University of Piraeus

School of Information and Communication Technologies

Department of Digital Systems

Postgraduate Program of Studies

MSc Digital Systems Security

Master Thesis

Protect the Ship

Paraskevas Pallas

Supervisor Professor: Prof. Christos Xenakis

Piraeus

1/6/2022

1 Abstract

This thesis' scope is the detailed study of the latest BIMCO guidelines regarding ship protection against cyber-attacks (*The guidelines on cyber security onboard ships, v.4*). We will examine it thoroughly and mine and highlight the key aspects that will bring the required actions and most appropriate countermeasures for the maritime industry, considering the challenges associated especially with their ships.

One of our main goals will be to identify the readiness level in the maritime industry; in other words, how prepared is the maritime sector to absorb these guidelines efficiently by applying appropriate countermeasures.

Finally, we will focus on academic bibliography and solutions implemented by cybersecurity companies that help maritime organizations adopt the BIMCO's guidelines. Our conclusions will gather the best and most viable practices in the field that will guarantee a safer, less uncertain, and more solid environment for the world's leader in commercial transfers from human history's origins, the maritime sector.

SUBJECT AREA: Guidelines on cybersecurity onboard ships

KEYWORDS: BIMCO, maritime, cybersecurity

2 Acknowledgments

As I wrap up my thesis, I catch myself retracing the first moments after being assigned this subject by my supervisor, Professor Christos Xenakis. I have always been fond of sayings and gnomes. I find them stimulating and inspiring, boosting my performance and targeting excellence.

Writing the last lines of my thesis, I am staring at a frame on my office's wall saying in bold letters:

"As you set out for Ithaka

hope your road is a long one,

full of adventure, full of discovery.…"

a representative part of *Ithaca* written by C. P. Cavafy[1], the famous Greek and influential poet, who lived in Egypt most of his life.

The current paper was not the first big project I worked. Running the fifth decade of my life, I have faced quite a few challenges, including academic papers and action in the field.

Not being a professional in cybersecurity, the first few weeks of this MSc were filled with stress and uncertainty. The experienced professors made this pressured period turn into an exciting journey in knowledge and made me a better person overall. Luckily, I had the chance to meet and cooperate with a few very detail-oriented and competent colleagues from several sectors, and their interference was invaluable. Unfortunately, due to the Covid-19's constraints, we never had the chance to meet face to face.

We ended our online courses in July 2021, and each of us was assigned their thesis. During this long and exhaustive journey, I encountered obstacles and frustrations that challenged my will and desire to continue my effort and commitment to my course.

Professor Christos Xenakis supported and guided me decisively and passed a portion of his experience on this thesis through his tutoring. I owe him gratitude for having the chance to attend such a demanding curriculum. *Digital Systems Security* is one of the

[1] Ithaka, https://www.poetryfoundation.org/poems/51296/ithaka-56d22eef917ec, Accessed on 9 May 2022

best MSc that one can find in the European region, and I am proud to reach its completion. I wish to thank S. Margaritis and K. Syntila for their honest and direct response to my requests regarding cybersecurity matters in the maritime sector and future trends. They reflected their experience and knowledge in critical sections of this paper.

I devote this thesis to my family, lovely wife, and children, who have always been by my side to support me and push me to overcome hard times and obstacles that seemed a lot higher at first sight.

"…Keep Ithaka always in your mind.

Arriving there is what you're destined for.

But don't hurry the journey at all.

Better if it lasts for years…"

3 Table of Content

4 Introduction

4.1 Target

Undoubtedly, the shipping industry's role in the global supply chain and the economy is vital and multifactor. The most significant civilizations have used trade to exchange goods and share their achievements with their neighbors, and the sea has always been the primary means of transportation. Nowadays, countries worldwide share multifaceted interests and dependencies with companies based in several places on the globe. This unforeseen complexity in the world's economy has given the maritime sector an even more strategic and crucial importance.

At the same time, malicious activities in the cybersecurity field are rising worldwide in all sectors, and the maritime industry is among the ones that see the related attacks rise dramatically. More importantly, the dependence level on technologies based on the Internet is expected to rise too in the next few years as the 5G networks will be integrated into daily activities. Major maritime organizations like IMO and BIMCO take initiatives to mitigate the rising cyber threats to address these challenges.

Although the shipping industry's top management is aware and concerned about the disturbingly high cyber risk, they seem hesitant or unwilling to take the appropriate measures to strengthen their ships. Maritime companies have not taken the required countermeasures to defend against existing cyberattacks. Risk assessment is not fully implemented, and when it is, it seems to be insufficient. Simultaneously, future challenges are expected to widen this gap, leaving significant security holes affecting the supply chain worldwide if cyber criminals exploit them.

4.2 Background

IMO guidelines suggest that "*effective cyber risk management should start at the senior management level*" (IMO, 2017). This simple, still required principle is essential in building and sustaining a cybersecurity culture throughout all the company's assets, including offshore buildings, ships, and their people. Recently, other major organizations, like the National Institute of Standards and Technology (NIST)[2], the

[2] NIST, https://www.nist.gov/, Accessed on 8 May 2022

International Organization for Standardization (ISO/IEC 27001), and the British Standards Institution (BS 7799-2) (Zarrzuelo, 2021), have published standards to address cybersecurity concerns and feasible guidelines to achieve the highest protection in ports and ships. ENISA[3] also issued guidelines for cybersecurity in the maritime sector (ENISA, 2022).

All levels of management shall be committed to the same goal and follow high-level command's requirements in closing all the feasible security holes to make BIMCO *Guidelines* take effect. Humans are said to be the weakest link in the security chain (Hadnagy, 2011), (Schneier, 2011), (Bosworth, 2014). Therefore, it is not a surprise that IMO, BIMCO, ISO 27005, and NIST paid advanced attention to senior management's proven commitment to propagating the cybersecurity principles throughout the last employee. We will examine in the following chapters actual incidents where a simple employee opened a security hole and made a security breach possible.

Baltic and International Maritime Council (BIMCO)[4] is a non-profit organization and the world's most prominent shipping association having around 1,900 members in more than 120 countries. It published the 4th version of "*The guidelines on Cyber Security Onboard Ships"* (BIMCO, 2020).

Although the first guidelines were published more than six years ago (February 2016), not all companies have taken the required measures to contain cyber threats. Dimakopoulou et al. conducted insightful quantitative research in 2019 by answering questionnaires from executives working in major Greek shipping companies (A.Dimakopoulou, N.Nikitakos, I. Dagkinis, Th. Lilas, D.Papachristos, M.Papoutsidakis, 2019). The research focused on how aware the Greek shipping companies of the relative cybersecurity regulations and guidelines were and, consequently, how willing they were to confront them. Interestingly, only about half of the questioned executives participated in the research (39 responses out of 89

[3] The European Union Agency for Cybersecurity (ENISA) contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow, https://www.enisa.europa.eu/, Accessed on 8 May 2022
[4] BIMCO, https://www.bimco.org/, Accessed on 7 May 2022

questionnaires), showing a skepticism in sharing corporate secrets, although the research was conducted secretly.

Their work showed that the companies' heads are genuinely concerned about applying a secure cybersecurity framework (bulkers, tankers, containers, and gas carriers). They must invest in training their people and strengthening their offshore and onboard systems to achieve this. They were aware of the regulations and guidelines in their sector (IMO, BIMCO, ISO 27001, GDPR, TMSA3), and the majority (92%) applied a documented Cybersecurity Policy in their organization based on them. In the same context, once the Security Policy was established (with the help of consulting companies), the ship owners communicated this to all employees and applied it to the systems onboard vessels and on offshore premises. From 2017 to 2019, about 40% of the companies suffered a cyber-attack in their designs, highlighting the severity of the cyber threat.

On the other hand, the research demonstrated a significant gap between the willingness to adopt the guidelines and the present status of their fleet. When it came to the measures taken, the study showed plenty of room to cover to strengthen their ships. Two out of three companies ensured their firewalls were being up-to-date regularly. Similarly, only 72% carried out a detailed risk assessment and risk management, while one out of two (50%) conducted penetration tests against their network to reveal possible entry points.

Research conducted in June 2020 showed that most people working in the Greek maritime sector believed that the human factor plays a crucial role in defending against cyber-attacks (Pseytelis, 2021). Secondly, cybersecurity awareness and measures were low, although the participants identified their importance to their organization. Lastly, the participants were willing to follow global maritime organizations' guidelines and best practices like IMO and BIMCO.

Androjna, et al. highlight that shipping companies are partially prepared against (the rising number of) cyber-attacks on obsolete or modern digital systems (A. Androjna, T. Brcko, I. Pavic, H. Greidanus, 2020).

5 Cybersecurity

According to Cybersecurity & Infrastructure Security Agency (CISA), cybersecurity is *the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information*[5]. The International Telecommunication Union (ITU) defines it as *the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets*[6].

Figure 1: ENISA Threat Landscape 2021 – Prime threats

ENISA, being among the most reputable cybersecurity organizations, mentions that managed service providers are considered high-value targets for cyber criminals (ENISA THREAT LANDSCAPE 2021, 2021). Monetization is an increasing motivation

[5] What is Cybersecurity?, https://www.cisa.gov/uscert/ncas/tips/ST04-001, Accessed on 8 May 2022
[6] Definition of cybersecurity, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets., Accessed on 8 May 2022

(i.e., ransomware), while the attacks against critical infrastructures escalate rapidly. The most common ransomware infection actors are phishing emails and brute-forcing on Remote Desktop Services (RDS). Cyber criminals take advantage of people's concerns and target their phishing emails accordingly. Thus, it makes sense that most of the recent phishing attacks refer to the Covid-19 pandemic matters.

Kaspersky highlights the rising dangers behind the Internet of Things' (IoT) expansion, the rise in ransomware, the increase in cloud services and related security matters, and the continued integration of Artificial Intelligence (AI) even from the attackers' side[7]. Similarly, CISCO's predictions for the immediate future focus on increasing the risk for the supply chain and third-party attacks[8]. Palo Alto argues that the expanding cryptocurrency market will fuel ransomware attacks. Also, the pandemic sped up the transition to a borderless workforce, and we will need to apply borderless solutions to meet the new working relationships[9].

6 Maritime Industry

6.1 Global Economy

Humans have managed to fly and make intercontinental journeys a daily routine during the last decades. Similarly, on land, they have invented high-speed trains operating at several hundreds of miles per hour (one of them having a speed record of 373 mph)[10]. At the same time, a growing interest in autonomous tracks transferring goods on land without the presence of a human driver seems to be a science-fiction scenario less and less each day. The 5G networks broaden the communication channels and allow synchronous monitoring and control of such heavy tracks.

[7] Top ten Cybersecurity Trends, https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends, Accessed on 8 May 2022
[8] Cisco reveals top cybersecurity trends of 2021, What to watch in 2022, https://www.msspalert.com/cybersecurity-research/cisco-reveals-top-cybersecurity-trends/, Accessed on 8 May 2022
[9] 5 Cybersecurity predictions for an eventful 2022: Palo Alto Networks, https://www.expresscomputer.in/news/5-cybersecurity-predictions-for-an-eventful-2022-palo-alto-networks/82088/, Accessed on 8 May 2022
[10] Visualizing the Fastest Trains in the World, https://www.visualcapitalist.com/visualizing-the-fastest-trains-in-the-world/, Accessed on 8 May 2022

These traditional means of transportation share the competitive advantages of speed and immediacy compared to their competitors at sea. However, when the goal becomes the highest volume of goods possible, the sea carriers are the most efficient and cost-effective solution.

The shipping industry's footprint is impressive in the global economy. Let us consider that nowadays, over 80 percent of the international trade by volume is carried by sea (UNCTAD, 2020), while about 1,89 million seafarers serve the world merchant fleet (ICS, 2021).

6.2 Ships' specific features

As the maritime industry pulls the cybersecurity industry's attention, we shall understand some critical differences from traditional offshore premises.

A ship is registered under a country's flag, and this country's laws are applicable when the vessel travels on international waters. On the contrary, the neighboring country's laws apply[11] in territorial waters.

A vessel is a moving platform floating on the sea and transiting from one port to another while carrying people or goods. While being at the port, crossing a channel, or at the open sea, several systems onboard work constantly and require supervision by specialized personnel. For many years, the only systems onboard were mainly the main engine plant, the steering system, the power plant, auxiliary machinery, primary navigation, telecommunication systems, and the relative devices for their control. All these devices were part of what we now call Operation Technology (OT) systems (see Figure 2[12]).

[11] United Nations Convention on the Law of the Sea, https://www.imo.org/en/OurWork/Legal/Pages/UnitedNationsConventionOnTheLawOfTheSea.aspx, Accessed on 8 May 2022

[12] Practice of Cyber Security Management System on Cargo Ship, https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.asef2015.com%2Fasef-forum%2Fpdf%2FASEF%25207-Practice%2520of%2520Cyber%2520Security%2520Management%2520System%2520on%2520Cargo%2520Ship%2520-%2520Zhibiao%2520Chen%2520-%2520CCS.pdf&psig=AOvVaw1XduE2zk0NIJsBAWD8SZHW&ust=1652006837577000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCLid5ZmbzfcCFQAAAAAdAAAAABAw, Accessed on 7 May 2022

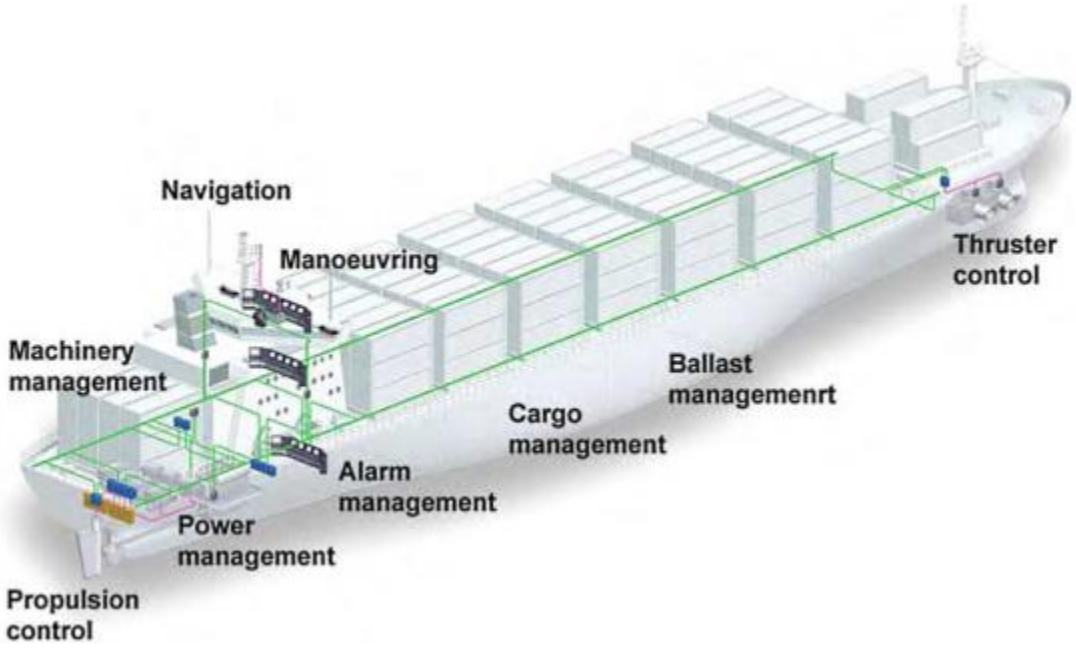

Figure 2: OT systems onboard a typical container ship

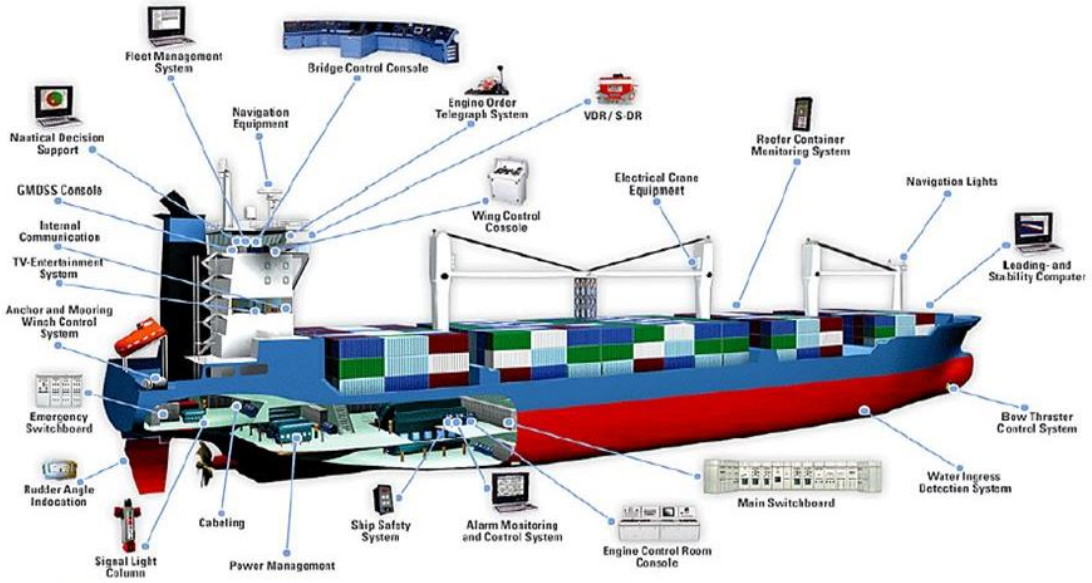

Figure 3: OT and IT systems onboard a typical container ship

Progressively, personal computers and intelligent devices found their place inside every room of the vessel to replace some of the manual work, develop an advanced and centralized control, make the transit safer, and make communications with the

rest of the world more frequent and reliable. Nowadays, we call these systems Informational Technology (IT) systems (see Figure 3[13]).

The two systems categories use networks where the devices are connected and communicate with each other and with centralized consoles. In the following chapters, we will have insights into both classes and comprehend the reason for separating these networks and the challenges they raised and collaborated with public networks like the Internet.

6.3 OT versus IT systems

The average human in developed countries is familiar with IT systems. A significantly small portion of the population is also familiar with concepts regarding OT systems. Most of them work in factories, industrial facilities, or sea vessels where automated sensors attached to internal networks monitor critical components like turbines, electrical plants, and ventilation systems. Such systems are also known as Supervisory Control and Data Acquisition (SCADA) or Industrial Internet of Things (IIOT).

In OT systems, the procedures have the highest value, while in IT systems, data takes priority. A typical OT machine has a 20 to 30 years cycle time, while an IT device's time is between 6 and 10 years. We seldom update or upgrade an OT system. On the contrary, an IT system requires frequent updates to prevent malicious attacks.

A breach in an OT machine may result in injuries or deaths, damage or destruction of assets, and severe environmental impacts. On the other hand, a breached IT system may disrupt operations and cause personal data leakage and financial losses.

For a long time, OT systems were separated from IT systems. The Internet wave, though, and the tendency to bring everything to the cloud increase the probability of having OT systems connected to IT systems, making their defense challenging. Traditionally, SCADA systems have been using proprietary protocols to connect remote devices to sensors. A few cyber incidents have been recorded in the last few years, raising the awareness level in the field. Building and sustaining a high level of

[13] Ships Now, https://slideplayer.com/slide/10615803/, Accessed on 7 May 2022

OT systems' resilience has driven an excellent practice indicating acquiring an inventory of such systems.

6.4 Cybersecurity concerns in the maritime industry

Ships have evolved to sophisticated platforms adopting technologies that dominate in land facilities. Figure 3 proves that a modern overseas vessel shall be considered a moving platform holding a great range of technologies that satisfy several needs. Consequently, all these devices, systems, and networks are subject to cyber-attacks and may lead to cyber incidents eventually. Attackers may target:

- Electronic Chart Display and Information Systems (ECDIS), the systems holding the electronic charts and the applications to ensure the safe navigation
- Sensors of Global Navigation Satellite Systems (GNSS) are generally known as Global Positioning Systems (GPS). These systems track the position of the carriers on the globe
- IT Systems running outdated operating systems or software
- OT systems that monitor vital operations such as propulsion or water ballast
- Crew members through phishing or social engineering techniques to retrieve sensitive data or import malicious code into the sip's internal networks

In *Annex A*, we provide a detailed catalog of onboard assets. Although not an exhaustive list, these assets cover most of the systems that may raise a cyber incident.

Ports have always been a vital part of the vessels' lifecycle and working routine. Their crews spend a significant portion of their time birthing in international seaports and terminals. Due to their corner side importance, the latest is considered critical infrastructures like transport means, telecommunication networks, banks, energy, and water resources. Critical infrastructures are feasible objectives for malicious and terrorist attacks (H. Boyes, I. Roy, L. Alexandra, 2016).

6.5 Known Safety Incidents

A few decades ago, attacking and taking control of a vessel while not being onboard would be a matter of science fiction, and no one would invest more time. In this section, we will mention some of the most well-known cyber-attacks against ports and vessels in the last decade and prove both the significant effects and the variety of methods and technologies used.

Antwerp is a Belgian city and one of the fastest-growing container ports in Europe. From 2011 to 2013, cyber criminals penetrated Antwerp's system to manage the traffic of thousands of containers (Bateman, 2013). Having direct access to the application made them hide vast quantities of drugs and direct abettors and truck drivers to pick up the containers before the authorities did. Their activity was exposed when the officers noticed the absence of containers. They compromised the software by sending an email with malicious code to the port's personnel. When the personnel executed the code, the criminals gained remote access to the port's management application. This first successful approach was tackled by integrating firewalls in the port's network. On a second, more sophisticated attack, they installed critical loggers on the corporate network and accessed what the port's personnel entered (on their keyboard) and viewed on their monitors. In 2013, when the second attack was exposed, the police reported that more than a million tons of heroine (nearly 170 million dollars) had already been transferred during the last couple of years.

