilitating malware cyber-attack resulting in the closure of its online systems for five days. Transport Malta implored its personnel to vigilantly observe their accounts for any potentially suspicious activity and to often modify their passwords, avoiding any passwords that can be easily ascertained or those that are identical for multiple accounts. Sources: (Agius, 2020; Azzopardi, 2020).

CMA CGM: The Ragnar Locker ransomware infects the computer systems of the French container transport business CMA CGM. A number of its branches in China were impacted, and the company was forced to temporarily disable a number of its internet services, including its scheduling system. Source: (Coble, 2020; Shen and Baker, 2020)

Red Funnel: British ferry company Red Funnel has been impacted by a malicious cyber-attack, resulting in a major disruption in its IT structures. Due to the unavailability of the reservation systems for some time, customers were necessitated to arrive earlier than the sailings to purchase tickets in person. Sources: (BBC News, 2020; Toogood, 2020).

Port of Kennewick: The Port of Kennewick in Washington State, USA has experienced a crippling ransomware cyber-attack on its IT systems. The hackers requested a ransom of two hundred thousand U.S. dollars, which was not received. The provenance of the attack is obscure; however, the authorities believe that it may have been initiated by a spurious email sent to a port staff member. The systems had to be reconstituted from offline backups, resulting in an extended period of unavailability. Source: (Maritime Executive, 2020d).

Hurtigruten: The Norwegian cruise operator Hurtigruten has experienced a detrimental ransomware cyber-attack, greatly compromising its IT structure. The company's public reports indicate that the probability that attackers had accessed larger amounts of guest data is minimal; however, Hurtigruten is not ruling out the possibility that some employee information might have been infiltrated. Sources: (Bøe and Jordheim, 2020; Maritime Executive, 2020b; Safety4sea, 2020a)

AIDA: The Doppel Paymer ransomware attack has affected the headquarters of the German travel provider AIDA, which is located in Rostock. Because of the severe IT problems caused by the assault, AIDA was forced to postpone several cruises. Source: (Walker, 2020).

4.3.10. Year 2021:

K-Line: In March 2021, the Japanese shipping company, 'K' Line, suffered a cyber-attack resulting in disruption to some of its enterprise systems. The company hypothesized that the deficit was a result of a malware infection initiated by its foreign affiliate. Due to the attack, it was necessary to suspend the operations of the enterprise systems and their external connections. Source: (Safety4sea, 2021b)

Cape Town and Durban: There has been a cyber-attack resulting in disruption to container operations at the ports of Cape Town and Durban in South Africa. A surge of cyber incidents has caused significant disruption to the operations of major ports in South Africa. The mining companies experienced significant losses due to the blackouts that occurred in Durban and Cape Town. Sources: (Le journal 2L'Afrique, 2021; Schenkelberg, 2021)

CMA CGM: The French shipping company CMA CGM has encountered its second cyber incident within less than one year. The company disclosed to its clientele that it has been subjected to another cyber assault. Approximately one ear prior, the French company experienced a ransomware cyber-attack of a similar nature. Sources: (Port Technology International, 2021; Safety4sea, 2021a)

4.3.11. Year 2022:

BlackCat: Several major oil terminals situated in a few of Western Europe's largest ports have been subject to a cyberattack. The Amsterdam-Rotterdam-Antwerp oil trading hub, which is a cross-border Dutch and Belgian entity, appears to be one of the prime casualties resulting from the attack, with corporate IT systems being adversely affected. The initial report by the German security services determined that the BlackCat ransomware was the malware utilized in the cyberattack in Germany. Sources: (RTE, 2022; Safety4sea, 2022b)

Port of Lisbon: In December of 2022, the Port of Lisbon underwent a cyber-attack, resulting in the shutdown of the port's website and internal computer networks. Cyber analysts additionally noted that the attack was perpetrated through a pervasive malware program labeled LockBit. The perpetrators disseminated statements via the 'darknet'. Sources: (Safety4sea, 2022a; The Portugal News/Lusa, 2022)

5. RESULTS

By the criteria outlined in the methodology section, an analysis of cyber-attacks targeting the maritime industry between 2010 and 2022 revealed that 30 out of a total of 40 attacks were related to the vulnerability of cyber security awareness. The disclosure indicates that among the 30 instances of attack, the vulnerability was exploited by hackers via social engineering in 12 cases through malware, 15 cases through ransomware, and 3 cases through phishing techniques which is depicted in Figure 2.