In 2012, an employee working in Saudi Aramco, one of the world's biggest oil suppliers (10% of the world's oil), visited an infected website by clicking an email's hyperlink (Bronk, 2013). More than 35,000 corporate systems were infected, a significant portion of data was gone, and they lost Internet access for the entire network. The company sustained their activities for 17 months to mitigate this critical situation and purchased 50,000 hard drives to recover its network.

In 2013, a severe attack occurred at an oil extraction platform in the Gulf of Mexico (Shauk, 2013). The attackers infected the corporate network when some workers connected personal devices to the platform's critical systems. The malicious code disconnected the platform from the navigation system and locked it up.

In 2013, a research team in Texas managed to take control of the navigation systems of a luxurious 80 million dollars yacht (Brewin, 2013). They used a 3,000 dollars

equipment and GPS spoofing[14] to achieve their goal. By sending navigation data to the ship through stronger signals than the original satellite signals, they changed the ship's route without letting this course change displayed in the electronic charts. GPS and AIS spoofing are known techniques used in navies around the world trying to lure or confuse opponent ships.

In June 2017, the *NotPetya* virus[15] infected A.P. Moller – Maersk (McQuade, 2018). Among the biggest shipping companies, Maersk holds over 600 container ships and 16% of the global market. During the attack, the company was forced to sustain its IT systems and limit the number of containers delivered by 20%. The *NotPetya* ransomware locked the affected system's data and adjusted the Master Boot Record, thus preventing the users from logging in to their PCs' desktops. The attackers requested $300m in bitcoins to decrypt/unlock the infected systems. The ransomware was installed through a typical software upgrade of the logistics department (ME Doc) in Ukraine's headquarters, exploiting a known Windows vulnerability (*EternalBlue*). During the first few days of the infection, the company suspended all its operations for 10 days to install 40,000 servers, 25,000 PCs, and 2,500 applications. Such a huge transition takes place within 6 months under normal conditions, according to the company's CEO, Hagemann Snabe. Some estimated the financial losses to be about 300 million dollars.

The incidents mentioned so far are only the iceberg's top. Their diversity and severity indicate the need for emergency countermeasures and activities that the maritime sector shall undertake without delay. Cyber-attacks on the maritime sector's OT systems increased from 50 OT hacks in 2017 to 120 in 2018 and more than 300 in 2019[16].

[14] GPS spoofing happens when someone uses a radio transmitter to send a counterfeit GPS signal to a receiver antenna to counter a legitimate GPS satellite signal. Most navigation systems are designed to use the strongest GPS signal, and the fake signal overrides the weaker but legitimate satellite signal., https://www.mcafee.com/blogs/internet-security/what-is-gps-spoofing/, Accessed on 8 May 2022

[15] NotPetya is widely viewed as a state-sponsored Russian cyberattack masquerading as ransomware, https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html, Accessed on 8 May 2022

[16] Maritime Cyber Attacks Increase By 900% In Three Years, https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/#, Accessed on 1 May 2022

7 Challenges

The human race has seen its life-changing exponentially over the last three centuries. Historically, we have specified three milestones in which extraordinary innovations boosted evolution and progress. From steam-powered mechanisms in the late 18th century (1st Industry Revolution) to electricity labor division and mass production in the 19th century (2nd Industry Revolution) and IT expansion and automated production in the 20th century (3rd Industry Revolution), human achievements are impressive.

The maritime sector continues to evolve, having been the entrepreneur in many human activities and most significant moments in history. We live in the technology era, a period some call the 4th Industrial Revolution (Industry 4.0 or I4.0).

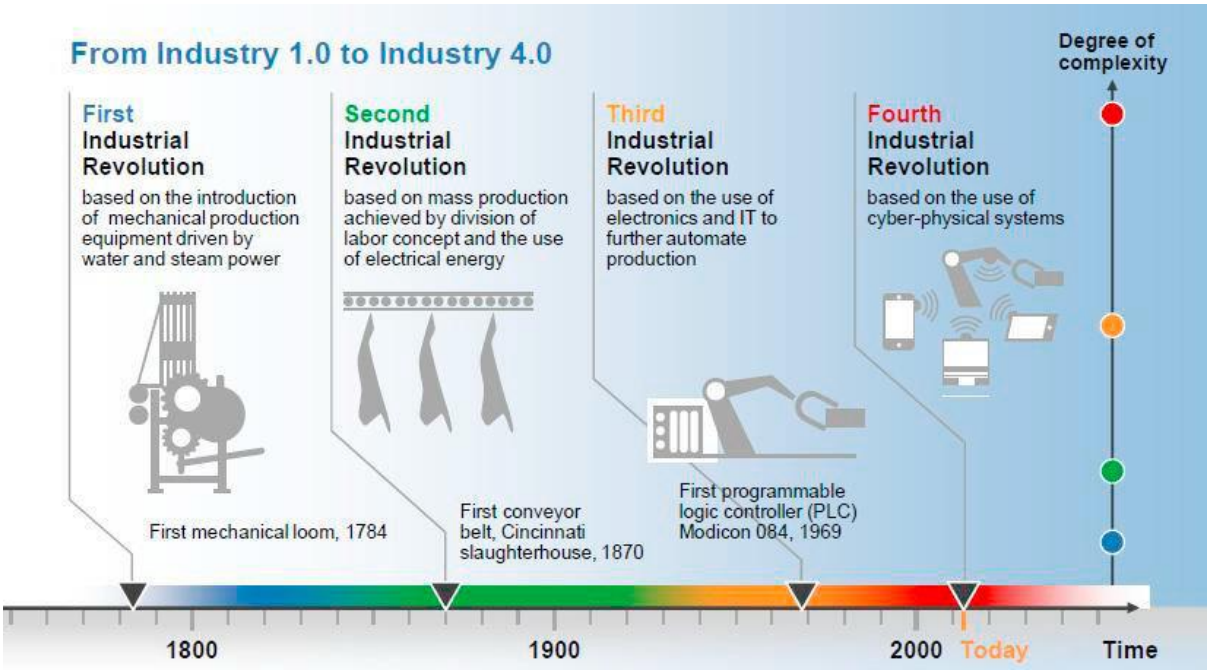

Figure 4: Industrial Revolutions[17]

Industry 4.0 is based on nine pillars (Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., Harnisch, M., 2015): Augmented Reality (AR), Simulation Modelling (SM), IoT, autonomous robots and systems, horizontal and vertical system integration through new standards, cloud computing, 3D printing and additive manufacturing, big data and analytics, and finally, cybersecurity.

[17] From Industry 1/0 to Industry 4.0, https://www.researchgate.net/figure/Industrial-revolutions-timeline-Source16_fig1_344457200, Accessed on 10 May 2022

People have been trading goods, thoughts, customs, and beliefs for thousands of years. Sea channels have brought different cultures in touch, helping them evolve together. According to the International Chamber of Shipping, about 11 billion tons of goods are transported by ship each year[18], representing an impressive 1.5 tons per person (Figure 5). We live in a fast-growing technology age, having a steady tendency to automate tasks we were doing manually in the past.

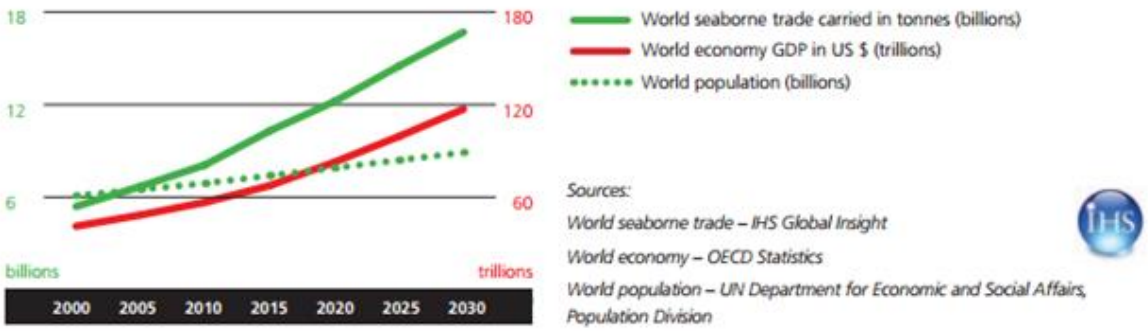

Figure 5: Predicted increases in world seaborne trade, GDP, and population

Autonomous, self-driven cars are driving on the roads[19], not a fiction dream anymore. Self-driven trucks and ships are the ones to follow soon. In this direction, the new 5G technology is implemented gradually, bringing life to high-speed communication channels. Sea giants' navigation and overall management will come true soon through these channels.

The onboard sensors' advanced technology is so mature that autonomous ships can prove a mainstream approach in the next few years (Iakovleva, E. V., & Momot, B. A., 2017). A critical success factor for this gigantic step to autonomous vessels is the bidirectional, accurate, and scalable communications supported by multiple systems that build redundancy and minimize risk (Mäkinen, 2016). The 5G technology ensures sufficient bandwidth and sets the basis for fully controlling the maritime giants. At the same time, cyber risks raise the impact level for all connected systems since everything connected to the Internet is considered vulnerable and can be hacked (Duck, 2017).

[18] Shipping and world trade: driving prosperity, https://www.ics-shipping.org/shipping-fact/shipping-and-world-trade-driving-prosperity/, Accessed on 10 May 2022
[19] Future of Driving, https://www.tesla.com/autopilot#:~:text=Tesla%20cars%20come%20standard%20with,and%20new%20generations%20of%20vehicles., Accessed on 10 may 2022

During the last 3 years, the world has faced the worst pandemic ever seen, with millions already passed away. To tackle the unprecedented spread speed of Covid-19 on a global scale, the governments have implemented quarantine in several ways. This has led to a constrained workload and, in many cases, economic slowdown and lack of necessary materials. Our world is much more complex than it used to be, even a century ago. Many parts of a complex item are manufactured in different parts of the world. Thus, a lack of a single material can affect the item's availability. Perhaps the most representative example of this interdependence is the car industry. Global car manufacturers based in Germany have decided to delay car deliveries due to the lack of chips made in Eastern Asia. Allianz reported a significant rise of 400% in attempted cyber-attacks against ships during the same period since the pandemic broke out (Allianz, 2021).

Initiatives on the political chessboard result in significant footprints and alter how we realize our world and interact with our fellow citizens. Let us consider the recent Russian invasion of Ukraine in February 2022. Some argue that we have stepped into World War III. Unlike the first two world wars, it will be mainly conducted through financial sanctions rather than on the field, having NATO's army fight against Russia's troops. This scenario scared humanity during the Cold War period. It is not a secret that Russia affords one of the world's biggest and well-trained hackers' team. Even before the invasion of Ukraine, this team has been accused of conducting two attacks against the US satellite Internet firm Viasat and government agencies[20].

Furthermore, an increasing digitalization takes place in every activity and field. Significantly, in the maritime sector, digitalization improves the connectivity among ships and shore premises and supports more complex shore-based ship operations as a regular practice (Baldauf, M., Kitada, M., Mehdi, R.A., Al-Quhali, M.A., Chong, J.C., 2018). Baum-Talmor, et al. revealed a significant gap between the seafarers' required and acquired skills, including technical skills and cyber-specific knowledge. To be competent, a seafarer must invest their own money in accomplishing training curriculums and be awarded the appropriate certificates since their companies seem unwilling to undertake this cost (P. Baum-Talmor, M. Kitada, 2022). A ship owing

[20] Ukraine suffered two cyberattacks in the lead-up to Russia's invasion, https://www.washingtonpost.com/politics/2022/03/30/ukraine-suffered-two-cyberattacks-lead-up-russia-invasion/, Accessed on 7 May 2022

company’s senior management committed to digital transformation should invest in strengthening their sailors’ knowledge level, including skills in the IT and cybersecurity field. Therefore, covering the training cost seems a reasonable measure. Consequently, a failure to do so will probably raise the cyber risks considering that the gap between existing knowledge and desired awareness will create problems for seafarers with digital skills.

8 The Guidelines on Cyber Security Onboard Ships

8.1 Introduction

Figure 6: The guidelines on Cyber Security Inboard Ships version 4

An essential pillar in BIMCO's *Guidelines* is the continuous engagement of the senior management throughout the cyber risk management life cycle. BIMCO follows a holistic approach to identifying the different entities playing a role in the cybersecurity context and supplying solutions in developing proactive and post-active measures in defending or mitigating the effects of cyber attacks. This holistic approach has a circular flow, always active and running on a maritime platform. A key concept of this approach is the need to breed a cybersecurity culture among all stakeholders that cyber defense cannot be exhausted once but has to be a living procedure, subject to constant revisions and updating to meet the newer, advanced, more sophisticated challenges.

The *Cyber Risk Management Approach* proposed by BIMCO splits the ship's defense against cyber threats into six procedures (Figure 7):

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

Figure 7: Cyber Risk Management Approach

A second key concept is how individual parts contribute to calculating their parent entity (Figure 8). All parts are multiplied by having equal weights. For instance, the Threat entity is the multiplication effect of Intent, Opportunity, and Capability. The final Risk is calculated as follows:

Risk = Impact * Likelihood

= Impact * (Threat * Vulnerability)

= Impact * ((Intent*Opportunity*Capability) * Vulnerability)

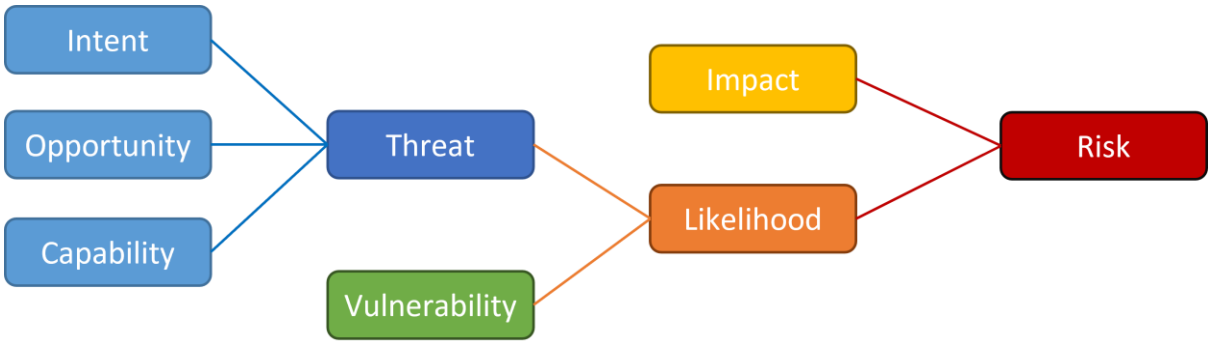

Figure 8: The relationship between different factors influencing the risk

To calculate the risk for a single threat, we must multiply all these five entities. We only need to turn just one of them to zero to turn their outcome be zero too! This principle is paramount and should accompany our efforts while building the defense net with countermeasures later.

Similarly, *ISO 27005* suggests that the estimated risk is a "*combination of the likelihood of an incident scenario and its consequences"* (ISO/IEC 27005/2018 Information technology - Security techniques - Information security risk management, 2018). The principle in both documents converges to the assumption that a Risk (**R**) is the product of the Probability (**P**) of happening and the effect (Impact - **I**) it will have on the organization's functionality, thus

R = P * I

8.1.1 Plans and Procedures

During the *Cyber Risk Management Approach*, the company will need to establish generic plans and procedures and apply them to most of its fleet. In contrast, others will be applicable to a small portion of their ships or diversified.

All relative material regarding the cybersecurity onboard shall be kept in the Ship Security Plan (SSP)[21].

8.1.2 Stakeholders

We already discussed the necessity of having the senior management engaged and determined to have all command levels lined up in defense against cyber threats. The way the administration will decide to propagate the relative values to their subordinates is of the essence.

Several stakeholders' groups shall be aware and lined up on the same principles. Ship managers and ship owners usually have separated entities, and special care should be given to dividing and assigning the proper, concrete responsibilities. The economy gets globalized, and so does the legislation worldwide. In the meantime, there are discrete differences in laws and legislation even between western countries sharing common beliefs and moral values. The General Data Protection Regulation (GDPR) highlights the legislation frame diversity. GDPR aims to protect the privacy rights of European Union (EU) citizens. A ship owner based in Greece will have to consider GDPR and other countries' legislation when their ships enter coastal waters or birth in their harbors. US and Australia have their acts for data privacy, for instance. We notice a tendency in having similar legislations to converge, but until a single law framework is applied worldwide, different stakeholders shall be aware of such discrepancies.

Agents link the ship with harbor facilities, port authorities, terminals, etc. It is common to have agents coming onboard a birthed ship and bringing their laptops. Connecting their computer to the ship's network is expected, but so is the likelihood of cyber criminals targeting these agents to access the ship's network.

[21] Understanding Ship Security Plan On Board Ships, https://www.marineinsight.com/marine-safety/understanding-ship-security-plan-board-ships/#:~:text=Ship%20Security%20Plan%20(SSP)%20is,from%20any%20security%2Drelated%20risks., Accessed on 10 May 2022

Vendors and other external parties can also be used by an attacker and should be treated with consciousness. The ship's cyber defense is as strong as its weakest link. Following the BIMCO's *Guidelines,* we may establish robust safety procedures and apply proactive measures that will lower the risk residuals to an acceptable level. However, letting an external party connect with their laptop in the ship's internal IT network without performing safety checks or applying a software upgrade to an OT system without testing it beforehand can ruin our SSP and lead to a cyber incident.

Therefore, it is common for companies to sign agreements and contracts with vendors and suppliers they trust and expect high performance and service quality. In short, a company having raised cybersecurity to a high level shall require its contractors and associated parts to comply and follow all the national requirements and obligations agreed upon in contracts between the two parties.

8.1.3 Improvements from the previous version

The previous version (v.3) of these guidelines was issued in November 2018 and supplied the initial guidance in implementing cyber risk management in the Safety Management Systems (SMSs). Cyber incidents that went public during the last few years, as mentioned in Chapter 6.5, led to a revised version having learned from the attacks and their goals.

The latest version contains updated best practices in the cybersecurity field[22]. The risk management model is updated and treats the threat as the product of capability, opportunity, and intent. Similarly, it treats the likelihood of a cyber incident as the product of threat and vulnerability.

Reputable organizations in the maritime sector contributed to the fourth edition: Chamber of Shipping of America, INTERCARGO, Digital Containership Association, INTERTANKO, IUMI, INTERMANAGER, OCIMF, IMCA, Sybass, Interferry, and WSC.

[22] Industry publishes new and improved cyber security guidelines, https://www.bimco.org/news/priority-news/20201223-new-cyber-security-guidelines, Accessed on 10 May 2022

8.2 Cyber Security and Risk Management

To understand the concepts involved in this section, we will begin with the entities' definitions and their relationships. An asset is a valuable resource for an organization; thus, it requires protection.

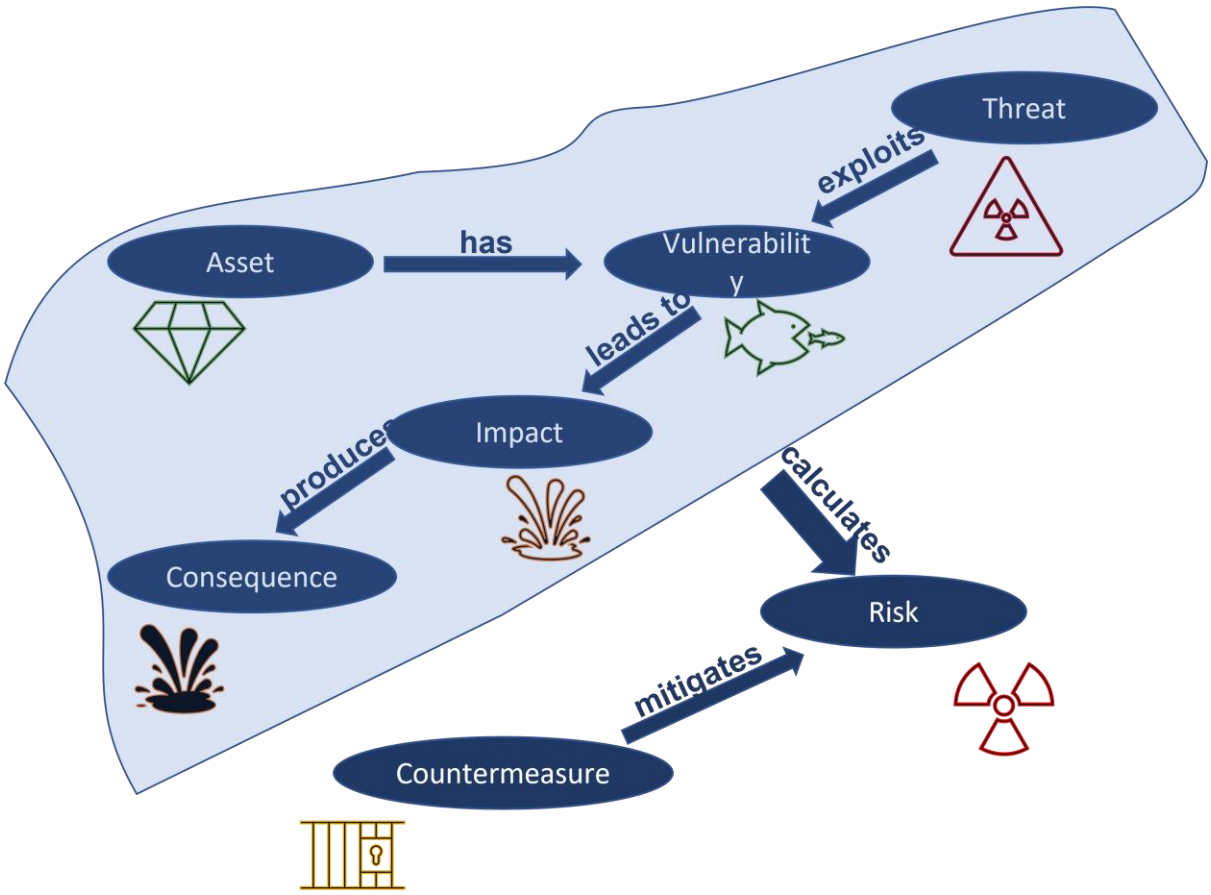

Figure 9: The relationship between entities involved in Risk Management

According to ISO/IEC 27000/2018 (ISO/IEC 27000/2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary, 2018), a threat is a "*potential cause of an unwanted incident, which can result in harm to a system or organization,"* a vulnerability is "*the weakness of an asset or control the one or more threats can exploit"* and consequence is the "*outcome of an event affecting objectives."* Moreover, the risk is "*the effect of uncertainty on objectives,"* while control is a "*measure modifying risk."* Finally, the impact is the change a vulnerability brings to the organization for an asset and is often confused with consequence**.**

As shown in Figure 9, risk can only exist if an asset is valuable for an organization and an existing threat takes advantage of known vulnerabilities to affect the asset so that the organization's operations will be affected.

8.2.1 Identify Threats

Identifying threats becomes a priority in developing a risk management system. Some of the threats are not intentional and act accidentally, without having the intention of causing harm. Personnel lacking the required cyber awareness essentials and inserting removable drives (USB sticks) in the corporate network relies upon this category. Most threats attempt a cyber security breach intentionally, motivated by personal or group/state interest like gain of several kinds (financial, reputational, commercial), espionage (commercial, industrial), the challenge, taking revenge, seek for media attention, or result in the most extensive damage possible:

- Activists
- Criminals
- Opportunists
- States, state-sponsored organizations, and terrorists

We distinguish cyber threats affecting ships and their companies as:

- Untargeted attacks using tools and techniques found on the Internet like *malware* (*trojans, viruses, worms, ransomware, and spyware*), *water holing* (fake website), *scanning,* and *typo squatting* (*URL hijacking*).
- Targeted attacks against specific companies and ships using more advanced techniques like soci*al engineering, brute force, credential stuffing, DOS attacks*, and *phishing*. A rather exciting and sophisticated process, called *subverting the supply chain*, targets compromising equipment delivered to the ship or company.

An attacker using targeted cyber-attacks will generally follow four stages:

- *Survey/reconnaissance*. The attacker uses publicly available information about an achievable target (internet, newspapers, editions). At this stage, the attacker

gains this information passively, without exposing his identity or position. The amount of data that can be obtained is not to be underestimated since search engines like *Google* or most advanced crawlers like *Shodan*[23] can expose crucial data about the target.

- *Delivery*. The attacker attempts to gain access to the target's data either on-site (infected USB sticks) or remotely through Internet (fake websites, emails containing malicious files or links, online company services)
- *Breach*. The attacker exploits a vulnerability and opens a window to the target system.
- *Pivot*. The attacker uses an already compromised system to target another, more effective system.

These stages are not exhaustive or mandatory but highlight the core elements that constitute an organized attack and the commitment and patience that an attacker must demonstrate to succeed.

We can distinguish threats against onboard systems into threats against IT systems, driven by financial aim, and threats against OT systems. Ship owners hesitate to make attacks against OT systems public; thus, historical statistics in this field are limited. These attacks have no direct financial reward for the criminal initiating the attacks in comparison to IT systems. Moreover, OT systems are generally isolated from the IT systems and public networks like the Internet. Finally, a compromised OT system can raise physical risks significantly by causing material damage to machinery and human injury or even death, as we show in Chapter 6.3.

8.2.2 Identify vulnerabilities

Creating a list of vulnerabilities is the second step in the Risk Assessment procedure. Although this catalog will be unique for every platform, some vulnerabilities are common and will most likely apply to most of the cases:

[23] Shodan Search Engine, https://www.shodan.io/, Accessed on 10 May 2022

- Outdated operating systems are not supported anymore (Windows XP, Vista, and 8)
- Outdated or not patched system software, outdated or missing antivirus software, outdated software against malware
- Inefficient network implementation/segmentation and/or lack of protection in their boundaries
- Misconfiguration of security systems (usage of administrative accounts and passwords and network management)
- Critical equipment, always connected with shore systems
- Inefficient access control over third parties (contractors, subcontractors, suppliers, service providers), including both assets (devices) and their services
- Personnel lacking the basic cyber security training and awareness
- Untested or inappropriate contingency plans and procedures

To support every risk assessment step, we need to identify the IT and OT systems onboard and record them in an official document called *Asset Register*. Once created, the responsible staff shall ensure it is updated regularly and appropriately since the quality of these tasks will directly impact the Risk Assessment process overall. For each asset, both its initial cost and the maintenance cost shall be mentioned. In *Annex A,* we have included the first Annex of the *Guidelines,* providing a list of systems commonly fitted on modern ships. In short, we are concerned about the following categorized assets:

- Communication systems
- Bridge systems
- Propulsion, machinery management, and power control systems
- Access control systems
- Cargo management systems
- Passenger or visitor servicing and management systems

- Passenger-facing networks
- Core infrastructure systems
- Administrative and crew welfare systems

IACS Recommendation no. 166 on Cyber Resilience (IACS, 2020) recommends several fields to be documented:

- Network communication devices (switches, routers, gateways)
- Communicating devices (PLCs, sensors, actuators, meters, circuit breakers)
- Logical map of the networks including:
    - IP address ranges (inventory of switches, functional description of each range, connections with other IP ranges)
    - Non-IP addresses (MAC addresses, inventory of switches, functional description of each network, devices connected to other networks)
    - Non-Ethernet Access Points (list of access ports, connected devices)
    - Desktop and Logical Servers (IP address, operating system's details, underlying physical server, applications, services, and their versions)
    - Connectors and communicating devices (remote I/O, sensors, actuators)
- Software inventory (name, publisher, installation date, version, local/remote maintenance, access control list (read, write, execution rights), license number)
- Network services for each equipment:
    - IP based services (protocol name, protocol version, listening ports)
    - Non-IP based services (listening interface)

Although these recommendations are intended for newbuilds only, they can be used for older platforms.

A general rule is that a stand-alone system is less vulnerable to external cyber threats than connected systems, especially those connected to other networks. Isolating each

system is not always feasible or efficient since many systems utilize connectivity at the core of their functionality. For instance, integrated communication systems use various devices to automate communications and offer advanced availability, thus making use of connected physically compound equipment from different locations onto the ship. Although tempting, complete isolation of systems is not always feasible. On the other hand, network segmentation is, and we will refer to this technique in Chapter 9.

While developing the Asset Register, we shall record each system within a category/subcategory of Annex A and answer the same set of questions that will help us in assessing how vulnerable they are:

- Is the system connected to other networks or stand-alone?
- Has the system an external interface (direct or through other systems)?
- Does the system utilize protection measures (encryption, hashing)?
- How often does the system require software updates?
- Does it need removable devices to run diagnostic tests?
- How easy is it to access the system physically?

Another factor we shall consider is the ship-to-shore interface. As the onboard systems become more sophisticated and for logistics reasons, there is a tendency to move a portion of the monitoring responsibility from the ship to shore facilities. Onboard personnel is sometimes unaware of the devices' equipment, whose functionality and availability are solely based on the shore's availability and efficiency. This raises a significant risk in two ways. At first, maintaining a live link between the ship and a shore facility increases the chances of an attacker managing to sniff. Secondly, accidentally or after a malicious attack, a failure in the link will lead to a complete loss of the service without a backup plan. It is not uncommon to outsource some of the ship's functionalities to third parties. It is common to outsource ECDIS maintenance to a specialized company that will update the navigation software. Such major tasks take a few hours to days and raise a risk that we shall consider while developing the Security Plan.

The diversity of the ships compared to shore facilities in terms of cyber security is that, by default, a ship is a moving platform that eventually will visit ports and facilities

outside the jurisdiction and close control of the ship's ownership. It is common to get visits by external personnel on predetermined dates or an emergency basis. Technicians, contractors, agents, suppliers, port officials, pilots, and more will eventually embark for a few hours or even days. It is also expected that some of them will bring their devices like laptops, tablets, and mobile phones that will need to charge or connect to the Internet to provide their services. Some may request to insert their removable devices into a ship's computer or use a printer to print a document. Such cases shall be explicitly documented in the Cybersecurity Procedures. In general, sensitive data shall be removed from the ship and reinstalled once the visor disembarks to prevent data loss. Also, a backup plan is always helpful and appropriate as long as it is efficient and the backups are taken as documented. Prior to using the ship's system, all external devices shall be scanned for malware. Finally, OT systems should be checked that they work flawlessly.

8.2.3 Likelihood and Impact assessment

We saw in Chapter 8.1 that the *likelihood* is the product of two other entities, *threat,* and *vulnerability*. The following equation illustrates the significant role of both in determining the likelihood of a security event:

Likelihood = Threat * Vulnerability

To end up with real and valuable data regarding every cyber security incident that we have specified, we need a neat and meticulous process. Moreover, we need to establish a just and consistent system in applying the same severity to both the incoming data and its outputs. There is no need to develop the same scale of levels; however, it is paramount to use it methodically and globally once established. This is the only way to ensure that the products (in this case, the likelihood of incidents) will tell the same story every time and will ring bells if the predetermined alert level is reached.

A significant differentiation spotted in the maritime industry compared to other sectors is a semantic effort to hide corporate secrets even if related to security incidents that could affect others too. The competition is severe, and ship merchants look for

opportunities even in their sleep. It only needs a whisper of a minor data breach to shake the company and make its shares dive in the global marketplaces.

Level	Likelihood description
1	Never heard of in industry. Close to being something unimaginable.
2	Heard of in industry, but only extremely rarely and as the result of a chain of many unfortunate events.
3	Incident has probably occurred in own company, but in the context of faulty equipment or by surprising mistakes made by people involved.
4	Happens occasionally in own company, typically in the context of faulty equipment or by mistakes by people involved (the kind of mistakes that tend to happen on board from time to time).
5	Happens frequently when undertaking the work in question.

Figure 10: BIMCO – Example of likelihood scale from an SMS

The Likelihood Assessment occurs in a matrix similar to the one shown in Figure 10, suggested by the *Guidelines*, but it cannot be taken for granted. Every organization shall make its own if it does not meet its requirements. The challenge is linking individual incidents with the levels seen on the left side. For decades, this unwillingness to share security incidents (obviously not only cyber incidents) has been the case. During the last few years, more and more security consultants have suggested combined solutions based on common databases for several companies that update live and build a robust firewall against common attacks.

The next step in our process is the Impact Assessment of each incident. Working similarly, we need to establish a matrix like the following:

Level	Impact description
1	No health effect/injuries. No damage to environment, assets, finances, or company's reputation.
2	Very slight health effect/injuries. Very slight damage to environment, assets, finances, or to company's reputation.
3	Some health effect/minor injuries. Minor damage to environment, assets, finances, or to company's reputation.
4	Major health effect/relatively serious injuries. Local but major damage to environment, assets, finances, or to company's reputation.
5	Fatality or permanent disabilities. Widespread, significant damage to environment, assets, finances, or company's reputation.

Figure 11: BIMCO – Example of an SMS's verbal description of impact levels

Again, this suggestive matrix can be reworked and brought closer to the company's needs. However, now that we have both tables on hand, we must highlight a few aspects that shall not be underestimated:

- Both the entities we assess, thus likelihood and impact, are considered to have equal weight. That is why the requirement that the number of levels shall be identical in both cases. We may decide that we need 10 likelihood levels in a specific company. If this is the case, we must specify 10 impact levels too.
- No level shall be left empty without a description. Moreover, the description shall be concrete and leave no room for doubts.
- There is no need to fill the Levels column with integers starting from 1 and ascending by one until the final level. Using decimals can only confuse the personnel who will assess the dangers and born doubts on the board.

While assessing the impact, we shall be aware that information may suffer due to the CIA model's sawn pillars (Confidentiality, Integrity, Availability). The relative importance among these three components is based on the data or information used. It is seldom to face a confidentiality issue for the OT systems specifically.

According to the *Guidelines*, we shall perform the Impact Assessment on every critical equipment and system aboard whose temporary and timely downtime will affect significant functions of the ship or even lead to aborting its mission and heading to the nearest port.

We have completed both the Likelihood and Impact Assessment, and we are ready to move forward to the next and probably most exciting part of the assessment process, the Risk Assessment.

8.2.4 Risk Assessment

This is the assessment part, where we will gather the findings from the previous steps and quantify the results by applying simple multiplication operations with a trivial calculator. This is also the section where we will confirm the integrity and correctness of the expected results based on our experience.

The Guidelines split Risk Assessment into four phases:

- *Pre-assessment activities*. As faced in similar assessments, a robust level of knowledge shall be gained regarding the ship scheduled to be inspected. To establish this knowledge, the assessors shall:
    - Review documentation about the maintenance and support of the IT and OT systems onboard
    - Review the documentation in identifying vulnerabilities and determine feasible impact levels
    - Specify leading manufacturers of critical equipment and systems
    - Identify security POCs with the major manufacturers and establish a communication channel with them
    - Identify the requirements regarding maintenance and support for equipment and networks that have been outsourced

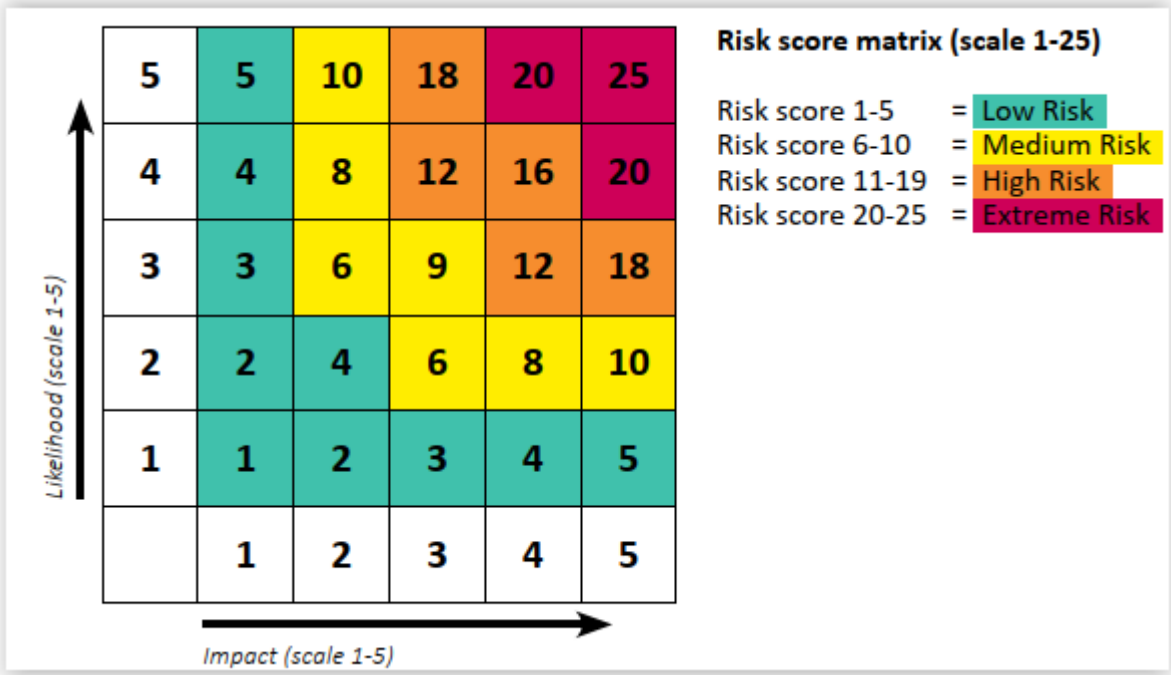

Figure 12: BIMCO – Example of a company's risk score matrix

- *Ship assessment*. The more aware and experienced the accessors, the more accurate results they will probably have. In assessing the risk for every system, though, they may ask for help from specialized personnel about specific systems requiring advanced technical skills and knowledge. A combined matrix

resulting from the likelihood and impact evaluation can look like Figure 12. In this combined matrix, one can understand why we insisted on using the same scale for both entities. Symmetry is not only eye-catching but also proof of smooth operation. ISO 27005 suggests that in cases where the output risk exceeds the assessment criteria established by the company before the assessment's start, we shall apply countermeasures to mitigate this level and lower it to an extent acceptable by the board. The Guidelines include the same principle. Extending this context, they suggest using a holistic approach whenever possible. Suppose a better configuration on a server mitigates the risk to an acceptable level. This same configuration shall be applied to the rest servers unless there is a good reason for exclusion. Following a typical Risk Assessment, it is not uncommon to end up with a thorough update in security procedures and IT and OT devices documentation. The same can happen for configurations on various IT devices like routers, servers, and firewalls.

- *Debrief and reporting*. We expect to have a Risk Assessment conducted by internal and external personnel. In the first case, the used procedures and limits shall be well documented and updated regularly. In the case of a third party performing the assessment, we shall expect a list of technical findings (vulnerabilities, exploits, impact, and feasible countermeasures) and a prioritized catalog of actions to mitigate these findings. The shipowner will get the assessment's results and have the time to digest the findings and discuss them with the assessors.

- *Manufacturers debrief*. In this final stage, the manufacturer gets informed regarding the flaws and possible backdoors of their systems using a limited portion of the assessment made for the ship owners. Giving a manufacturer a warning about danger can benefit the community long-term.

As mentioned above, a third-party assessment is on the table in all cases. It is strongly suggested to be included in the assessment process if the company's finances can afford it. A cybersecurity consultant is typically accompanied by more experience and global knowledge compared to the company's Security Officer. The extent to which a risk assessment can deploy has no limits. That said, the consultant and their team

may organize and perform penetration tests[24] or even physical intrusion exercises into a secured area onboard. Before execution, such advanced testing techniques shall have been agreed upon with the top management to prevent unexpected behavior from unsuspecting personnel and loss of business continuity.

8.3 Protection Measures

All possible risks have been quantified and their treatment prioritized at this stage. To mitigate their impact below the agreed levels set by the company's board, we can use procedural or technical protection measures, while a combination of them is always on the table.

Two essential terms are defined to describe the approaches we can use solely or, most effectively, in parallel as parts of the holistic approach mentioned above, the *Defense in Depth* and the *Defense in Breadth*.

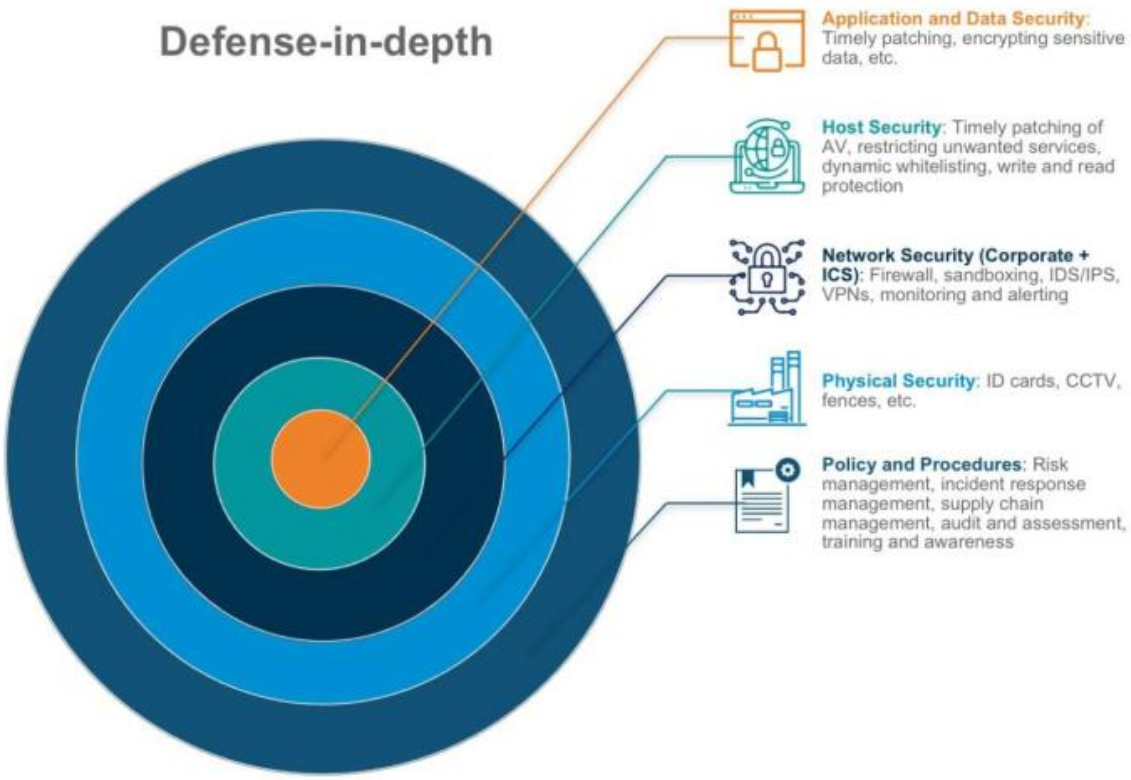

Figure 13: Example of Defense in Depth

[24] not appropriate for OT systems most of the times

On the one hand, the *Defense in Depth* implements adding more security layers to an already secured device. Like an onion shell, a system's security shall be composed of several layers to reveal before entering the core data. As suggested by the Cybersecurity Strategic Planning Department, a single countermeasure cannot guarantee a bulletproof secure network by itself (Planning, 2021). However, different countermeasures put strategically can defend against several cyber-attacks and eliminate the cybersecurity risk to an acceptable level. Figure 13 shows a related implementation of this approach[25].