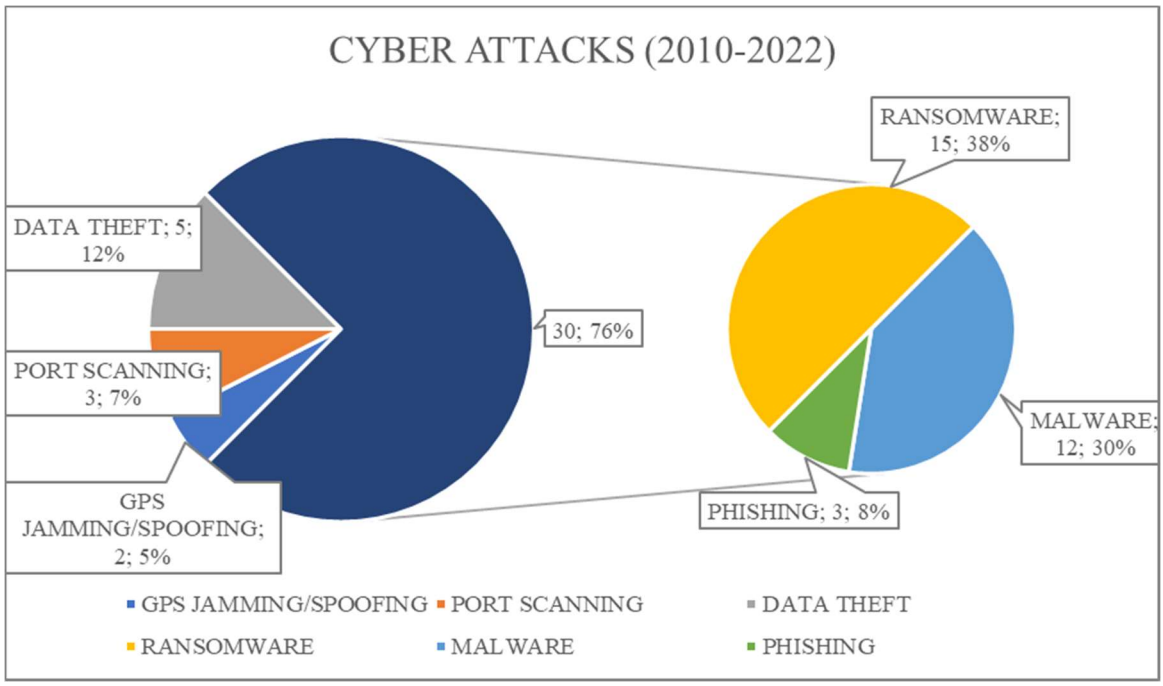

Fig. 2. Type-by-percentage analysis of cyber-attacks on the maritime industry between 2010 and 2022

Upon evaluating incidents about cybersecurity within the maritime industry, it has been observed that the absence of awareness and inadequate proficiency in cultivating secure conduct are significant contributors to the incidence of cybersecurity breaches. The observation of individuals who are engaged in cyber activities reveals that they lack awareness of the protective measures implemented to safeguard the system.