The *Defense in Depth* is encouraged to integrate the following measures in conjunction:

- *Limited and monitored physical access based on the SSP*
- *Effective separation of networks, including segmentation and firewalls*
- *Detection of intrusion*
- *Performance of vulnerability scans and tests periodically*
- *Software whitelisting instead of blacklisting[26]*
- *Access controls and user controls*
- *Strict procedures about the password and removable devices usage*
- *Familiarity with security procedures and incidents reports*
- *Personnel's awareness and knowledge over time regarding cyber matters and their impact on them personally and their company*

On the other hand, the *Defense in Breadth* has a horizontal orientation. It refers to applying the same defensive measures across all vulnerable or critical equipment, including procedural and technical countermeasures. This approach is preferred to prevent exploiting a vulnerable device that could be used as a pivot system to infect adjacent systems. This is a known technique used by hackers who compromise one

[25] Best-practices for securing ICS environments using a defense-in-depth approach, https://moderncISO.com/2018/05/15/securing-industrial-control-systems-a-holistic-defense-in-depth-approach/, Accessed on 10 May 2022

[26] Whitelist vs blacklist, https://www.manageengine.com/application-control/whitelisting-vs-blacklisting.html, Accessed on 7 May 2022

system after another to access their ultimate target. Such an indirect attack requires many resources, both human and material, and can pay back in the long term, thus making it appropriate for significant targets.

In the following two chapters, we will describe the technical and procedural protective measures we shall have in our top priorities.

8.3.1 Technical Measures

Mentioning the changeability of technology and its means is not something new or innovative. We need to remind ourselves from time to time, though, how versatile and variable the IT environment can be. Based on this doctrine, it is self-evident that everything documented, including the measures, shall be reviewed and updated in predetermined intervals or after significant changes.

In this context, the Guidelines suggest technical principles that shall be followed. Apparently, due to their abstract content, one cannot simply copy them in their procedures. Still, they need to dig deeper into each of them and apply the appropriate measures that apply to their ship and system significantly.

Limitation and control of the network specifics. This includes the ports, protocols, and services used. The company's security policy must specify which traffic is permitted through their facilities and allow only that to propagate. Although pronounced, all unused ports and services shall be closed to prevent unauthorized access to the network's data or systems.

Configuration of networking devices. Such devices can be switches, routers, gateways, and firewalls. Only the documented devices shall be attached to the networks and be used for this purpose specifically. The networks themselves shall service the ship's functionality and always be controlled. Any uncontrolled network may pose a threat to the ship's overall operation. Advanced caution shall be applied for networks communicating with public networks like the Internet. Such networks are uncontrolled and shall be treated as potential threats to the ship's command.

Simple, still decisive measures technical measures include the following:

- Critical networks shall be under constant and positive control

- The same goes for networks providing remote access to the navigation system or other OT systems onboard. In such networks, though, there shall be a contained access point on board to do their job. The external access points shall also be secured to prevent unauthorized access on the shoreside.
- A network servicing cargo stowage, container management, or reporting essential ship details (destination, cargo, flag) to public authorities. Such networks shall also be controlled.
- On the opposite, some networks onboard may be controlled. Networks to give sailors access to the Internet and, in general, leisurely shall be considered off-the-grid networks.

To tackle the networks mentioned above, especially the uncontrolled networks, we may use software and hardware solutions using the correct configurations of the networking devices.

Network segmentation is a successful strategy that, if implemented correctly, can guarantee high-level and adequate protection overall. Such a strategy shall be analyzed and designed precisely to consider the required access levels of the personnel. Businesses commonly utilize a secure internal network and an untrusted zone with intermediate zones in the middle. Usage of firewalls proves to be the most apparent measure in segmenting a network from another network utilizing a different security level. Hardware and software firewalls apply rules of controlling traffic based on the IP, port, or application level. Figure 14[27] demonstrates a minimal segmentation example consisting of an internal zone, the untrusted zone (Internet), and two DMZs. DMZ stands for Demilitarized Zone and refers to subnetworks that accommodate servers like Domain Name System (DNS), File Transfer Protocol (FTP), web or proxy servers, and more that are isolated from the internal network and are given limited access to internal resources.

Physical protection is evident in personal or even corporate life, but we tend to pay less attention when it comes to the cyber field. When we think about cyber defense, we envision the malicious attacker being behind their device in some dark room in a

[27] Best Practices for Network Segmentation, https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/, Accessed on 10 May 2022

distant country. Although this may be true, implicating that they act in the dark, there is no excuse to exclude the possibility of trespassing a facility of our company and bringing themselves closer to their target while saving them a ton of work. Securing the physical defense of critical equipment is bonded to cybersecurity, and it is somewhat a prerequisite before applying the technical and procedural IT measures. Essential equipment and areas shall be locked and monitored. Cables running through unsecure areas or USD ports on routers or switches shall also be secured.

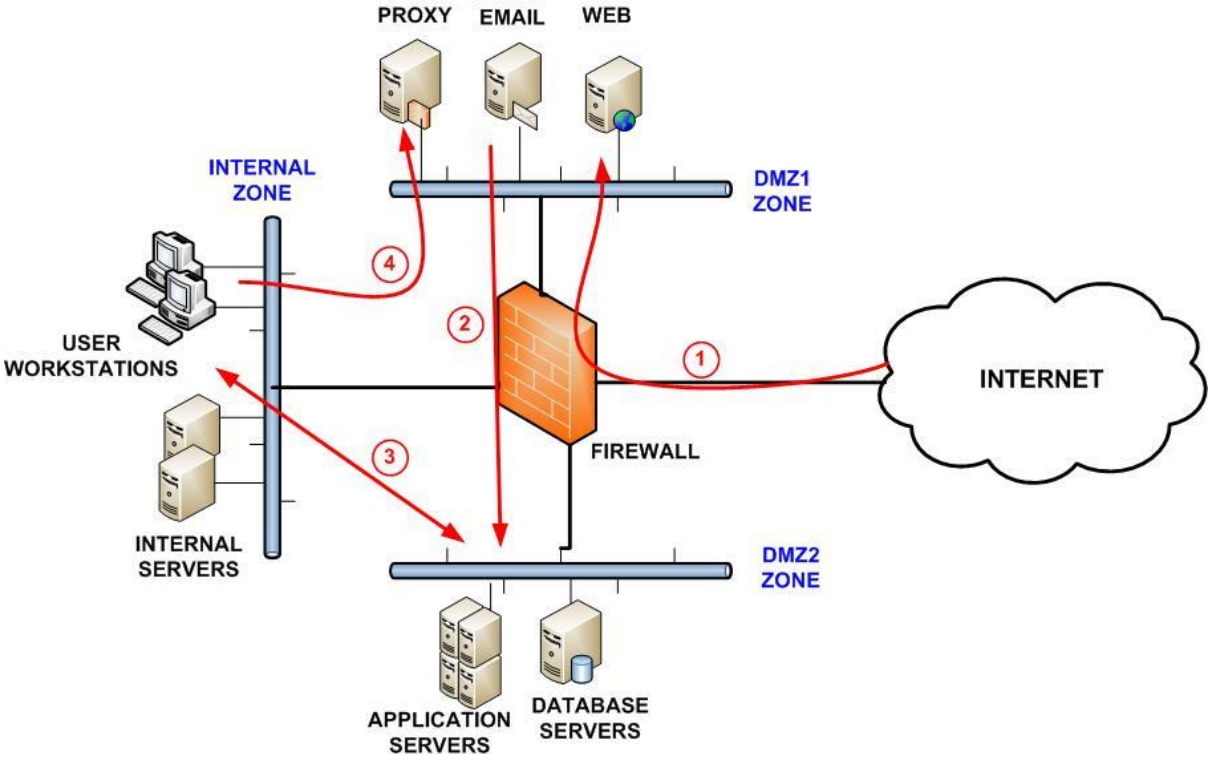

Figure 14: Firewall Security Zone Segmentation

Previously, we referred to the measures we need to take to shield the internal networks. Internal and External Communications play a crucial role in a ship's operation and performance. A wide range of devices covering different spectrum ranges are used throughout the vessel to integrate communication services. Satellite and radio communications shall be protected against malicious attempts by implementing the following protective measures:

- Virtual Private Networks (VPNs) and encrypted protocols strengthen the defense against *eavesdropping*[28]. A firewall at the entry points on board, and a dedicated secure server onshore, owned and operated by the ship's company, are also advised.

- An attacker will initially look for administrative functions like *port forwarding* and *remote administration page*. Deactivating such functions will make their attempt more challenging during their reconnaissance stage.

- An attempt to gain access to onboard satellite systems shall be expected. The second level of access shall be established by hiding the onboard device's address behind an onshore route to challenge this attempt. We shall not assign a public IP address to the satellite terminals onboard, thus making them routable from a browser. Instead, all connections should be routed through shoreside networks to cut off unauthorized access through firewalls.

- Web interfaces help personnel manage the communications services. Although helpful, such publicly accessible interfaces pose a potential threat. To limit this type of threat, we shall restrict access to administrative interfaces. Some are used only through the initial setup or during major maintenance sessions. That said, permitting access to them once their purpose is no longer valid is an expected measure. In the same context, default passwords used during the initial configuration shall be altered the soonest as possible (in the next login).

Wireless access control is a significant aspect and is always present at port or underway. The facilities supported by wireless networks spread from daily routine tasks to sailors' leisure and free time. That is why access to the wireless networks should be limited to only authorized devices using an appropriate encryption key that is changed regularly and meets high-encryption standards. Securing wireless communications is a real challenge due to their architecture, though[29]. To implement access control, we can:

[28] What is Eavesdropping in Computer Security?, https://www.ecpi.edu/blog/what-is-eavesdropping-in-computer-security, Accessed on 7 May 2022
[29] A detailed diagram of the four-way handshake, https://www.researchgate.net/figure/A-detailed-diagram-of-the-four-way-handshake-Msg-Message_fig1_328632250, Accessed on 7 May 2022

- Segment networks and use enterprise authentication systems[30]
- Adopt a wireless *Intrusion Prevention System* (IPS) to cut unauthorized access from rogue or illegitimate devices
- Implement *Network Access Control* (NAC) to label wireless devices as either corporate or personal, and treat them accordingly
- Shield the interconnection points that link wireless with wired networks, like routing devices (racks, routers) and network plugs

A general rule of thumbs detects that a user shall be given the access level required to perform their tasks and only for the time needed. Implementing a *whitelisting* approach in accessing the various networks onboard is part of a cybersecurity culture that shall be maintained throughout the organization constantly and without exceptions. In this context, users shall have access to workstations or servers required for their tasks and not be allowed to execute scripts and programs, or install irrelevant applications. Such a secure configuration of hardware and software shall be mirrored in the Ship's Security Plan, and the responsible person shall ensure its seamless appliance.

Accessing the web implies using email and web browser services, thus making email and web browser protection a part of protective measures against cyber-attacks that should not be underestimated. Relative directives include:

- Protection against social engineering
- Prevention against sensitive data leakage through emails
- Using encryption to shield crucial information transmitted with email or by voice
- Disqualifying web browsers from executing malicious scripts

Transferring emails as zipped or encrypted files, disabling hyperlinks in emails' bodies, cutting emails from providers not being whitelisted, and proper user accounts configuration are all well-tried technical safeguards and shall be treated accordingly.

[30] Enterprise Authentication Solutions, https://www.kuppingercole.com/research/lc80062/enterprise-authentication-solutions, Accessed on 7 May 2022

There is no bulletproof human innovation. Modern software and hardware may integrate extraordinarily unique and innovative security features. Still, it is only a matter of time for an intelligent person to discover how to overcome them. Vendors release security patches to address major flaws that could be exploited and lead to severe damage.

The ship's ownership shall develop a consistent application software security policy of applying such patches the soonest as possible after their release without disturbing the business continuity at the same time. Security holes are communicated through dark channels, and malicious attackers are more than willing to pay for them. They may face cases where a patch deployment is not feasible. In such a scenario, alternative options like isolating the unpatched network or system through physical and virtual techniques (VPNs) shall be applied.

8.3.2 Procedural Measures

The second pillar supporting the ship's cybersecurity fence is the development of procedures that the onboard personnel will follow while the ship is far from its base. These procedures shall be designed carefully based on supporting the sailors being away from home and working autonomously without constant intervention from specialized personnel in the headquarters or the outsourced partner. The procedural safeguards will delimit the manner and extent to which every tasked person will operate with the onboard systems.

Many people claim that human is the weakest link in an organization's cybersecurity defense. Although true, we can turn the human factor into the cornerstone that will support overall protection through procedural measures. Therefore, it is not a surprise that training and awareness rely on the core of this effort. Both shoreside and onboard personnel shall be trained accordingly to ensure that everybody talks the same language. It is common sense that every sailor shall be aware of the systems involved in their daily routine, operation, and emergency circumstances. The Standards of Training, Certification and Watchkeeping Convention (STCW)[31] highlights this

[31] International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978, https://www.imo.org/en/OurWork/HumanElement/Pages/STCW-Convention.aspx, Accessed on 7 May 2022

requirement. Apart from this necessity, though, we need to raise awareness regarding cyber security matters through the following issues:

- The risks following emails and how to handle them safely (malicious links, unknown sender, attachments)
- The risks raised by the Internet usage and especially on social media and chat forums
- Dangers regarding publicly available geolocation data that can link the personnel with their ship
- The risks related to using outdated personal devices. Malicious code may be transferred to the workplace once connected to a corporate network
- The importance to use clean (virus, malicious code) hardware (USB sticks) and software during the initial setup or maintenance
- The impact of using unauthorized software, where no antivirus checks or authentication procedures are followed
- Securing sensitive data like user information, digital certificates, and passwords
- The importance of supervising third-party personnel and never letting them alone without proper oversight
- The importance of detecting fast and reliably a feasible cyber incident. A suspicious event like an unknown device connected to a regular working system can ring a bell. The proper way of reporting this follows the detection of such an event.
- Having a clear view of the impact that a security breach may have on the safety of the ship
- Performing regular anti-virus and anti-malware checks, taking and testing backups, performing drills on detecting and reporting cyber incidents
- Scanning removable devices from third-party personnel before connecting them to a ship's system (if such an action is permitted)

- The ones specializing in handling software for malicious code detection shall be aware of the importance and practical usage of Intrusion Detection Systems (IDS) is used.

It is essential to admit that cutting off every communication of a ship with the outside world is not feasible. Therefore, a realistic approach shall be applied on any occasion. The visitors may be technicians, authorities, agents, suppliers, etc. Some will require access to the ship's facilities, including computers, photocopiers, or an Internet connection. It is strongly advised that an isolated workstation is used to contain the risks associated with computer access to visitors. Such a workstation shall be disconnected from all the ship's networks and have a printer, Internet connection, and sockets for removable media. Ideally, this system would cover all the external personnel needs and should never be used by the ship's personnel. In the lack of such a system, we could use a dedicated system running a Virtual Machine or a Sand Box to isolate possible risks transferred from their removable media.

Commonly, the crew will bring their own devices to accompany them on their long trips. Procedures shall describe using personal devices when connected to a ship's network. This applies to connecting the crew's devices to the leisure network of the ship coming with an Internet connection. There shall be described instructions about the usage and restrictions of applications like Skype, video streaming, emails, and web browsing.

Upgrading and maintaining software is among the first recommendations from a security specialist. There is no exception in the maritime industry; however, due to their routine, ships may spend a considerable amount of time before being available to have their systems upgraded. On the other hand, some vendors stop supporting a system and provide no upgrades or patches[32]. Such circumstances threaten existing systems, turning them into a luting target for hackers. Therefore, it is paramount to establish concrete procedures for updating existing software on time. Some updates may be more critical than others and need to be applied before reaching the next port while the ship is underway. Internet connection in the middle of the ocean is far from being considered equal to wired connection speeds and is a continuous challenge for

[32] Windows XP, Vista, 7

security experts. Luckily, this gap gradually degrades due to new satellites by developing global satellite internet networks[33] and 5G networks. We shall not forget that anti-virus and anti-malware tools are software themselves, and their update lifecycle is minimal, meaning that they are updated frequently. Thus, updating these tools shall be pulled towards the top of the prioritized updates pyramid.

The same principles apply to the firmware of IT and OT onboard systems. In Chapter 8.2.2, we referred to the list of apparatus that need maintenance. Detailed instructions should be put on the devices, and the responsible person shall be aware of the frequency and the processes involved in updating their firmware and software.

Based on the ship's type, some of the IT and OT systems may be accessed remotely. In such cases, access control shall be well-documented, including who has the right to access when and which system and following procedures. Such systems shall be defined, monitored, and regularly reviewed to update the need-to-use principle. Furthermore, remotely-accessed systems shall be recorded for future reference in case of failure or discontinuity.

Whoever has more privileges than the average person is a feasible target for a malicious mind. Administrative rights shall be given consciously, recorded, monitored, and updated periodically. Only specialized and trained personnel shall grant such rights required by their role and constrained within their duties without gaining access to irrelevant fields. Consequently, administrative rights shall be removed as soon as an administrator disembarks. Administrative accounts are personal and not duties-based, meaning no two persons shall use the same account. Among other things, this security measure supports accountability and even forensics effectiveness if needed.

Strong password and multifactor authentication policies are advised to advance secrecy and access to sensitive data. According to NIST (NIST, 2017), memorizing passwords is a bad habit and should be avoided since a human cannot remember complex passwords by heart, and the ones containing actual words or phrases are prone to brute-force attacks. To prevent such attacks, CISA suggests[34]:

[33] Starlink: SpaceX's satellite internet project, https://www.space.com/spacex-starlink-satellites.html, Accessed on 7 May 2022
[34] Brute Force Attacks Conducted by Cyber Actors, https://www.cisa.gov/uscert/ncas/alerts/TA18-086A, Accessed on 7 May 2022

- Enable multifactor authentication and review its settings
- Review passwords policy based on NIST's guidelines for secure passwords
- Review IT helpdesk's procedures regarding initial passwords, password resets, and shared accounts. There is a chance that their policies do not align with the company's policy which suggests a significant security hole

On the other hand, multi-factor authentication introduces more protection layers by proving one's identity using different sources. For instance, we can use something we know (password) in conjunction with something we own (smart card) or something that identifies us (biometrics).

Removable media control is required and shall be in place due to the severe effects of importing an infected USB drive into a ship's network. Although the deactivation of USB ports is strongly advised, there are cases where an exception to the rule is mandatory. Software maintenance, especially on a major scale, requires the insertion of removable media in onboard systems. It is paramount to check such devices thoroughly with various anti-virus and anti-malware software before connecting them to the ship's device. During this thorough scan, digital signatures and watermarks will confirm that the software is also legitimate and appropriate. Whenever technically possible, trusted online repositories shall be used instead of removable media.

Finally, when we need to dispose of a system containing confidential information, we need to ensure that this data will be destroyed, leaving no room to retrieve it. Detailed procedures for destroying the collected data will avoid data leakage.

8.4 Detection Measures

Following the Cyber Risk Management Approach (Figure 7), we shall effectively detect every feasible cyber incident. An ideal implementation includes a well-defined series of alert thresholds that will ring bells when they are reached. Specialized personnel shall grant roles and tasks regarding the detection process. The more explicitly these roles are documented, the more meaningful the accountability will be when the time comes.

Companies shall consider the integration of an IDS or/and IPS into their firewall solution or as a separate system attached to their critical networks. Their ability to identify malicious threats or suspicious activity and log the data flow can prove invaluable in keeping outsiders away from internal networks and critical systems.

As already mentioned, the responsible person shall be skilled in understanding the IDS or IPS' scope, complexity, and operating parameters and be aware of the specific triggers that will alert them and call the cyber security contractor in case of an emergency.

Scanning possible threats at the network's perimeter cannot guarantee a malware-free environment. We shall expect a malware infection from time to time. To address circumstances where the malicious code has entered the network, we need to document procedures about frequently scanning the whole network using antimalware software. Good practice suggests installing anti-virus and anti-malware software on every system onboard, which will be updated regularly and run systematic scans that the working load permits throughout the day.

8.5 Contingency Plans

Contingency Plans are the next chain in the *Detect – Establish Contingency Plans – Respond and Recovery* flow. An interesting suggestion is to keep all the documented contingency plans in hard copy. This will allow the personnel to follow the procedures and take over a flawless response to cyber incidents, even in cases where the incident is so severe that the network is down or locked by ransomware. Having access to these plans is critical and can make a difference.

As stated in other parts of this thesis, the impact of a cyber incident on an IT system is generally lower than on an OT system in terms of safe navigation and safety of the ship overall. An attack on an IT system (low impact) may result in the loss or lock of data, while the downtime of an OT system (high impact) may state the personnel's health and ship's integrity at risk.

That said, disconnecting the OT systems from the shore network connection is an option, although it is luring to monitor or control such systems. This will be more

challenging as 5G[35] technology expands, and more sophisticated systems will allow remote operation from the headquarters in real-time. On the other hand, in case of incidents on an IT system, the designated person shall be available to the Master, thus raising the importance of defining the roles we described above and bringing roles separation under careful consideration. For instance, having the First Engineer be that person is not the optimum solution.

Designated personnel, both ashore and on board, are advised to be aware of the contingency plans and trained regularly to familiarize themselves with the emergency procedures and decrease the response/recovery time to regular activity.

8.6 Respond and Recover

Unfortunately, we are there! A security event has evolved into an incident, and we need to ensure the business continuity and safety of the ship. It is that time to prove that our training was thorough and precise, and we will be called to apply the contingency plans' procedures most effectively and directly.

A system will be unavailable or malfunctioning so intensively that it sets safety at stake. Before shutting this down and initiating the alternative or backup system, careful consideration regarding such a decision shall take place. Perhaps, the backup system is also infected, or this action may cause more severe effects. All possible scenarios will be included in the contingency procedures in an ideal situation, but critical thinking also plays a key role. It is not uncommon to face incidents going beyond the powers and skills of the designated personnel on board. Calling for external help from security contractors ashore is also part of the response policy.

We referred in Chapter 8.2.3 that an *omerta*[36] regarding onboard cyber incidents prevents the propagation of such cases and their handling among different organizations worldwide. However, we will see later that some cyber companies implement solutions that use data from several incidents and build databases in real-time, like the anti-virus software companies implement to keep their product updated.

[35] What is 5G and why does it matter?, https://www.verizon.com/about/our-company/5g/what-5g, Accessed on 7 May 2022
[36] Definition of 'omerta', https://www.collinsdictionary.com/dictionary/english/omerta, Accessed on 7 May 2022

NIST splits incident response into four phases[37]:

- *Preparation*. It involves preparation measures we have already mentioned like
    - establishing lists with the critical systems, and location
    - taking frequent back-ups
    - determining single points of failure and suggesting solutions to overcome them
    - creating an incident response plan and rehearsing it regularly
- *Detection and Analysis*. The designated personnel shall discover how the incident occurred, what systems and to which extent were affected, if commercial or operational data was affected, and the remaining threat to the systems.
- *Containment and Eradication*. If this is feasible, disconnecting the infected system from the network shall be our priority. Alternatively, we can quarantine the system from its physical or virtual network for as long as it is infected. Furthermore, we need to:
    - Inspect the firewall rules and correlate them with the ones that should be in place
    - Check that the anti-virus and anti-malware databases are updated
    - A full disk image of the infected system shall be taken and kept safely to support the forensics procedures and protect accountability integrity. This may be investigated later more thoroughly by cyber experts ashore. In the same context, memory dumps (RAM images) shall be taken before restarting the infected system, as this will destroy critical data for good.
- *Post-incident Recovery*. At this stage, several actions are taken to clean and recover the systems, investigate the circumstances, and take measures to prevent their reoccurrence, thus:

[37] NIST Cybersecurity Framework, https://www.nist.gov/cyberframework, Accessed on 7 May 2022

- All infected IT, and OT systems shall be cleaned and recovered to their initial state based on a documented *Recovery Plan*.
- Investigate the causes and circumstances that let the incident occur. The gained knowledge will prove invaluable for the following action.
- Prevent the reoccurrence of similar incidents by taking measures to block similar attacks. These measures may be technical or procedural, as we have already explained.

The *Recovery Plan* contains detailed procedures for recovering the infected systems to their operational state and shall be kept in hard copy in case of an emergency. Perhaps the most valuable and self-evident measure to ensure a fast recovery is taking regular backups of IT systems. This has proved an effective solution in many ransomware cases. However, as ransomware and worms get more sophisticated, they tend to affect backups too. A possible workaround is to keep the backups offline. Recovering OT systems may be more complex and need assistance from specialized technicians ashore. The responsible person's details and contact information shall be part of the *Recovery Plan*. Moreover, a data recovery policy is efficient only if a backup can be restored successfully. To make themselves ready for this critical time, the responsible person shall rehearse restoring an existing backup.

Investigating a cyber incident can help a company understand the way their system was exploited and take preventive measures to avoid similar instances from reoccurring. A detailed investigation goes beyond the required capabilities and job description requirements for sailors, and it will probably need external help from a cyber security specialist. In such cases, providing a full disk image can boost the forensics team’s work significantly. A thorough investigation can better understand the feasible cyber threats on the maritime sector and benefit all companies if shared. Good practices arise with procedural and technical measures being applied to repel similar attacks.

9 Solutions

This chapter will present the solutions proposed theoretically or implemented in the field. We will begin with short but concise guidance included in Annex 3 of the *Guidelines*, specialized for onboard networks. Then we will move forward with examining the academic proposals and practical implementations by major cyber security companies.

9.1 BIMCO's Proposals

BIMCO's *Guidelines* include a highly concise annex dedicated to the onboard networks. Nowadays, it is common to have all systems attached to one or more networks. On the contrary, standalone systems serve specific purposes, being the exception to the rule. Compromising one system, probably the weakest on the network, gives the attacker the chance to penetrate their ultimate targets, typically specific IT or OT systems.

A fundamental rule while bridging networks is preventing direct communication between controlled and uncontrolled networks. Moreover, network segmentation and traffic management, encryption protocols to encrypt transferred data, and certificates to verify the sender's identity are among the practices that can raise a steep defensive perimeter. The *whitelisting* approach is highly recommended, meaning that only the devices that need to communicate with each other over the network shall be granted access to do so.

Connecting devices like servers and routers shall be considered carefully during the network design. Networking devices, firewalls, and the cables connecting them shall be physically secured.

Every network's traffic shall be monitored by default except for leisure and entertainment (which should be totally disconnected from the other networks). The architect shall be concerned about its administration and access control during the network's design. This can be automated through relative software and/or hardware.

An excellent tool for settling new obstacles in an attacker's attempt to penetrate the network is a technique called network segmentation. In general, we expect to have

three significant networks onboard, regardless of the ship's size or purpose, that cover different requirements:

- Communication between OT systems, including data traffic, configuration, and monitoring.
- Administrative tasks on a daily routine between IT systems, like sharing files, exchanging emails, and accessing software for managing everyday tasks (cargo load, finances, etc.). Essentially, this is a standard network of an organization ashore.
- Public network used during leisure/free time by the crew and visitors, including internet access and services

As described above, network segmentation implements the *Defense in Depth* technique. Essentially, OT, IT, and public networks shall be separated logically or physically with hardware and software solutions. This does not mean that further segmentation should not be implemented. Applying segmentation for subnetworks supporting relevant functionalities like navigation and propulsion equipment makes sense.

The *Guidelines* suggest the following measures whenever affordable and applicable (Figure 15):

- A firewall is set at the perimeter between the network onboard and the internet service
- Switches between every network segment. A separate hardware switch may be set on every network to achieve an even greater security level.
- Firewalls between network segments communicating with each other
- Virtual Local Area Networks (VLANs) configured to host separate segments

Moreover, each segment shall have a separate and distinguished IP address range. Following the *whitelisting* approach, the firewalls shall deny all communications by default and grant access to wanted communication through rules. Careful consideration while designing these rules will ensure only required, and legitimate traffic is exchanged in the network keeping it both efficient and safe. In addition, all

uncontrolled networks (namely the public networks) shall not communicate with the corporate networks (IT and OT systems). Such networks shall be treated as unsafe and the most critical danger of compromising the other networks.

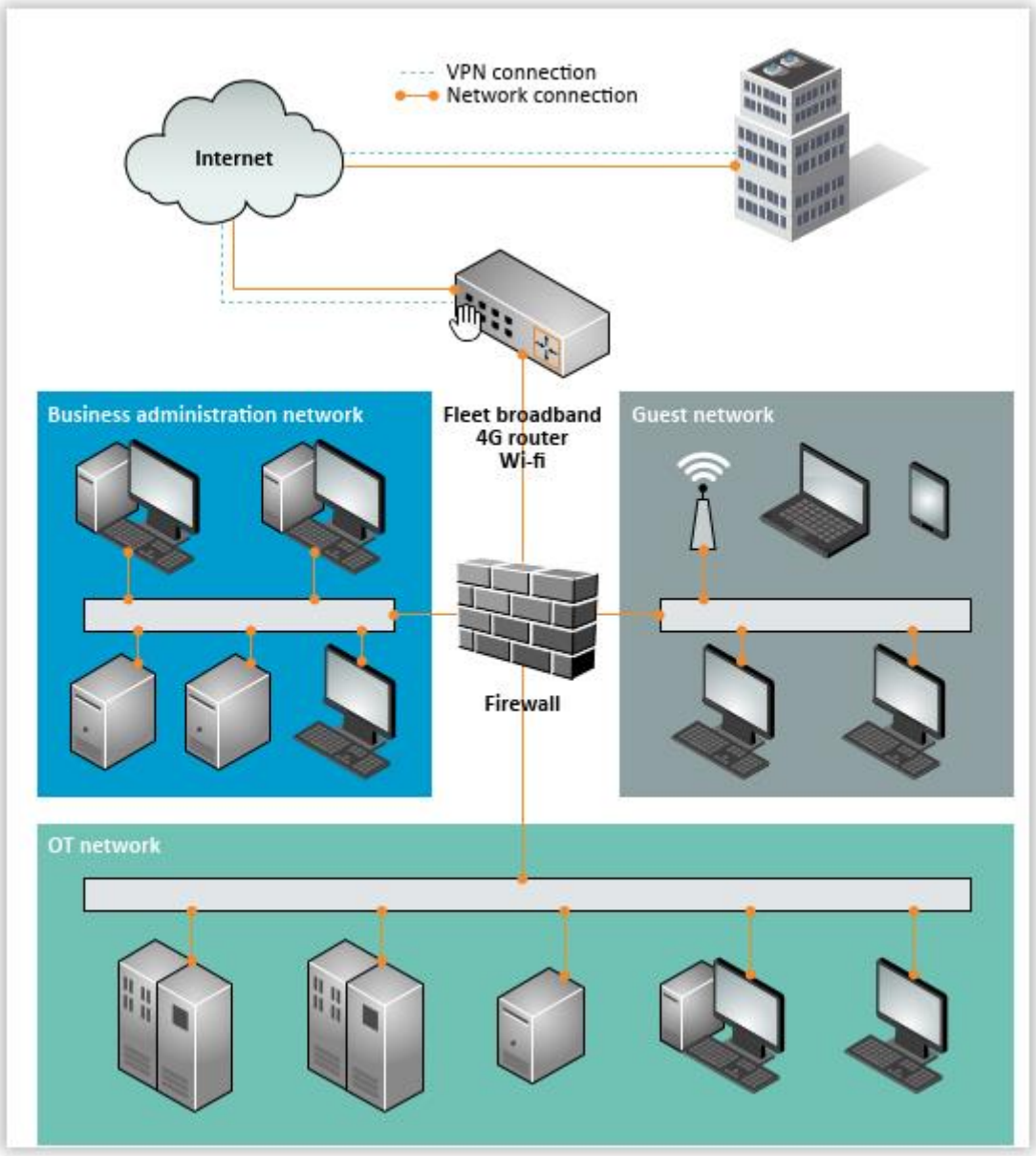

Figure 15: Indicative design of an onboard network

Apart from the proper network design and implementation, monitoring live data is a significant step towards a bullet-proof defense net. Firewalls and systems attached to each network shall log activity to detect that the hacker's specific actions can be retrieved or replicated. A properly configured IDS or IPS will inspect exchanged traffic and raise real-time alerts in suspicious content. Such a system should be placed on the segment facing the Internet, thus on the interface connecting the onboard networks

with the Internet. Another IDS/IPS should be placed behind the firewall to monitor the data exchanged between the internal networks and the Internet. Finally, a remote-access segment could also be established, like a VPN.

Are we secure? Let us imagine the following scenario. We have completed the analysis and design of our network's topology. We reserved the budget, and after a competitive procedure, we ended up with the vendor of our choice. Before selecting a single vendor or security device to secure the points we have mentioned so far, we shall be aware of an underestimated fact. Every machine is as secure as it is constantly updated, but what happens in the meantime? Or, to put it otherwise, why do they update if they are secure? The answer is obvious, to patch security holes discovered over time. A feasible attacker can exploit the device until the new patch is applied. We can add multiple protection layers that serve the defense in depth strategy to prevent this inconvenient circumstance. Placing a second firewall at the exit of the existing firewall is an excellent choice if this new system comes from another vendor. Such strategic decisions are made by critical infrastructures like banks and energy providers to ensure business continuity.

Finally, there are times that we need to run executables, new versions of programs, or new applications. An isolated system shall be used to run executables solely isolated from the network. Alternatively, a Virtual Machine can be used inside our system. Keeping the executable's impact inside a sandbox will ensure that a limited number of resources is occupied and the daily routines are not disturbed. More importantly, malicious or malfunctioning code will have no way to reach critical IT and OT systems.

9.2 Academic Proposals

This chapter will dive into bibliographic references trying to translate the BIMCO's *Guidelines* into specific actions and initiatives. Due to the vessels' diversity and complexity, following a universal approach is not a viable solution. Most researchers address a single countermeasures pillar like staff education or network segmentation. On the other hand, Kechagias, et al. suggest a holistic approach targeting procedures, humans, and technology. Finally, Goudossis, et al. argue that we must use novel

security models and metrics to assess the onboard networks and construct the defensive mechanisms based on real-case scenarios.

9.2.1 Strengthening the Defensive Net

Recent independent research papers indicate the lack of the required awareness regarding cyber security matters. One of them queried maritime professionals and revealed that 75% of the participants showed a lack of knowledge about cyber risks (J.I. Alcaide, R.G. Llave, 2020). Thus, it is mandatory to increase the learning levels in maritime cybersecurity and change the mistaken belief that technological systems can solely address cyber-attacks. A shift in mindset is strongly suggested to assign resources to mitigate cybersecurity threats (A. Androjna, T. Brcko, I. Pavic, H. Greidanus, 2020). Alcaide's research brought to the surface another disturbing truth, the significant gap between the practices of actors in the maritime industry and the vulnerability of systems.

Pseytelis suggests a straightforward training process leading to a recognized certification in the maritime industry (Pseytelis, 2021). The process would require the attendance of specific educational curriculums. The candidate would be trained in cybersecurity awareness and daily tasks, security policies, and countermeasures. After completing these training sessions, they would sit on exams conducted by a certified company.

It is worth mentioning that most ships have an age of 20 years on average. Let us consider the cyber threats 20 years back. Although fully functional and reliable, we will identify why their OT systems are considered outdated in terms of cyber countermeasures. Thus, apart from the cyberculture that we need to build gradually, the maritime sector needs to apply upgraded, more secure, cyber-proof IT and OT systems.

Many researchers have focused their work on identifying the cyber threats against ports or sea terminals. However, they agree that these are just a node in the supply chain and that vessels play a crucial part in delivering goods. Consequently, their recommendations regarding the proposed solutions in mitigating vulnerabilities can also be expanded to the sea carriers.

Beacmont and Polemi (Beaumont, 2018), (Polemi, 2017) based their research on NIST's and BIMCO's Identify-Protect-Detect-Respond & Recover action framework and proposed that ports shall adopt a series of actions:

- Identify the gaps and vulnerabilities in the supply chain, including ports and vessels
- Identify port threat scenarios and analyze the feasible impact on the rest supply chain's components
- Conduct a risk assessment
- Apply preventive countermeasures to protect their assets against cyber threats
- Carry out periodic updates and audits on those measures
- Develop contingency and recovery plans after cyber incidents

Moreover, Dingeldey suggests strong passwords, regular updates in operating systems, resilience drills, secure satellite connections, information sharing, and employee awareness (Dingeldey, 2022). Furthermore, he puts the human factor in a vital position to defend against cyber-attacks. Most of them are suggested by many specialists and researchers. On the other hand, information sharing implies that information is not shared, and that's true.

Until recently, the *omerta* regarding sharing data breaches in the maritime sector has allowed cybercriminals to act with less hesitation and, in a way, out of control. When company A suffered a ransomware attack, it kept it internally, fearing the collateral damages that it would cause. This tactic left the rest maritime companies in the dark and gave the attacker the chance to use the same hacking tools to compromise the next company. Zarzuelo, et al. claim that cybersecurity and trust in sharing information in the maritime super competitive world are the main barriers to taking off the game-changing technologies such as blockchain, AI, and 5G, to name a few (I.P. Zarzueloa, M.J.F. Soeanea, B.L. Bermúdez, 2020). Androijna, et al. argue that a company under attack should share this information confidently with other companies in the maritime sector (A. Androjna, T. Brcko, I. Pavic, H. Greidanus, 2020).

During the last few years, these old habits seem to change with governmental and commercial cyber solutions keeping an updated and shareable database of maritime

attacks that act preventively and tackle similar attacks. In the port of Amsterdam, a cyber hotline was established, and the Cyber Resilient North Sea Canal Area (CYREN) network was used to collect and share critical information about cyber threats with its collaborated companies[38]. Similarly, the EU developed a Common Information Sharing Environment (CISE) for the maritime domain aiming to strengthen the proactive cyber security in EU countries' facilities and vessels (J. Rajamäki, I. Tikanmäki, J. Räsänen, 2019).

Androijna, et al. suggest making the GNSS signals more immune to spoofing, jamming, and other malicious techniques. These signals are used from navigation systems onboard and are paramount in ensuring safe navigation at sea, especially in the proximity of navigation treats and land formations. Androijna, et al. argue the need to use public and private GNSS arrays in the logic of a blockchain network, propagate encrypted signals on the air, and intelligent processing on the receiver's side (A. Androjna, T. Brcko, I. Pavic, H. Greidanus, 2020). They pay attention to applying encryption and authentication methods in terrestrial signals. At the same time, a relatively advanced, still feasible measure could be the harbor's laser-based aid system for birthing and docking. Such laser-based systems are used in some airports worldwide to make aircrafts land more safely under severe weather conditions[39].

9.2.2 Cybersecurity Systemic Approach

Overall, to build and maintain an efficient defensive net against all feasible cyber threats, a systemic approach is recommended, an effort that will apply the cybersecurity cycle in a vast organization like a maritime company, an approach that will address every single aspect that may lead to a breach.

Such a Cybersecurity Systemic Approach is advised by Kechagias, et al. (E.P. Kechagias, G.Chatzistelios, G.A. Papadopoulos, P. Apostolou, 2022). This proposal assumes that integrating cybersecurity policies into existing operational procedures is a core element. Safety and security have traditionally been the core elements in

[38] New cyber programme for Port of Amsterdam, https://smartmaritimenetwork.com/2019/01/30/new-cyber-programme-for-port-of-amsterdam/
[39] Russia Presented New Laser Aircraft Landing System, https://mil.today/2019/Science11/, Retrieved on May 1, 2022

maritime policies and procedures described in a unified entity called Integrated Management System (IMS). Each shipping company publishes and updates documented procedures and policies aligned with maritime regulations such as IMO. Recently, IMO included cyber security procedures as part of an ongoing effort to protect the ship's assets, systems, and data.

The shipping company must apply a Plan-Do-Check-Act (PDCA) cycle for the management system to achieve the desired results in the long term. Such an approach will ensure that cyber safety remains updated and efficient. Let us mention that BIMCO assigns a significant portion in their *Guidelines* on this cycle. The systemic approach suggests the following actions in each of the four steps:

- *Plan*: The shipping company identifies the cybersecurity objectives for their offices and vessels, publishes an inventory of systems (hardware) and software, executes a cyber risk assessment, and sets cybersecurity Key Performance Indicators (KPIs) to measure the effectiveness of the applied countermeasures.

- *Do*: The company establishes the policy and procedures regarding cybersecurity, such as Cyber Security Plan and Cyber Security Policy. These high-level documents shall be propagated from top management downwards. In this stage, the roles and responsibilities are defined explicitly within every job description, providing a clear image of the company's expectations from the employee occupying the position. Moreover, cybersecurity training is developed and performed, while official forms and checklists are defined to be fulfilled in cyber events or incidents. A Security Operations Center (SOC) monitors the corporate systems 24/7 and can handle cyber reports sent from the vessels.

- *Check*: At this stage, we must evaluate the effectiveness of the applied countermeasures and how their performance permits the top-level objectives accomplishments. This is where the KPIs established in the Plan stage are evaluated. A special team analyzes the incidents and reports regarding cyber events and incidents and updates the identified risks and threats. Finally, a designated and specialized group of employees will perform internal audits

about cybersecurity matters. An external party (cybersecurity consultors) can also help in auditing and should be included whenever affordable.

- *Act*: In this final stage, before starting a new iteration in the PCDA cycle, we've got all the required products from the Check phase to define the Lessons Learned. We have gained a deep, valuable knowledge of what went wrong and what proved correct that will direct the corrective and preventive actions we need to apply. A key success factor is the commitment level of top management on this course and the strong will for ongoing improvement, a strive not only documented in the relative cybersecurity documents but also proved in the field by allocating the adequate resources and requiring the subordinates to embrace the company's vision and expectations.

The Cybersecurity Systemic Approach highlights the importance of a detailed risk assessment and suggests the well-known ISO 27005 assessment. It also bases the Cyber Security program on three pillars: procedures, humans, and technology. Productive collaboration is required among these pillars to ensure a successful implementation. The cybersecurity policy and procedures are described in the IMS, while the personnel and the technical controls strive to implement them.

Procedures and policy constitute the first pillar, and timely speaking should be addressed first. As already mentioned, IMS is the central documentation system that holds all the documented procedures and policies for the company's assets (ashore and vessels) required from the maritime organizations and national or international authorities regarding safety. A new chapter about cybersecurity was recently added to the IMS document consisting of three main sections: Cyber Security Policy Statement, Cyber Security Plan, and Procedure Manuals.

As its name implies, Cyber Security Policy Statement is an abstract high-level policy depicting the vision of the company's owners regarding cyber security and their commitment to safeguarding the company's assets by assigning the required resources.

Cyber Security Plan (CSP) describes the steps to secure the company's assets against cyber threats. This is the document where one can find the definition of cybersecurity objectives, the required and prohibited activities, duties, responsibilities,

threats combined with vulnerabilities, the adopted countermeasures, the Contingency & Incident Response Plan, and the Cybersecurity Incident Analysis procedure.