According to reports, there has been an increase in the occurrence of ransomware and other types of cyberattacks in 2020, with the maritime sector being among the recent targets of cybercriminals. Based on Naval Dome, a cybersecurity expert, there was a rise of 400% in attempted cyberattacks on the maritime sector between February 2020 and December 2020. This increase in attacks coincides with the industry's heightened reliance on technology and remote work arrangements, which were adopted as a response to the COVID-19 pandemic. The rise in phishing attempts, malware, and ransomware attacks can be linked to the alterations in operations and procedures resulting from travel restrictions and operational obstacles experienced during the pandemic. (Hellenic Shipping News Worldwide, 2020)

Another study that reveals the cyber security vulnerabilities of employees is Bolat and Kayişoğlu (2019) *"Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector"*. As an output of their study:

- Education plays a significant role in enhancing cybersecurity awareness among maritime employees, positively impacting their behavior concerning cybersecurity.
- Personal experiences with cybersecurity incidents have a noteworthy influence on employee cybersecurity awareness and their subsequent behavior in this domain.
- Maritime cybersecurity awareness has a substantial impact on promoting secure user behavior among employees.

Furthermore, the study reveals that rules and policies related to information sharing do not significantly affect cybersecurity awareness or the development of secure employee behavior. (Bolat and Kayişoğlu, 2019)

Thus, it can be concluded that the maritime transportation industry poses a significant level of risk about cybersecurity, while simultaneously exhibiting a low level of awareness in this domain. The aforementioned assertion was corroborated by the European Network and Information Security Agency, which identified seven significant inadequacies of cybersecurity in the maritime sector, as outlined in reference (ENISA, 2011a).

- "Low awareness and focus.
- Complex structure of Maritime systems.
- Absence of holistic management approach in national and international contexts in the maritime field.
- Inadequacies related to the security of cyberspace in maritime regulations.
- No holistic understanding of cybersecurity.
- Lack of economic incentives and initiatives for work to increase cybersecurity in the maritime sector.
- Lack of incentives to motivate work."

6. CONCLUSION

Technological developments and Industry 4.0 have made rapid and effective decision-making processes and cost-effective operations possible in the maritime sector. Blockchain, smart ports, autonomous ships, IoT-based real-time monitoring, digital twins, and similar technologies are innovations that the cyber world has brought to the maritime industry. Nevertheless, the technological advancements in the maritime industry have certain unfavorable implications. The emergence of innovations in technology has resulted in susceptibility to cyber-attacks in the maritime industry, thereby creating opportunities for both criminal actors and commercial stakeholders.

Regardless of the different subfields, the common finding of all studies related to cybersecurity is that employees' cybersecurity awareness levels are very low, and significant and selfless efforts are required to improve the situation. Moreover, it is known that the ongoing malicious activities in the sector do not represent the true amount of publicly reported incidents, and there is a significant difference between reported incidents and actual rates. This study highlights the role of human cybersecurity awareness in successful cyber-attacks in the maritime sector. When analyzing attacks carried out since 2010, it was found that 76% were carried out through social engineering methods such as phishing, malware, and ransomware. The individuals targeting stakeholders in the maritime industry are cognizant of the fact that employees within the industry lack adequate cybersecurity awareness and a comprehensive grasp of cybersecurity principles. While certain initiatives like the *"Manual on the International Law Applicable to Cyber Warfare"* also known as the *"Tallinn Manual"*[2] have emerged from an expert-driven process to create a non-

[2] The Tallinn Manual, initially named the Tallinn Manual on the International Law Applicable to Cyber Warfare, serves as an academic exploration into the application of international law in the context of cyber conflicts and warfare. Produced between 2009 and 2012, the manual was authored by an international assembly of roughly twenty experts at the request of the NATO Cooperative Cyber Defence Centre of Excellence located in Tallinn. (Schmitt, 2017)

binding document that applies existing laws to cyber warfare, the intricate nature of these systems makes it challenging to establish a permanent and universally applicable solution. This thesis is supported by the fact that three out of every four cyber-attacks managed within the scope of the criteria in the methodology section are due to a lack of cyber security awareness.

To prevent situational awareness vulnerabilities in humans, the role of human behavior in cybersecurity structures should be taken more into account. Within the scope of Industry 5.0, which offers a new perspective, especially towards the use of technology for the benefit of society and aims to eliminate the disadvantages created by Industry 4.0, it is considered necessary to move the human factor from an operational position to a supervision and decision-making authority position, to minimize human-caused cybersecurity vulnerabilities in execution.