Procedure Manuals describe the related actions that the crew should take regularly and in an emergency. Representative manuals are the following: *Information Technology and Data Control* (establishing user accounts, access control, backup actions, training, and more), *Software Management* (updates and upgrades in installed software, data backup, new software acquisition, and testing), *Forms* indicating lists of installed hardware or software. The proposed and self-explanatory forms are as follows: *Office IT Infrastructure Inventory*, *Office IT Software Register*, *Vessel IT Infrastructure Inventory*, *Vessel OT Infrastructure Inventory, IT/OT Software Update Form, Software Evaluation, Cyber Security Incident Evaluation, Antivirus Update / Scan Form, PC Inspection Form, IT Training Form, Back-Up Monitoring Form,* and *Password Change Monitoring Form*. Finally, a widely known range of related policies shall be accessible regarding the following areas: Personal computer, Backup, Email, Third-party access, Software Installation, User Accounts Control and User Access Management, Password, Removable Media, and finally, the Bring Your Own Device Policy (BYOD).

To support the human pillar, the company assigns qualified personnel both ashore and on board the vessels, properly trained through training programs to address daily routines and sudden incidents. All ships are equipped with cybersecurity e-learning software, and all onboard personnel attends seminars and sends their scores to the head office, where decisions are made about corrective measures. Training seminars on cyber content are scheduled and conducted monthly. New crew members are obliged to review and get familiar with the company's cybersecurity policy. Officers in the shore-based premises will attend seminars every two years (in-house seminars) or every year for foreign officers. Awareness and training are further reinforced by a certified third party that will conduct regular cybersecurity training seminars for the company's entire personnel, both ashore and onboard. Specifically for software usage, there must be an established Training Policy that will guide the designated personnel to operate the IT and OT systems effectively and securely. Finally, cybersecurity drills will regularly simulate actual attacks and realistic scenarios. These drills will stimulate

and trigger the crew's responses according to the existing contingency plans, build the crew's confidence and familiarity, and prove the training program's efficiency overall.

Technology is the third and last pillar of the systemic approach. Each shipping company shall select from a long list of available technical countermeasures enlisted in email technical infrastructure, corporate network, and remote working laptops.

The company shall apply anti-spamming, antivirus, and antimalware software centrally implemented in three levels: network perimeter, email server, and email client to protect the email technical infrastructure. Strong passwords and multi-factor authentication are also used. Finally, the system will perform URL filtering and HTTP proxy filtering on the perimeter allowing only the whitelisted sites according to the company's policy.

In the corporate network, it implements physical security, network segmentation, firewalls, Access Control Lists (ACLs), Multi-Factor Authentication (MFA), IPS/IDS, Endpoint Security Protection (ESP), secure software design and configuration, intime software updates and patches, scanning and patching of discovered vulnerabilities, Data Loss Prevention (DLP) systems, data encryption, Security Information and Event Management (SIEM), SOC, sandblast/sandboxes to run applications in a virtual environment, regular backups on all servers.

Lastly, to address the advanced risks of remote working laptops, the company shall implement additional safeguards: a VPN, hard disk drive encryption, endpoint detection, and report domain policy (forcing each system to be a member of a domain).

Additionally, developing cyberculture is a real long-term challenge. Kechagias et al. suggest a great variety of supportive actions, parts of a cyber security campaign, that can set the solid foundations. Indicatively:

- Post a printed copy of (inside brackets the recommended place/position):
    - BYOD policy [every cabin of the ship]
    - Cyber Security Response Plan and Immediate actions after a cyber security incident [public places (smoking places, bridge, ECR)]
    - Signs indicating a cybersecurity breach [public places]

- Instructions about using personal devices onboard [public places and every cabin]
- Required Actions (DOs) and Prohibited Actions (DONTs) [every cabin, also a copy given to every new crewmember or visitor]
- Cybersecurity Posters [accommodation rooms]

- Have a positive control over which systems should have USB access and restrict USB usage to only dedicated and recorded systems, especially by visitors.
- Ensure that the antivirus software gets updated at regular intervals in all onboard systems.
- Review the company's videos and interactive material regarding:
  - cybersecurity general training material aimed at non-technical personnel. Indicative material should address passwords, safe browsing, social media, and phishing issues.
  - Fleet or circular interoffice instructions about computer data security to learn the best practices in protecting ship's data from malicious or accidental loss or damage.
  - Backup instructions.
  - Disaster/Recovery instructions in case of emergencies related to IT systems' damage or failure.

9.2.3 Reassessing maritime vessels' networks

Undoubtedly, protecting the onboard networks shall be among the prioritized and critical actions to be taken by the vessel's owners. Significant organizations have published guidelines and standards implying or highlighting the required countermeasures. However, not much research has been conducted on quantitative and automated cybersecurity modeling for networks operating on the vessels (M. Caprolu, R.D. Pietro, S. Raponi, S. Sciancalepore, P. Tedeschi, 2020).

Nowadays, the best methods used to model and assess cybersecurity risks focus on IoT networks, cloud networks, etc.; Although these methods pay back at facilities onshore, they seem to be insufficient to address the advanced requirements in onboard networks, raised by the interoperability and need for cooperation among OT and IT systems, two system categories that have been working independently for many years (K. Tam, K. Jones, 2019). Also, the current cybersecurity assessment methods use risks for physical and human factors rather than the onboard systems' security modeling and analysis.

Researchers have tried to assess onboard network security risks by isolating their focus on specific topics rather than proposing a holistic approach. Svilicic, et al. (B. Svilicic, I. Rudan, A. Jugovic, D. Zec, 2019) focused on threats against the Integrated Navigation Systems (INS) using the well-known vulnerability scanner Nessus (Professional version 8.0.1) and qualitative metrics to measure the impact of an executed treat. Similarly, Svilicic, et al. (B. Svilicic, D. Brčić, S. Žuški, D. Kalebić, 2019) used Nessus to quantify the threats raised by the usage of ECDIS.

Sahay, et al. (R. Sahay, W. Meng, E. Sepúlveda, A. Daniel, C.D. Jensen, M.B. Barfod, 2019) proposed automatic defense enforcement for ship's IoT devices against attacks executed in the communication network. They based their proposal on a Software-Defined Networking (SDN) architecture that allows crew members with limited security experience to establish security policies that can be interpreted to low-level *OpenFlow* rules[40] , and the used framework relies on multipath routing, thus raising the resilience against Distributed Denial of Service (DDoS)[41] attacks.

Goudossis, et al. (A. Goudossis, S.K. Katsikas, 2019) examined how identity-based public and symmetric cryptography might strengthen the Automated Identification Systems (AIS) against intentional collision attacks.

All the above research works isolate a system and examine vulnerabilities, like being in a sandbox. On the contrary, Enoch, et.al. proposed the *Maritime Vessel-Hierarchical Attack Representation Model (MV-HARM)*, an innovative graphical security model

[40] OpenFlow Rules Interactions: Definition and Detection, https://ieeexplore.ieee.org/document/6702547?arnumber=6702547, Accessed on April 30, 2022
[41] What is a DDoS Attack? - DDoS Meaning, https://www.kaspersky.com/resource-center/threats/ddos-attacks, Accessed on 30 April 2022

(S.Y. Enoch, J.S. Lee, D.S. Kim, 2021). *MV-HARM* assesses the cybersecurity level on vessels considering a complete maritime vessel network. The researchers split their work into five specific steps:

- Develop an MV-HARM to capture security components (systems, running routines, connections, open ports, vulnerabilities, and events). MV-HARM consists of two layers:
    - *Upper Layer*: systems and the relationships between these systems and their reachability
    - *Lower Layer*: system's vulnerabilities using Attack Trees (AT)
- Use explicitly defined security metrics to measure the impact of attacks precisely. The metrics are split into node-level, attack path-level, and network-level. The node-level metrics are calculated based on the MV-HARM's Lower Layer, while attack path and network metrics are based on the Upper Layer.
- Assess the onboard network based on single or multiple function(s) as attack goals. An attacker may need to compromise a series of nodes before running their main attack; thus, understanding the threat is vital. The researchers used the *STRIDE* model to quantify the threat weight values under six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privilege.
- Use fictional attack trees-event-based scenarios to perform the vessel's analysis. Based on the existing systems, we can list the known vulnerabilities manually or with the help of automated tools like *OpenVAS* and *Nmap*. An attacker may use different approaches to reach their goal, thus paths based on the network configuration. Some require AND logical functions, while others require OR logical operations using alternative paths (Figure 17).
- Compare and evaluate the countermeasures' effectiveness against different attack scenarios. The value of this final step depends on how precisely we have captured the values in the previous steps that will help in determining the probability and the impact of each attack. The meticulous evaluation will highlight the countermeasures required to harden the network.

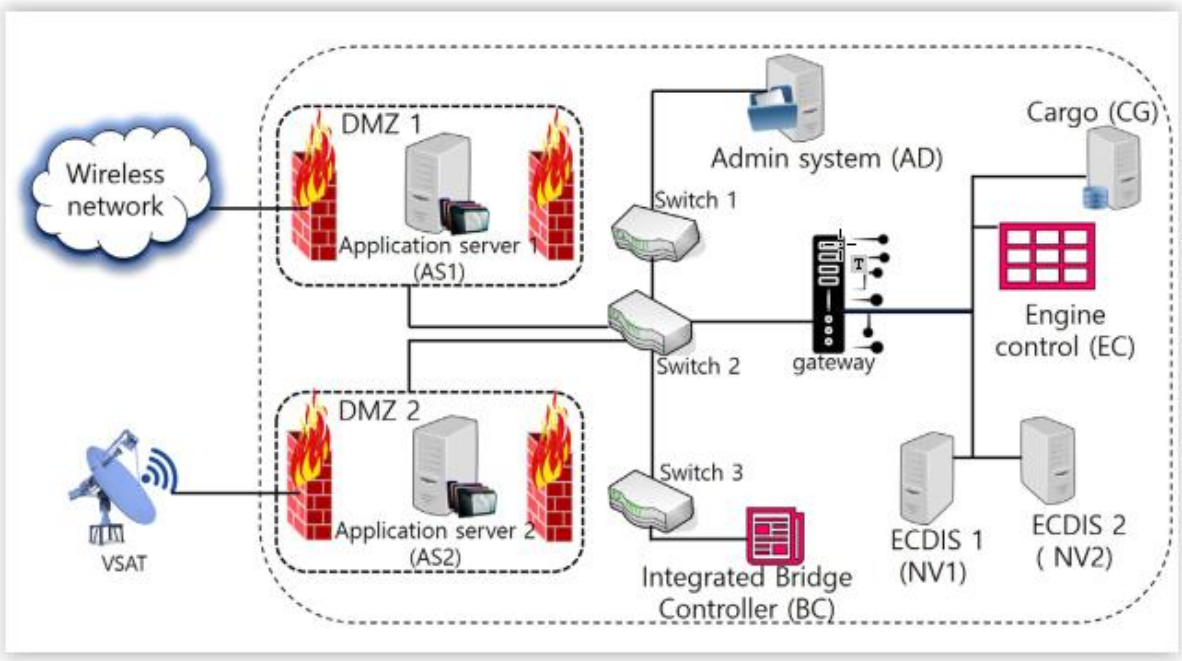

Figure 16: Typical maritime vessel network

Once the countermeasures are applied, the simulation process runs again. We end up with a new evaluation where we spot the differences against the previous state and conclude the measures' effectiveness. Generally, network segmentation (separation) implemented physically, logically, or using both techniques is one of the best countermeasures proposed by the research.

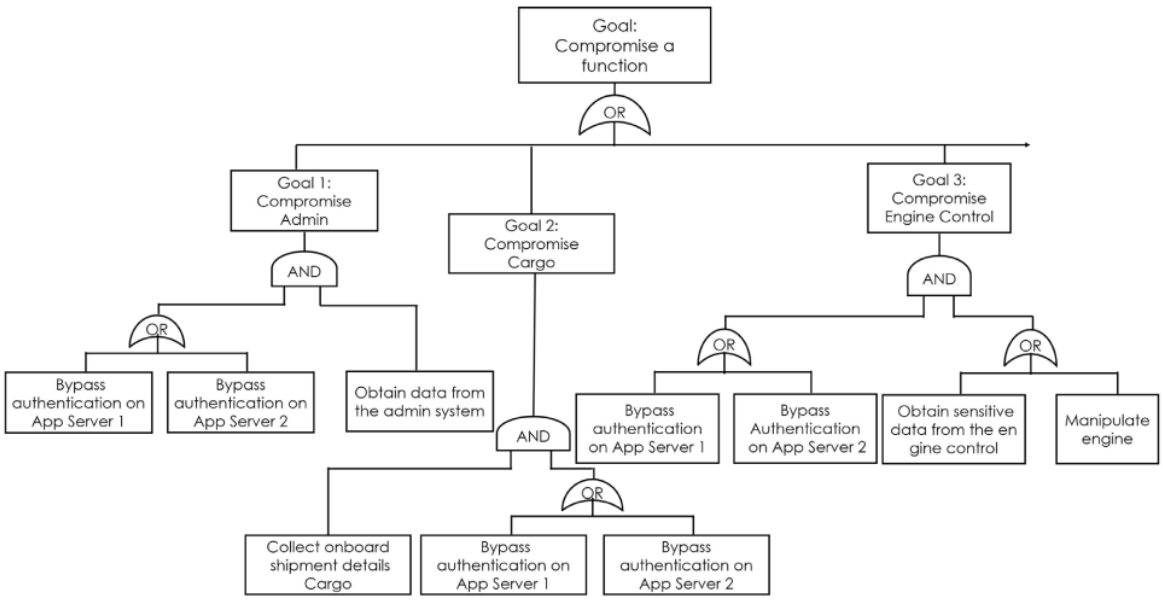

Figure 17: Feasible attack goals

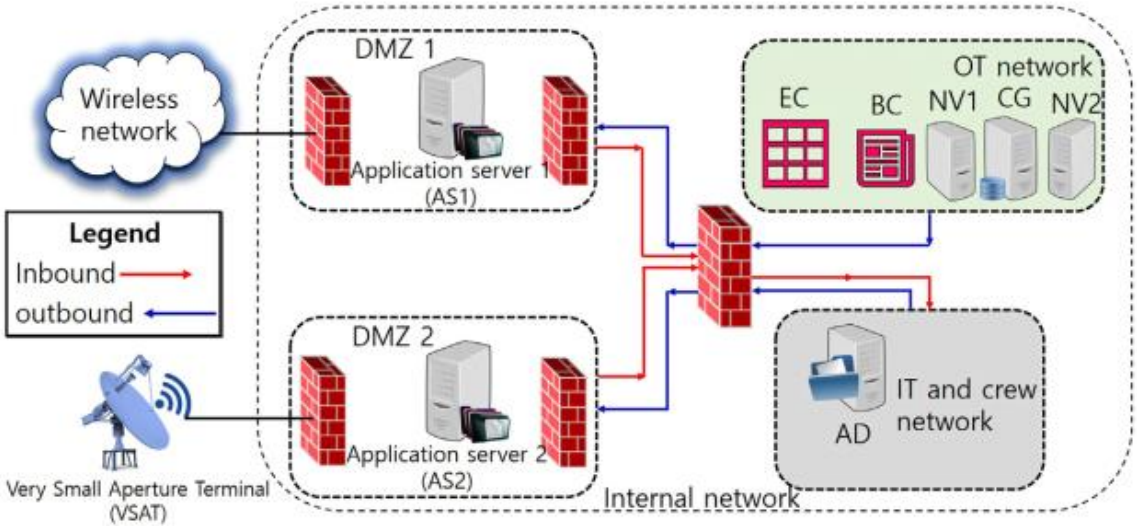

Figure 18: Network separation

If implemented carefully, the MV-HARM can discover potential attack paths in an onboard network, assess the security at different levels, evaluate the severity of each attack path, and propose effective defense measures based on probability and severity. The ship's Security Officer could use MV-HARM to identify potential risks and deploy defensive mechanisms effectively.

9.3 Solutions in the field

Cyber security companies have interpreted the BIMCO guidance in the maritime sector, moving from the theoretical to the practical implementation, were among the most exciting sections of the current thesis, and I was looking forward to running through. However, it became a real challenge to gather the required information since many cybersecurity vendors would not share their knowledge with me.

We contacted several companies, discussed their main concerns with their representatives, reached their available solutions on their sites, and attended webinars regarding cyber safety. This would present a spherical and representative road through how cybersecurity consultants have interpreted BIMCO's directives in real-world cases.

The vendors that agreed to share their experience implementing the BIMCO's guidelines on real maritime platforms have considerably contributed to this thesis' scope. They all agreed that not all naval industries show the same interest in securing

their ships against cyber-attacks. The ones willing to apply cybersecurity practices in their vessels are primarily seagoing shipping owing LPG (Liquified Natural Gas) and CNG (Compressed Natural Gas) carriers and tankers. Naturally, their extreme interest is driven by the explosive cargo of their vessels.

Still highly interested, but not that conscious, seem to be container ships due to their ever-growing cost, especially during the last couple of years of the pandemic.

9.3.1 Cisco

Cisco, founded in 1984 by Len Bosack and Sandy Lerner[42], is one of the leading suppliers of networking devices and communication solutions worldwide. The company offers solutions and consultation to maritime companies seeking to secure their ships against cyber-attacks. For the time being, the maritime companies being more worried about these attacks seem to be owing LPG ships, transferring liquified natural gas, oil tankers, and container ships.

Not surprisingly, Cisco sets firewalls usage and network segmentation as their top recommendations. Firewalls have become an essential component of every corporate network and range from free open-source (*iptables*) or low-cost solutions to more advanced and expensive options such as the Next-Generation Firewall (NGFW)[43]. A traditional firewall provides continuous network traffic inspection and allows or blocks data packets based on the configured rules that identify state, port, and protocols. An NGFW includes these capabilities, and it integrates intrusion prevention, blocks risky applications, contains sources about threat intelligence, absorbs the latest information feeds to upgrade paths, and combines methods to secure the network against evolving security threats.

As a leader in networking devices for the last few decades, the company focuses on network segmentation as a top priority countermeasure in keeping intruders outside. Thus, LAN's segmentation is implemented through hardware (top priority) with routers and switches, and VLANs.

[42] Cisco overview, https://newsroom.cisco.com/c/r/newsroom/en/us/company.html, Accessed on 7 May 2022
[43] What is a next-generation firewall?, https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html, Accessed on 11 May 2022

ENISA has assessed ransomware as the prime threat for 2020-2021 (ENISA THREAT LANDSCAPE 2021, 2021). The maritime industry is considered a high-value target for malicious attackers that require a ransom to unlock data or systems they have previously compromised. To repel such attacks, the integration of reliable antivirus software is of the essence. Such software shall be installed in all the systems connected to the network and follow a solid update policy that will make it offer the best protection.

Integrating an Endpoint Detection and Response (EDR)[44] is also highly recommended. EDR detects threats affecting the network's devices by examining their entire lifecycle. It highlights crucial metrics and gives answers to reasonable questions like *"what happened*," "*how it got inside*," "*in which places it was detected,*" and "*what it did*." Gathering the answers to the previous questions, EDR ends up with actions that may contain a threat at the endpoint and not let it spread to the other systems.

Cisco also suggests using IDS/IPS systems wherever applicable as part of a unified security solution. Such systems accompany NGFWs.

From Cisco's perspective, some of the most frequently identified issues are the dangerous practice of running old and updated systems, not being supported for years, like the Windows XP operating system on PCs. Microsoft has stopped supporting these systems, and a quick look at relative security sites will reveal how many exploits there are for such systems. Thus, upgrading these systems to newer and more secure Operating Systems (OS) is mandatory.

The lack of authentication procedures is another central security hole spotted by the company. Several methods could be established to address this, such as 802.1x authentication[45] and Two-Factor Authentication[46].

Cisco has identified the need for remote working on some of the systems in ships moving worldwide. In such cases, the traffic shall be encrypted with a robust protocol.

[44] What Is Endpoint Detection and Response (EDR)?, https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html, Accessed on 11 May 2022
[45] 802.1X: Port-Based Network Access Control, https://1.ieee802.org/security/802-1x/, Accessed on 8 May 2022
[46] What Is Two-Factor Authentication?, https://www.cisco.com/c/en/us/products/security/what-is-two-factor-authentication.html, Accessed on 8 May 2022

Most end users' devices are PCs, and the same goes with corporate devices onboard. To connect remotely to such a system, one will use the Remote Desktop Protocol (RDP)[47] , which is encapsulated in the TCP layer of the OSI model. RDP connects the Terminal Server and the Terminal Server Client and makes remote working possible through easy steps, but raises a significant risk that can be contained if strong encryption like Internet Protocol Security (IP/Sec)[48] is used.

Regarding the allowance or blockage in the applications level of the OSI model, Cisco suggests the whitelisting approach as mentioned above against the blacklisting approach required by the *need to have* doctrine.

9.3.2 Navarino

Navarino[49] is one of the biggest companies in the world that specializes in developing innovative IT solutions for more than 550 companies in the maritime industry.

Figure 19: Navarino Infinity

Their suggestion for the maritime industry converges to two solutions, *Infinity*[50]and *Angel*[51]. Started as a gateway, under development for the last 12 years, *Infinity* integrates an IPS system, thus not only detects but acts too.

Low satellite communication bandwidth between ships and ashore is a big challenge compared to the high-speed internet that most companies use in the civilized world.

[47] Understanding the Remote Desktop Protocol (RDP), https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol
[48] IPsec (Internet Protocol Security), https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security, Accessed on 8 May 2022
[49] About Navarino, https://www.navarino.co.uk/about-navarino/, Accessed on 8 May 2022
[50] Infinity, https://www.navarino.co.uk/infinity-new-category-2/, Accessed on 11 May 2022
[51] Angel, https://www.navarino.co.uk/portfolio/what-is-angel/, Accessed on 11 May 2022

Infinity filters data gathered through its IPS activity converts it into compressed text, and sends it to the facilities ashore to overcome this significant obstacle.

IPS systems, like other security systems, base their functionality and efficiency on the quality of their signatures database. Therefore, before the compressed text arrives at its destination, it goes through a Security Configuration Management (SecCM)[52] inland facilities using AI to detect security events. If such an event is detected, the SecCM triggers a security alert to the SOC to create a new signature and propagate it to the ship and other recipients to keep their signature databases updated. A portal gathers the signature updates and sends them as a compressed file to the ship whenever needed to minimize the data transferred to the ship to a minimum degree. The ship's *Infinity* instance receives the file, decompresses it, and pushes the new signatures into its database. A typical exchanged data size ranges from 500 to 700 MB per month. In case of a malicious attack, the IPS sends the suspicious traffic ashore for analysis, expanding the size mentioned above considerably above 1 GB. The onboard IPS suspends the suspicious traffic while waiting for the analysis results, thus containing the adverse contamination effects.

During the network design, the company engages ethical hackers to detect security holes by penetrating targeted systems. They strongly advise the maritime companies to keep their crew and business networks separated and to use VLANs on every distinguished IT/OT network. It is not uncommon that critical OT systems like an electrical plant or the main engine may have different manufacturers. At the same time, these systems interfere with each other as part of their regular activity, and their physical separation is not a feasible option. Moreover, their proximity may detect the usage of a single data cable in transferring communication and control signals. VLANs overcome this overwhelming obstacle of isolating different OT systems logically when physical boundaries cannot be applied.

Establishing a secure network by design is the first and more critical link in the security chain. However, its effectiveness will demolish if the human factor acts recklessly. Educating sailors in essential cyber security matters strengthens the existing

[52] The management and control of configurations for an information system to enable security and facilitate the management of risk, https://csrc.nist.gov/glossary/term/security_configuration_management, Accessed on 11 May 2022

defensive mechanisms and ensures their future durability. Handling incoming emails containing attachments or web links and avoiding inserting USB flash drives in systems onboard are among those cornerstone aspects that build strong security awareness.

Angel, the company's premium package, integrates *Infinity* and includes more advanced and sophisticated operations. A detailed, still concise guide on the technical implementation of *Infinity* can be found in *Annex B*.

9.3.3 Sophos

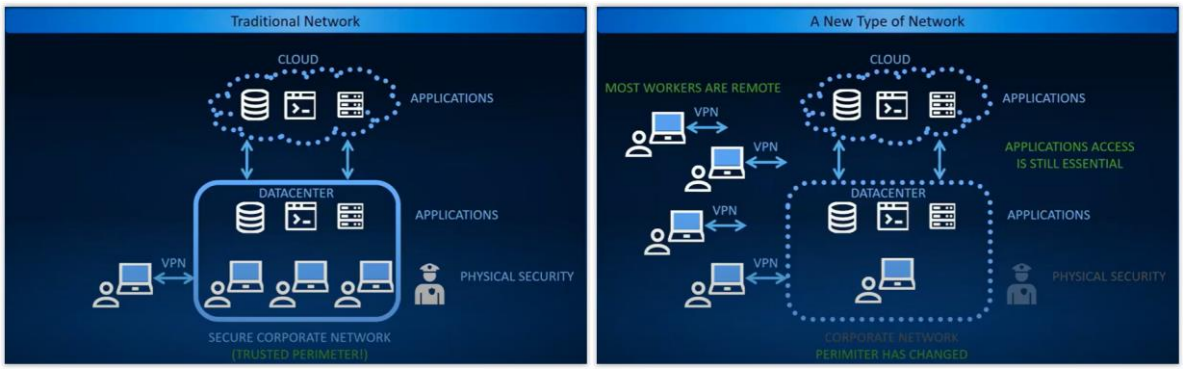

Figure 20: Traditional vs. new types of networks

The status quo in the working field has been transforming dramatically during the last couple of years. During the pandemic, the numbers of remote workers raised significantly, while these days, working from home for several days a week is not uncommon any more. Many say these working habits are here to stay and will be the mainstream basis for the next few years[53]. Since more employees access the corporate resources from a distance, using untrusted networks like the Internet, security companies like Sophos have identified the need to implement a more secure communications tube between their premises and their employees' residences. This has led to the adoption of a VPN. Due to the turn having happened forcibly (pandemic), we have seen an enormous growth of VPN services[54].

[53] Communication Technology and Inclusion Will Shape the Future of Remote Work, https://www.businessnewsdaily.com/8156-future-of-remote-work.html, Accessed on 8 May 2022
[54] The VPN Market in 2022, https://www.datamation.com/security/vpn-market/#:~:text=The%20global%20VPN%20market%20was,end%20of%20the%20forecast%20period., Accessed on 8 May 2022

The challenges focus on securing the data that is now spread through different places, the corporate data center, the cloud servers, and locally the personal devices. But not only that. Backing up data and synchronization issues are also critical matters.

To make the transferred data as secure as possible, a VPN seemed like a one-way road until recently. VPNs are ideal for hiding the data transmitted from one place to another, but what is really transferred can be monitored and filtered by other solutions, like firewalls, IDS, and IPS.

Sophos suggests the Zero Trust Network Access (ZTNA), a concept that will accompany us more and more. This notion involves three core components, *User Verification*, *Devices Validation,* and *Access Control*, as seen in the following figure. Essentially, ZTNA implements the onion's directives for *Security in Depth* we mentioned above. ZTNA applies security layers, one after another, to harden the actual data segments from being compromised. Thus, it runs an identification process both on the user and their device level before giving them access to the application level. Having passed the identity and device verification process successfully gives them the chance to reach the final checkpoint. At the access control level, they are granted access based on the access control policy of their corporation.

Figure 21: Zero Trust Network Access

It's inevitable of thinking the remote workers as moving platforms, like ships moving around the globe. It's not far from the reality since a *telecommuter*[55] may work while moving by train, a self-driven Tesla car, and why not, while onboard a ship. The Zero Trust Network's architecture can play a crucial role in designing future communication channels between onshore facilities and vessels.

9.3.4 Beyond Trust

BeyondTrust[56] has also identified the expanding need for telecommuting and the emerging need to apply more security layers to corporate data. The company suggests *Privileged Remote Access*[57] to interact with remote privileged access sessions regarding security, management, and auditing.

Privileged Remote Access substitutes the VPN connectivity and overcomes the *all-or-nothing* approach. A VPN has not had the tools to manage the traffic and can accept or drop the exchanged data packets. Instead, the users have access only to the systems they should see based on the Privileged Access Management (PAM)[58], and their activity is monitored and controlled. Two security layers are applied to Access Control and Application Sessions, respectively.

The administrator may give a registered user access to only the required tools to perform their tasks. For instance, a Windows PC data clerk may be granted access only to the Microsoft Office suite to perform their functions. Consider the case that the data clerk works from home every Monday. When they log in to the corporate PC on Monday morning, they will gain access only to the MS Office applications like Excel, Word, and Outlook. Moreover, they will use MS Teams to speak and coordinate with their director and other staff members. They won't even see the other Windows options, only a minimalistic desktop with shortcuts for the mentioned apps. The

[55] someone who works at home and communicates with his or her office by phone, email, or internet, https://dictionary.cambridge.org/dictionary/english/telecommuter, Accessed on 11 May 2022
[56] BeyondTrust, https://www.beyondtrust.com/, Accessed on 8 May 2022
[57] Privileged Remote Access, https://www.beyondtrust.com/remote-access, Accessed on 11 May 2022
[58] an information security (infosec) mechanism that safeguards identities with special access or capabilities beyond regular users. Like all other infosec solutions, PAM works through a combination of people, processes, and technology, https://www.onelogin.com/learn/privileged-access-management#:~:text=Privileged%20Access%20Management%20(PAM)%20is,people%2C%20processes%2C%20and%20technology., Accessed on 11 May 2022

administrator can even apply a time limit for each session to minimize a possible misuse of corporate resources or avoid the risk exposure. In another case scenario, we want to give view-only access to a feasible new contractor for our company. In this case, the administrator will minimize their access to a Linux system or a PC to view only a series of presentations regarding our company without the right to alter anything.

In terms of the network's topology, the software needs to be installed at the entry point between the users and the corporate network. An external firewall is also located to control the traffic between untrusted (Internet) and trusted networks (corporate). What is installed is a so-called *Jump Server* that acts like a *Pivot Server* used by the users' devices when trying to get access to the corporate resources, including systems and data. Thus, a *Jump Server* shall be installed at the entry point of every network.

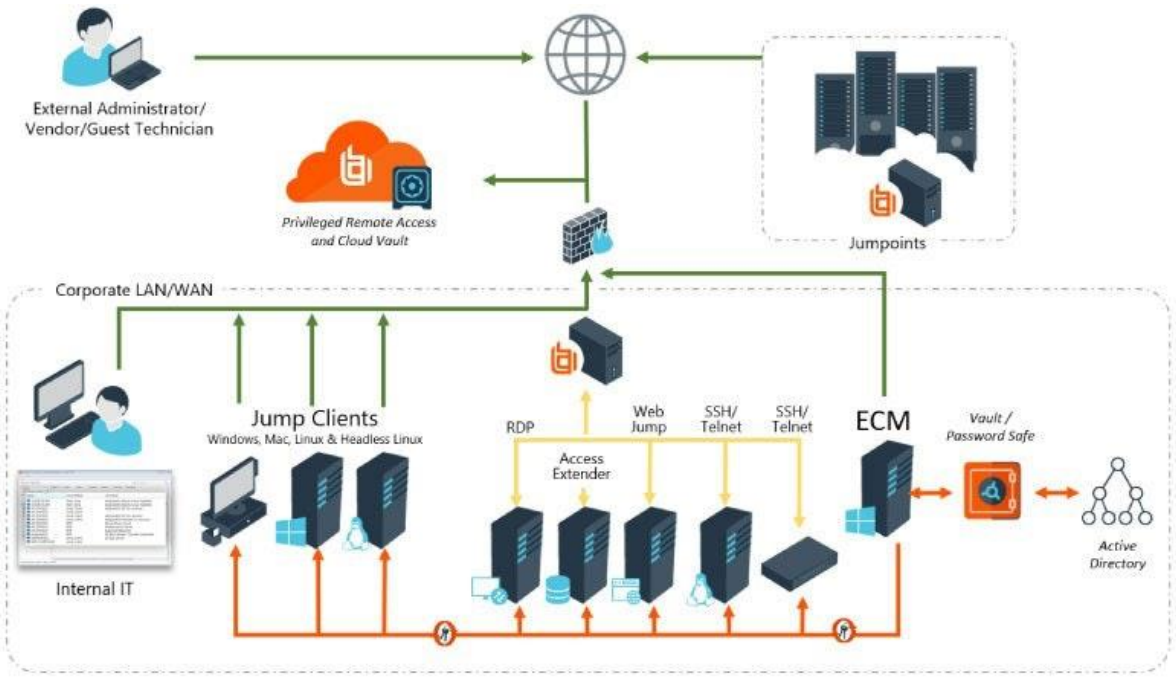

Figure 22: Privileged Remote Access (BeyondTrust)

Again, the great range of the available permissions that may be given to an internal or external user can benefit a ship's communication with resources on the land or when external partners and authorities get on the ship and ask for access to their systems. Let us consider the scenario of an external vendor getting on board with their removable drive to update one of the critical systems during a planned maintenance session. As explained above, the administrator working on the premises onshore can

limit the technician's interference to running only the selected executable in a single system for a dedicated period. Other features include access to specific folders, opening a command shell, gaining system information, and changing registry values.

Finally, all the sessions are recorded in real-time, giving the option to run reports about live sessions or refer to past sessions for accountability through a cyber forensics' procedure. In the same context, the users' sessions are logged like many monitoring applications do and recorded in high-quality videos that a privileged user can replay in an emergency.

Privileged Remote Access minimizes the risk of intentionally infecting the corporate systems through the different use of separate functionality on dedicated systems.

9.3.5 Cyber Noesis

Humans will always be present in the workflow and the ones to interact with the countermeasures suggested by BIMCO and other organizations. Cyber awareness is far from taken for granted; the buildup of a cyber security consciousness or culture, aka Cyber Awareness, becomes a real game-changer.

Common human errors can, held by a single employee, lead to a severe security breach. Such errors are delivering something to the wrong recipient, misuse of passwords (reuse on different occasions, using common passwords, holding them in non-secure places), low physical security (attackers watching physical desktops, screens, and printers), and, of course, email phishing.

The first moment we meet someone, we are inevitably suspicious and reserved until we get familiar with them. It is a normal human reaction, not only a human reaction, based on the inner fears about the unknown. However, certain occasions make people lower their suspicions and defenses rapidly if they get triggered by several events. Sharing a secret, a shared experience, or the same feeling can do the trick (K.D. Mitnick, W.L. Simon, 2002). This expected human reaction that social engineers take advantage of by trying to penetrate the corporate network of the victim's company (Rusch, 1999).

We shall strive to retain the suspicious levels at the highest degree to mitigate social engineering. In other words, cybersecurity awareness will raise red flags when a malicious stranger tries to lure us.

Cyber Noesis[59] is a company established in Greece in 2015 and offers cybersecurity consultation and solutions. It highlights the exact reasons behind the lack of human awareness before suggesting solutions. They mention the end-users lack of knowledge about the right course of action needed for each occasion. Their company's responsibility is to fill in this knowledge gap globally and keep the employees and their organization secure. The manner of achieving this is through employees' education on security matters and best practices, which will make them take better and solid decisions with the company's safety in mind.

The learning curve can be split into several stages, starting from a generic stage of security awareness common to all employees, followed by targeted training programs bonded with the employee's role (Figure 23, (Wilson M. , 2003)). A great example of such targeted programs is training the administrators due to their crucial role in the company's access and functionality overall. The final stage is gaining in-depth IT security knowledge through education programs. Instead, this type is not meant for everyone but is destined for distinguished consultors inside the company.

This learning continuum is suggested by NIST's SP 800-100 (Wilson M. , 2003). According to NIST, awareness should not be confused with training, but instead, focus the attention on security through presentations and seminars. Awareness targets all the employees by emphasizing building a basic level of knowledge, attitude, and response on relative matters. On the other hand, training targets required security skills and competencies expected from specific roles inside the company. Such an example is a training module targeting the system administrators, including *management controls* (policy, risk management, life-cycle security), *operational controls* (contingency planning, response to incidents, awareness and training issues, issues related to physical and environmental protection, and more), and *technical controls* (cryptography, identification, authentication, access control). The next stage, education, focuses on integrating security skills and competencies into producing IT

[59] Cyber Noesis, https://www.cybernoesis.com/, Accessed on 11 May 2022

security specialists who will have the capacity to act proactively and prevent rather than mitigate an incident's consequences.

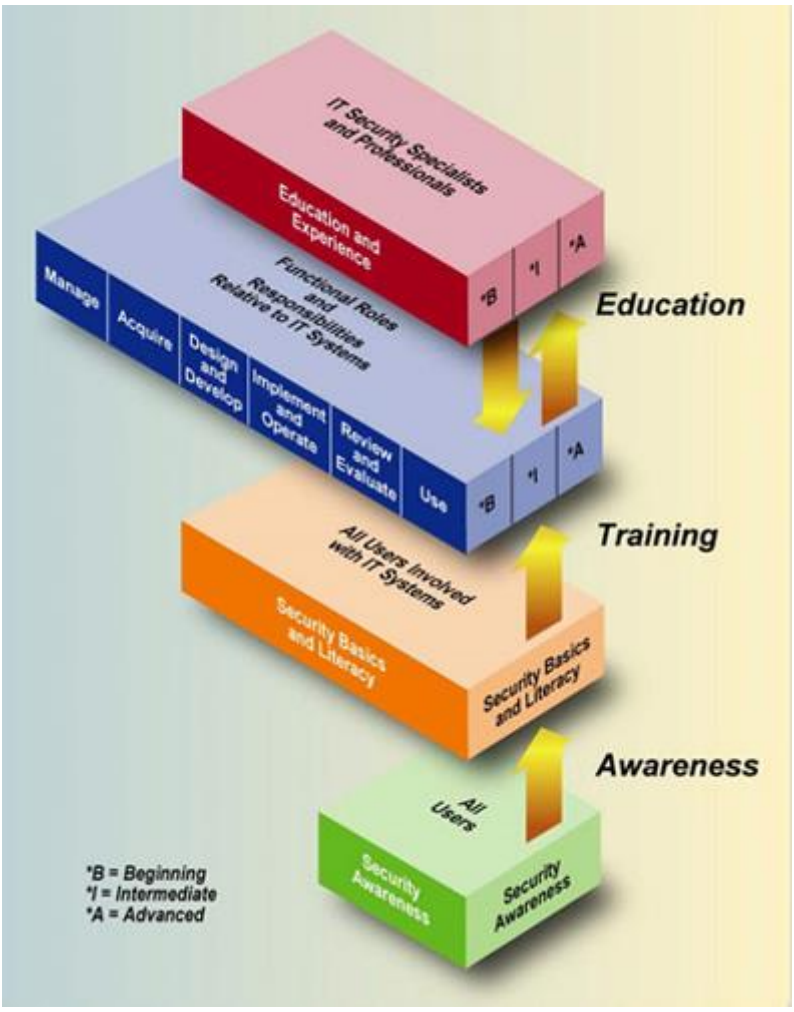

Figure 23:The IT Security Learning Continuum

Cyber Noesis stands on the first stage, Awareness, and sets specific targets since the awareness shall be part of all employees' daily routine without exception. Having a single employee unwilling to learn or less careful than others is all an attacker needs to penetrate the company's security defense. A key target is the gradual building of a standard security culture propagated from the top levels to the bottom, in terms of hierarchy demonstrating the top management's vision and concerns. Specifically, the company suggests a roadmap with the following fundamental principles:

- Change behavior gradually and consistently based on best security practices
- Train employees to recognize suspicious behavior and respond appropriately to cyber events

- There shall not be an exception to this rule. All need to share the same security culture independently of their seniority or role.
- Explain every person their role, responsibilities, and expectations the company has from them
- The cyber security awareness program shall be designed and implemented using various methods and techniques for several reasons, including optimized absorption, efficient integration in daily routine, and long-term performance

We shall implement the awareness program using a combination of onsite education (classrooms) and e-learning methods. We can train the employees using case studies, real-life news analysis, and presentations in the classroom. E-learning proves more flexible integrating *text-based and story-based material, interactive content, quizzes*. Controlled simulated phishing attacks trigger students' interest and demonstrate the easiness of malicious code propagation and its feasible impact on the company. Simulating phishing attacks can educate employees on the techniques and means used and build an awareness attitude progressively.

Being one of the most successful social engineers himself, Mitnick puts training at the core of countermeasures a firm must deploy to tackle Social Engineering (SE) attacks. He suggests assigning a potential victim some sort of self-interest about the feasibly requested information. In such a case, the possible data leakage would affect them directly and negatively, making them more concerned and paying attention to a higher degree. In employee training, Mitnick shares his training routine during the seminars he conveys, where he engages the participants in role-playing exercises and interactive games, simulating real-life SE scenarios.

Wilson (Wilson B. , 2018) suggests that building an efficient barrier against such attacks can be achieved by targeting the firm's employees to develop more psychological than technical skills. He does not underestimate the importance of technical knowledge, but he argues that focusing on alternative aspects may lead to dismissing similar attacks. A step in strengthening their defensive walls is to build a sense of ownership regarding the sensitive data an attacker can target. When the time comes, ownership makes people more alerted, concerned, and suspicious.

Both Mitnick and Wilson agree upon investing time and effort in training the employees in a holistic regime, considering the technical skills and the human factor equally. A more realistic aspect of employees' training is suggested by Aldawood (Aldawood, 2019), introducing real-life scenarios through which personnel learns to react responsively and tackle malicious attacks effectively. The latest trends in this field are serious games and simulations in a contained environment. Similarly, gamification, virtual labs, and tournaments are also utilized by simulating real-life cases, thus stimulating the participants' interest and raising the training absorption level. Moreover, awareness training programs integrating several components, such as security reports, awareness conferences, training campaigns, and tutorials, are essential in training the employees in using software and hardware security solutions effectively.

Cyber Noesis has gained a significant knowledge level regarding the reasons behind the inefficient implementation of similar educational seminars on cyber security targeting the overall personnel of a big organization, the most important of them being:

- Personnel is not involved emotionally in the education process, thinking of it as an obligation derived from the company's hierarchy and not as a tool to implement their duties more efficiently
- Major companies pay attention to communicating their goals on the strategic level, but often, they are not aligned with the objectives in the cyber security field
- The content is usually generic, without little practical demonstration and examples that fail to stimulate employees' attention and genuine interest
- Top management is not committed to a continuous education process that will be contacted, updated, and refreshed appropriately on regular intervals

Instead, the company suggests that progressively absorbing the cyber security matters and constructing a concise and solid cyber security culture is essential to the learning curve. The educational concepts shall be conducted in an amusing, regular

and multidimensional way, like the way children use to learn at an early age[60] to raise their absorption level. Stimulating more senses will help them make their daily routine adopt the techniques required to recognize and defend against more frequent and advanced threats. It is imperative to repeat actions to embed the knowledge and reward employees for adopting new habits.

Cyber Noesis suggests a methodology constituted of ten specific steps that make up the information security AWAREness[61]. This methodology follows the Plan-Do-Check-Act concept implemented in various critical sectors of human activities, like 27001 and NIST, software development, and total quality management. AWAREness is explained in more detail in *Annex C*.