As highlighted in this study, the success of cyberattacks on the maritime industry is directly proportional to the vulnerability in employees' cybersecurity awareness. Therefore, future studies should concentrate on measures to eliminate this vulnerability, aiming for more rapid, secure, and efficient utilization of the benefits brought about by technology. Prioritizing awareness-enhancing training over physical measures in these efforts and presenting alternatives for achieving this goal will lead to productive outcomes based on the results obtained in this study.

REFERENCES

Agius, M. (2020). *TM mum on whether cyber-attack affected ship, air registries - Newsbook*. https://newsbook.com.mt/en/tm-mum-on-whether-cyber-attack-affected-ship-air-registries/

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, *45*, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

Algarni, A., Xu, Y., Taizan Chan, & Yu-Chu Tian. (2013). Social engineering in social networking sites: Affect-based model. *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 508–515. https://doi.org/10.1109/ICITST.2013.6750253

Athens Group Services. (2019). *Cybersecurity – There Is No Silver Bullet*. https://athensgroupservices.com/cybersecurity-there-is-no-silver-bullet/

Azzopardi, K. (2020). *Investigation into Transport Malta cyber-attack has not yet determined whether hack led to data leakage*. https://www.maltatoday.com.mt/news/national/105593/watch_transport_malta_cyber_attack_investigation_has_not_yet_determined_whether_data_was_stolen#.ZBW3OhTP25c

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *Cornell University, Computer Science, Cryptography and Security*. https://doi.org/https://doi.org/10.48550/arXiv.1901.02672

BBC News. (2020). *Red Funnel ferry firm's IT system hit by "malicious attack."* https://www.bbc.com/news/uk-england-hampshire-54368110

Bolat, P. & Kayişoğlu, G. (2019). Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector. Journal of ETA Maritime Science, 7(4), 344-360.

Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information*, *13*(1), 22. https://doi.org/10.3390/info13010022

Bøe, E., & Jordheim, H. (2020). *Police investigate the computer attack against Hurtigruten – E24*. https://e24.no/hav-og-sjoemat/i/7KPeEK/politiet-etterforsker-dataangrepet-mot-hurtigruten

Borazjani, P. N. (2017). *Security Issues in Cloud Computing* (pp. 800–811). https://doi.org/10.1007/978-3-319-57186-7_58

Buurma, C., & Sebenius, A. (2020). *Ransomware Shuts U.S. Natural Gas Compressor Facility for Two Days*. https://www.carriermanagement.com/news/2020/02/20/203485.htm

Čekerevac, Z., Dvorak, Z., Prigoda, L., & Čekerevac, P. (2017). Man-In-The-Middle Attacks and Internet Of Things. *FBIM Transactions*, *5*(2). https://doi.org/10.12709/fbim.05.05.02.03

Cimpanu, C. (2018a). *Ransomware Infection Cripples Shipping Giant COSCO's American Network*. https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/

Cimpanu, C. (2018b). *Ransomware Infection Cripples Shipping Giant COSCO's American Network*. https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/

Cimpanu, C. (2019). *US Coast Guard discloses Ryuk ransomware infection at maritime facility | ZDNET*. https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/

CISA-US. (2020). *Avoiding Social Engineering and Phishing Attacks | CISA*. https://www.cisa.gov/uscert/ncas/tips/ST04-014

Clark, J. (2018). Cybercrime in the shipping industry. *A Presentation by Shipping Hill Dickinson LLP*.

Coble, S. (2020). *Ransomware Attack on Shipping Giant*. https://www.infosecurity-magazine.com/news/ransomware-attack-on-shipping-giant.

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry, 114, 103165. https://doi.org/10.1016/j.compind.2019.103165

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *49*(3), 229–233. https://doi.org/10.1177/154193120504900304

Dragos. (2020). *Assessment of Ransomware Event at U.S. Pipeline Operator*. https://www.dragos.com/blog/industry-news/assessment-of-ransomware-event-at-u-s-pipeline-operator/

ENISA. (2011a). *Analysıs of Cybersecurity Aspects in The Marıtıme Sector*.

ENISA. (2011b). *Cyber Security Aspects in the Maritime Sector*. https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

Fitton, M. O., Prince, D., & Lacy, M. (2015). *The Future of Maritime Cyber Security*. https://eprints.lancs.ac.uk/id/eprint/72696/

Futurenautics Maritime-KVH and Intelsat. (2018). *Crew Connectivity 2018 Survey Report Maritime*. http://www.navarino.co.uk/wp-content/uploads/2018/04/Crew_Connectivity_2018_Survey_Report.pdf

Goud, N. (2019). *Cyber Attack on James Fisher and Sons - Cybersecurity Insiders*. https://www.cybersecurity-insiders.com/cyber-attack-on-james-fisher-and-sons/

Goud, N. (2020). *Ransomware attack on Norwegian Ship yard results in job loss to many - Cybersecurity Insiders*. https://www.cybersecurity-insiders.com/ransomware-attack-on-norwegian-ship-yard-results-in-job-loss-to-many/

Grinter, M. (2020). *Maritime cyber-attacks up 900% in three years - Hong Kong Maritime Hub*. http://www.hongkongmaritimehub.com/maritime-cyber-attacks-up-900-in-three-years/

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629–3654. https://doi.org/10.1007/s00521-016-2275-y

Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R., & Helkala, K. (2018). Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*, *71*(5), 1025–1039. https://doi.org/10.1017/S0373463318000164

Hellenic Shipping News Worldwide. (2020). *Greater Cyber Security Needed For Coronavirus And Economic Crises*. https://www.hellenicshippingnews.com/greater-cyber-security-needed-for-coronavirus-and-economic-crises/

Hindy, H., Tachtatzis, C., Atkinson, R., Bayne, E., & Bellekens, X. (2021). Developing a Siamese Network for Intrusion Detection Systems. *Proceedings of the 1st Workshop on Machine Learning and Systems*, 120–126. https://doi.org/10.1145/3437984.3458842

IMO. (2017). *Guidelines on Maritime Cyber Risk Management.* https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

Interpol. (2020). *Cyber Crime: COVID-19 Impact*. https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf?inLanguage=eng-GB

Jensen, L. (2015). Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*, *5*(4), 35–39. https://doi.org/10.22215/timreview/889

Kapalidis, P. (2020). Cybersecurity at Sea. In L. Otto (Ed.), *Global Challenges in Maritime Security. Advanced Sciences and Technologies for Security Applications.* (pp. 127–143). https://doi.org/10.1007/978-3-030-34630-0_8

Kessler, G. C., & Uk, A. (n.d.). *Cybersecurity in the Maritime Domain Cybersecurity in the Maritime Domain CORE View metadata, citation and similar papers at core*. Retrieved March 21, 2023, from https://commons.erau.edu/publication/1318

Kim, J., & Saul, J. (2016). *South Korea Revives GPS Backup Project After Blaming North for Jamming*. https://gcaptain.com/south-korea-revives-gps-backup-project-after-blaming-north-for-jamming/

Kokar, M. M., & Endsley, M. R. (2012). Situation Awareness and Cognitive Modeling. *IEEE Intelligent Systems*, *27*(3), 91–96. https://doi.org/10.1109/MIS.2012.61

Lam, J. S. L., & Bai, X. (2016). A quality function deployment approach to improve maritime supply chain resilience. *Transportation Research Part E: Logistics and Transportation Review*, *92*, 16–27. https://doi.org/10.1016/j.tre.2016.01.012

Larsen, M. H., & Lund, M. S. (2021). Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. *IEEE Access*, *9*, 144895–144905. https://doi.org/10.1109/ACCESS.2021.3122433

Le journal 2L'Afrique. (2021). *Cyber attacks cripple South African ports*. https://lejournaldelafrique.com/en/cyber-attacks-paralyze-South-African-ports/

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lemos, R. (2019). *Coast Guard Warns Shipping Firms of Maritime Cyberattacks*. https://www.darkreading.com/vulnerabilities-threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks

Linton, A. (2016). *Port Authority Role in Cyber-Security -LinkedIn*. https://www.linkedin.com/pulse/port-authority-role-cyber-security-art-linton/

Lubold, G., & Volz, D. (2018). *Chinese Hackers Breach U.S. Navy Contractors - WSJ*. https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401

Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010). Cognitive Task Analysis for Cyber Situational Awareness. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *54*(4), 279–283. https://doi.org/10.1177/154193121005400403

Mallik, A., Ahsan, A., Shahadat, M. Md. Z., & Tsou, J.-C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, 77–92. https://doi.org/10.5267/j.ijdns.2019.1.001

Maritime Executive. (2020a). *Carnival Corporation Reports Ransomware Attack Accessed Data*. https://www.maritime-executive.com/article/carnival-corporation-reports-ransomware-attack-accessed-data

Maritime Executive. (2020b). *Hurtigruten Reports Passenger Data Exposed in Cyberattack*. https://www.maritime-executive.com/article/hurtigruten-reports-passenger-data-exposed-in-cyberattack

Maritime Executive. (2020c). *Naval Dome: Cyberattacks on OT Systems on the Rise*. https://www.maritime-executive.com/article/naval-dome-cyberattacks-on-ot-systems-on-the-rise

Maritime Executive. (2020d). *Ransomware Cripples IT Systems of Inland Port in Washington State*. https://www.maritime-executive.com/article/ransomware-attack-cripples-systems-of-inland-port-in-washington-state

McNeese, M., Cooke, N. J., D'Amico, A., Endsley, M. R., Gonzalez, C., Roth, E., & Salas, E. (2012). Perspectives on the Role of Cognition in Cyber Security. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *56*(1), 268–271. https://doi.org/10.1177/1071181312561063

Mcquade, M. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Meland, P. Há., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(3), 519–530. https://doi.org/10.12716/1001.15.03.04

Mraković, I., & Vojinović, R. (2019a). Maritime Cyber Security Analysis – How to Reduce Threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Mraković, I., & Vojinović, R. (2019b). Maritime Cyber Security Analysis – How to Reduce Threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Mraković, I., & Vojinović, R. (2019c). Maritime Cyber Security Analysis – How to Reduce Threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Nguyen, L. (2018, February). *e-paper: Collaboration in the Shipping Industry: Innovation and Technology.* KNect365. https://informaconnect.com/epaper-collaboration-in-the-shipping-industry-innovation-and-technology/

NSI, N. S. I. (2017). *A Brief User's Guide to Getting the Most from Your Employee Security Connection Subscription*. https://www.nsi.org/pdf/ESC_User's_Guide.pdf

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, *37*. https://doi.org/10.17705/1CAIS.03743

Parizo, E. (2019). *Maersk CISO Says NotPeyta Devastated Several Unnamed US firms*. https://www.darkreading.com/omdia/maersk-ciso-says-notpeyta-devastated-several-unnamed-us-firms

Perez, G. F. (2019). *Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry* [Nova Southeastern University]. https://nsuworks.nova.edu/gscis_etd

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Port Technology International. (2021). *CMA CGM faces cyber attack leading to data leak - Port Technology International*. https://www.porttechnology.org/news/cma-cgm-faces-cyber-attack-leading-to-data-leak/

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. *Journal of Marine Science and Engineering*, *9*(12), 1384. https://doi.org/10.3390/jmse9121384

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-Risk Management*. Springer International Publishing. https://doi.org/10.1007/978-3-319-23570-7

Reuters. (2012). *Saudi Arabia says cyber attack aimed to disrupt oil, gas flow | Reuters*. https://www.reuters.com/article/saudi-attack/saudi-arabia-says-cyber-attack-aimed-to-disrupt-oil-gas-flow-idUSL5E8N91UE20121209

RTE. (2022). *European oil port terminals hit by cyberattack*. https://www.rte.ie/news/world/2022/0203/1277569-oil-terminal-cyberattack/

S. de Vleeschhouwer. (2017). *Safety of data. The risks of cyber security in the maritime sector*. https://maritimetechnology.nl/media/NMT_Safety-of-data-The-risks-of-cyber-security-in-the-maritime-sector.pdf

Safety4sea. (2018). *2018 Highlights: Major cyber-attacks reported in maritime industry*. https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/

Safety4sea. (2020a). *Hurtigruten hit by cyber-attack*. https://safety4sea.com/hurtigruten-hit-by-cyber-attack/

Safety4sea. (2020b). *Vard shipbuilder experiences ransomware attack - SAFETY4SEA*. https://safety4sea.com/vard-shipbuilder-experiences-ransomware-attack/

Safety4sea. (2021a). *CMA CGM face to face with another cyber-attack - SAFETY4SEA*. https://safety4sea.com/cma-cgm-face-to-face-with-another-cyber-attack/

Safety4sea. (2021b). *K Line issues apology after yet another cyber-attack*. https://safety4sea.com/k-line-issues-apology-after-yet-another-cyber-attack/

Safety4sea. (2022a). *Cyber attack hits Port of Lisbon*. https://safety4sea.com/cyber-attack-hits-port-of-lisbon/

Safety4sea. (2022b). *Cyber attacks hit European oil terminals - SAFETY4SEA*. https://safety4sea.com/cyber-attacks-hit-european-oil-terminals/

Schenkelberg, B. (2021). *S. Africa Cyber-Attack, Durban & Richards Bay Terminals - X-Industry - Red Sky Alliance*. https://redskyalliance.org/xindustry/s-africa-cyber-attack-durban-richards-bay-terminals

Schmitt, M. (2017). Introduction. In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (pp. 1-8). Cambridge: Cambridge University Press. doi:10.1017/9781316822524.006

Secureworks. (2018). *Gold Galleon: How a Nigerian Cyber Crew Plunders the Shipping Industry*. https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry

Shauk, Z. (2013, April 28). *Malware on the offshore rig: Danger lurks where the chips fail*. https://www.houstonchronicle.com/business/energy/article/Malware-on-the-offshore-rig-Danger-lurks-where-4470723.php

Shen, C., & Baker, J. (2020). *CMA CGM confirms ransomware attack*. https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack

Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, Port*18*(1), 129–163. https://doi.org/10.1007/s13437-019-00162-2

The Maritime Executive. (2018). *Saipem's Servers Hit by Cyberattack*. https://maritime-executive.com/article/saipem-s-servers-hit-by-cyberattack

The Norwegian National Security Authority (NSM). (2020). *RISIKO 2020*. https://www.digi.no/filer/NSM_Risiko_2020_a_pen.pdf

The Portugal News/Lusa. (2022). *Cyberattack at Lisbon port - The Portugal News*. https://www.theportugalnews.com/news/2022-12-26/cyberattack-at-lisbon-port/73281

Toogood, D. (2020). *Red Funnel Suffers "Malicious Attack" on IT Systems Causing Major Disruption*. https://www.islandecho.co.uk/red-funnel-suffers-malicious-attack-on-it-systems-causing-major-disruption/

Torbati, Y., & Saul, J. (2012, October). *Iran's top cargo shipping line says sanctions damage mounting | Reuters*. https://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022

Volz, D. (2019). *Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets - WSJ*. https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800

Walker, J. (2020). *AIDA Cruise Ships Under Cyber Attack - Are Costa Ships Also Affected? | Cruise Law News*.https://www.cruiselawnews.com/2020/12/articles/cyber-attacks/aida-cruise-ships-under-cyber-attack-are-costa-ships-also-affected/

Walker, J., & Spencer, J. (n.d.). *Cyber Marine: Risks & Loss Scenarios*. International Marine Claims Conference. Retrieved March 8, 2023, from http://www.marineclaimsconference.com/imcc-docs/docs/Cyber%20workshop.pdf

Warrick Joby, & Nakashima, E. (2020). *Officials: Israel linked to a disruptive cyberattack on Iranian port facility - The Washington Post*. https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE '14*, 1–10. https://doi.org/10.1145/2601248.2601268