[60] Learning: primary and secondary school years, https://raisingchildren.net.au/school-age/school-learning/learning-ideas/learning-school-years#:~:text=Children%20learn%20in%20different%20ways,balance%20formal%20lessons%20at%20school., Accessed on 8 May 2022
[61] isAWARE, https://www.is-aware.com/, Accessed on 11 May 2022

10 Conclusions

Vessels traveling worldwide and transferring their cargo will continue to face rising dangers, especially in the cybersecurity field. Malicious attacks against ships will continue for as long as they carry a valuable load. Moreover, more sophisticated and advanced attacks are expected in the following years. The ships' structural and operational differences compared to onshore facilities (IT and OT devices) makes their efficient defense challenging.

Influential maritime organizations like BIMCO and IMO have published guidelines and directives to help ship owners take appropriate action in strengthening their ships against cyber threats. Other reputable organizations like ENISA and several researchers claim that the vessels, like ports, are just a node in the supply chain. A data breach or failure in one node can affect the supplies worldwide. That is why protecting the ports against cyber-attacks should be taken seriously. We show several incidents that went public during the past ten years and demonstrate how vulnerable the supply chain is and the severe impacts of these attacks.

Several researchers sent questionnaires to maritime industry personnel to answer how prepared the maritime companies are *to repeal cyber threats.* The answers proved that most of the recipients take cybersecurity and its impact seriously, and they are willing to implement the relative guidelines and directives in the field. However, we identified a considerable distance between the maritime sector's current and required cybersecurity status. Top management seems hesitant and unwilling to invest the necessary resources to protect their assets (vessels) from malicious attacks.

Cybersecurity in the maritime industry is a relatively new concept. However, quite a few security companies specializing in ships and their constraints propose solutions to cover cybersecurity guidelines like the ones published by BIMCO. Academic bibliography exists in this field, trying to translate BIMCO *Guidelines* to a concrete and solid list of countermeasures. On the other hand, applying a universal list of measures to every vessel seems infeasible. A portion of the actions will need to be specified while working closely with a specialized security company.

Generally, we can define the countermeasures in education, procedures, and technical countermeasures.

Education: We need to build cybersecurity awareness gradually to address the rising cyber threats. A shift in mindset is strongly advised. The same goes for employees' reactions against feasible cyber-attacks, including social engineering. Some claim that a sense of ownership is the key in this attempt. Gaining cyber skills shall be a continuous process that will involve several learning manners (e-learning, classroom, webinars, leaflets, drills, games, virtual labs) and can lead to a nationally or globally recognized certification. Simulated phishing attacks or social engineering attacks can also educate the crew members to respond responsively to similar attacks.

Procedures: BIMCO dedicates a significant portion of the *Guidelines* to identifying threats and vulnerabilities and assessing risk exposure. Identifying and recording the ship's assets in the Asset Register (separately for IT and OT systems) is the first significant step. Establishing a solid Risk Management procedure is essential in understanding the company's assets and the ways their security could be compromised (Likelihood Assessment, Impact Assessment, Risk Assessment). While designing the ship's cyber defense, a *Defense in Depth* approach will add more defense layers and thus make the breach less feasible. All security policies shall be documented appropriately and be part of the Ship Security Plan. Password and multi-factor authentication policies will advance secrecy and access to sensitive data, while removable media storage, usage, and disposal are also required. Backup policies shall describe backing up data and settings and the procedures to restore a backup. The ship's hierarchy shall conduct related drills periodically. Contingency Plans is the document that will help the crew recover their systems in case of a breach and should be kept in hard copy too. Information sharing regarding cyber incidents (trust in sharing information) will help the rest of the maritime companies address the same attacks. Some security companies implement this approach on their platforms already.

Technical countermeasures: Exploiting outdated systems (i.e., Windows XP) is relatively easy, and companies should seriously consider upgrading their systems to newer and supported ones. Network segmentation is paramount and should separate networks with different scopes (communication between OT systems, IT systems, public networks) using hardware or software solutions (LANs, VLANs). The following measures that protect the CIA model's entities shall be applied: traffic management and incidents prevention (firewalls, IPS, IDS, EDR), encrypting transferred data with

encryption protocols, and certificates to verify the sender's identity. Limiting the used ports, protocols, and services to the ones necessary for a crew member to complete their daily tasks is a step toward securing the network traffic. A SOC manned 24/7 will minimize the time needed to bring systems online in case of a cyber incident in the land facilities.

Whitelisting is preferable to the *blacklisting* approach when referring to the OSI's application level. Although sometimes underestimated, the physical protection of the networking devices (routers, switches, cables) is also essential. The third-party technicians and agents shall use isolated working stations (Sandbox, Virtual Machines) and never be allowed to insert removable disks (USB) in the ship's systems. If this is not possible, the external devices should be scanned with updated software (anti-malware, anti-virus, anti-ransomware). Especially for technicians upgrading an OT/IT device, an isolated system should be applicable to run and test the new software before installing it in the targeted system.

Regarding satellite and radio communications (including the connection to the Internet), effective measures include VPNs and encrypted protocols, a firewall at the entry points, avoiding public IP addresses, and making the GNSS signals more immune to spoofing, jamming, and other malicious techniques. 802.1x authentication and MFA are also advised to authenticate the user before letting them connect to the ship's network remotely, combined with RDP and strong encryption like IP/Sec. Lately, the ZTNA is an architecture gaining field that combines user verification, device validation, and access control before letting the user access specific resources.

5G networks and broadened satellite Internet will open the road to crewless ships. At the same time, they will open security holes that malicious individuals will try to exploit. As long as the vessels transfer valuable goods from one place to another and play a crucial geostrategic role, the cyber threat will be authentic, feasible, and growing. Until they stop being such an imperative threat, we are called to apply the required countermeasures and protect the ship.

11 Annex A – Potentially vulnerable systems onboard ships

Communication systems

- Integrated communication systems
- Satellite communication equipment
- Voice Over Internet Protocols (VOIP) equipment
- Wireless networks (WLANs)
- Public address and general alarm systems
- Systems used for reporting mandatory information to public authorities

Bridge systems

- Integrated navigation system
- Positioning systems (GPS)
- Electronic Chart Display Information System (ECDIS)
- Dynamic Positioning (DP) systems
- Systems that interface with electronic navigation systems and propulsion
- Automatic Identification System (AIS)
- Global Maritime Distress and Safety System (GMDSS)
- Radar equipment
- Voyage Data Recorders (VDRs)
- Bridge Navigational Watch Alarm System (BNWAS)
- Shipboard Security Alarm Systems (SSAS)

Propulsion, machinery management and power control systems

- Engine governor
- Power management
- Integrated control system
- Alarm system
- Bilge water control system
- Water treatment system
- Emissions monitoring
- Heating, ventilation, and air-conditioning monitoring
- Damage control systems
- Other monitoring and data collection systems e.g., fire alarms.

Access control systems

- Surveillance systems such as CCTV network
- Electronic “personnel-on-board” systems.

Cargo management systems

- Cargo Control Room (CCR) and its equipment
- Onboard loading computers and computers used for exchange of loading information and load plan updates with the marine terminal and stevedoring company
- Remote cargo and container tracking and sensing systems
- Level indication system
- Valve remote control system

- Ballast water systems
- Reefer monitoring systems
- Water ingress alarm system.

Passenger or visitor servicing and management systems

- Property Management System (PMS)
- Ship management systems (often including electronic health records)
- Financial related systems
- Ship passenger/visitor/seafarer boarding access systems
- Infrastructure support systems like DNS and user authentication/authorization systems.
- Incident management systems.

Passenger-facing networks

- Passenger Wi-Fi or Local Area Network (LAN) internet access, for example where onboard personnel can connect their own devices22
- Guest entertainment systems.

Core infrastructure systems

- Security gateways
- Routers
- Switches
- Firewalls
- VPNs

- VLANs
- IPSs
- Security event logging systems.

Administrative and crew welfare systems

- Administrative systems
- Crew Wi-Fi or LAN internet access, for example where onboard personnel can connect their own devices.

12 Annex B – Infinity

Navarino has developed *Infinity*[62] targeted to maritime communications and requires an IP-based network. Two main components constitute *Infinity*, a virtual server installed both on the ship and ashore. Multi-factor authentication ensures the two parties' identity and credibility.

The software is available in different versions. The generic topography of the Standard Version of the *Infinity* family is shown in the following figure.

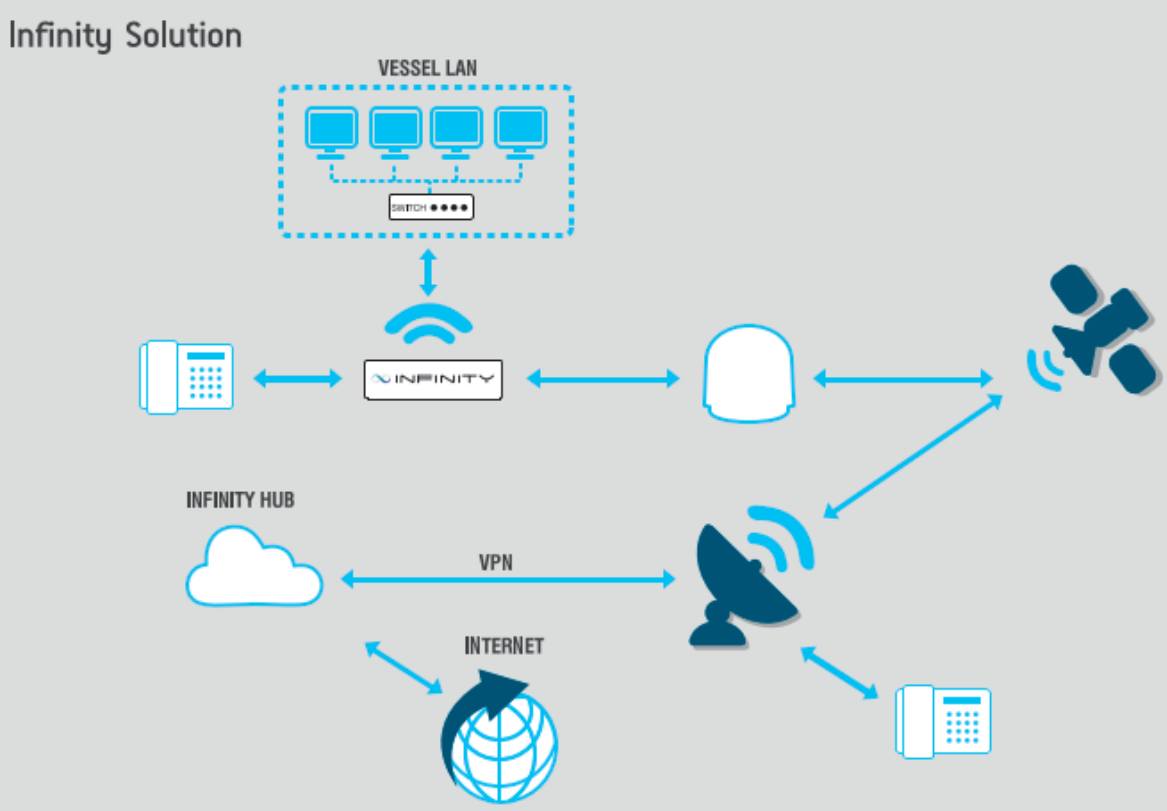

Figure 24: Infinity Standard Solution

Infinity Plus includes an onboard virtualization environment, compared to the standard version, that can deliver heavy tasks like central data processing and running multiple applications virtually at the same time. The Plus edition focuses on virtualizing and consolidating the IT infrastructure to use critical applications flawlessly onboard. Other features include the initialization of set up and administration of Virtual Machines remotely, their scheduled backup, and seamless deployment of new applications. The hardware is mounted on a convertible rack that can be upgraded to the higher version.

[62] Navarino Infinity, https://www.navarino.co.uk/portfolio/infinity/, Accessed on 11 May 2022

Infinity Cube is an *onboard* clou*d* implementation consisting of several peripherals like an automated switch, a Protocol Data Unit (PDU), and relative equipment mounted safely in a unified rack. Beyond the features of the first two versions, this version promises a higher degree of availability and performance, implementing full hardware redundancy, cluster equipment to manage shared storage, and more features. A luring feature that distinguishes this edition is its ability to detect CPU, memory, and disk failures and bypass them to ensure business continuity. In the same context, Cube focuses on eliminating single points of failure and activating alternative communication channels that keep availability levels on a high level.

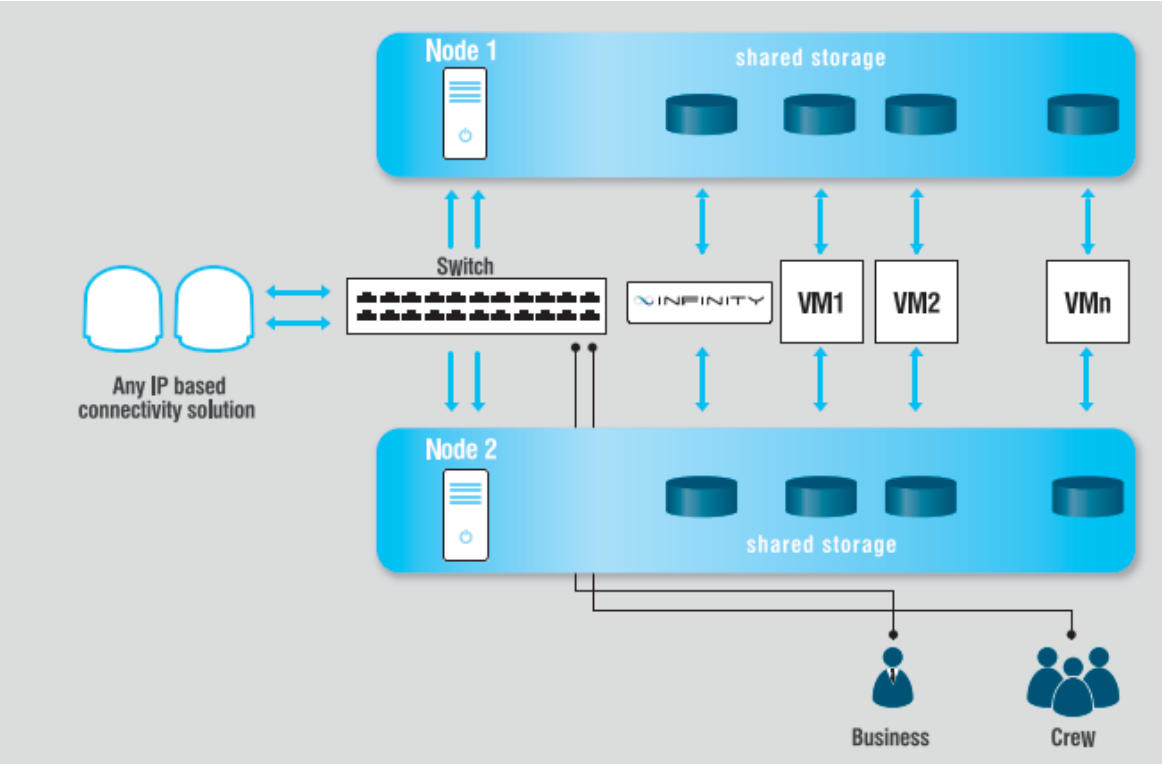

Figure 25: Infinity Cube Solution

The user operates the sophisticated software through a straightforward and user-friendly web-based environment (Infinity Hub), as shown in the following Figure. The Cube's significant advantage is that the centralized management features release sailors from additional tasks of maintaining software and other tasks unrelated to their skills. The skilled personnel onshore can work remotely and troubleshoot situations where their expertise is required.

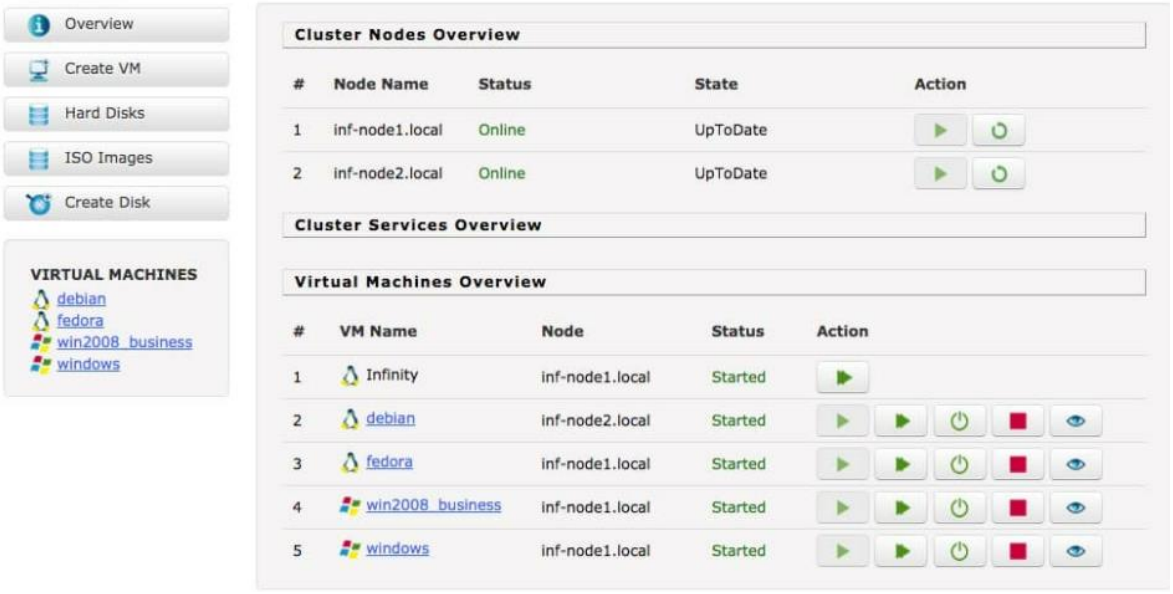

Figure 26: Infinity Cube's Management Interface

13 Annex C – isAWARE

Cyber Noesis has invested significant effort in developing the isAWARE tool[63], an advanced awareness platform destined to train users on critical cyber security concepts by conducting customized asynchronous training curriculums and running simulated phishing attacks.

Their methodology follows the abstract Plan-Do-Check-Act model and segments the overall procedures in ten steps, as shown in the following figure.

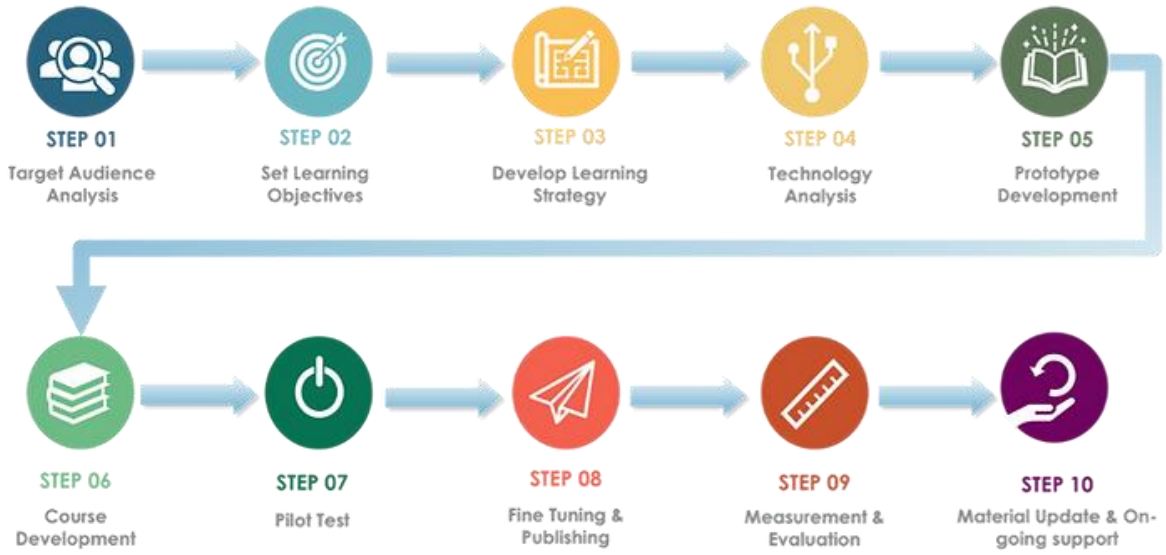

Figure 27: information security AWAREness' methodology

Rather than developing a versatile material for every company or sector, the isAWARE platform pays attention to identifying the target audience. All steps are linked in sequential order. Thus, every one of them depends on the previous and bonds the following stage. Consequently, the target audience's analysis will set the frame in which the next nine steps will be performed and the tool's efficiency will depend on the first step to a great extent. Working closely with each client, the experienced personnel set the learning objectives in coordination with the company's top management. Steps 3 to 8 implement the generic Do phase of the Plan-Do-Check-Act model and consist of the separate stages that produce the educational material. Developing a learning strategy, analyzing the technology to be used, creating a prototype and a course, performing a pilot test, and fine-tuning and finalizing the course are all actions implementing the plans made in the initial stages. All methods utilizing a circular,

[63] isAWARE, https://www.is-aware.com/, Accessed on 11May 2022

never-ending process integrate some sort of reviewing and updating. Similarly, isAWARE measures and evaluates the actions taken in the previous stages and compares the results against the expected targets. Based on this evaluation, the educational material is updated and enriched while triggering the next round of the ten steps.

As mentioned above, there are various methods to be used to make the learning process funnier, more direct, efficient, and successful. Cyber Noesis contacts its clients and tries to reach a balanced collection of text-based material, storyline material, short videos (demos), interactive content, quizzes, narrations, and games.

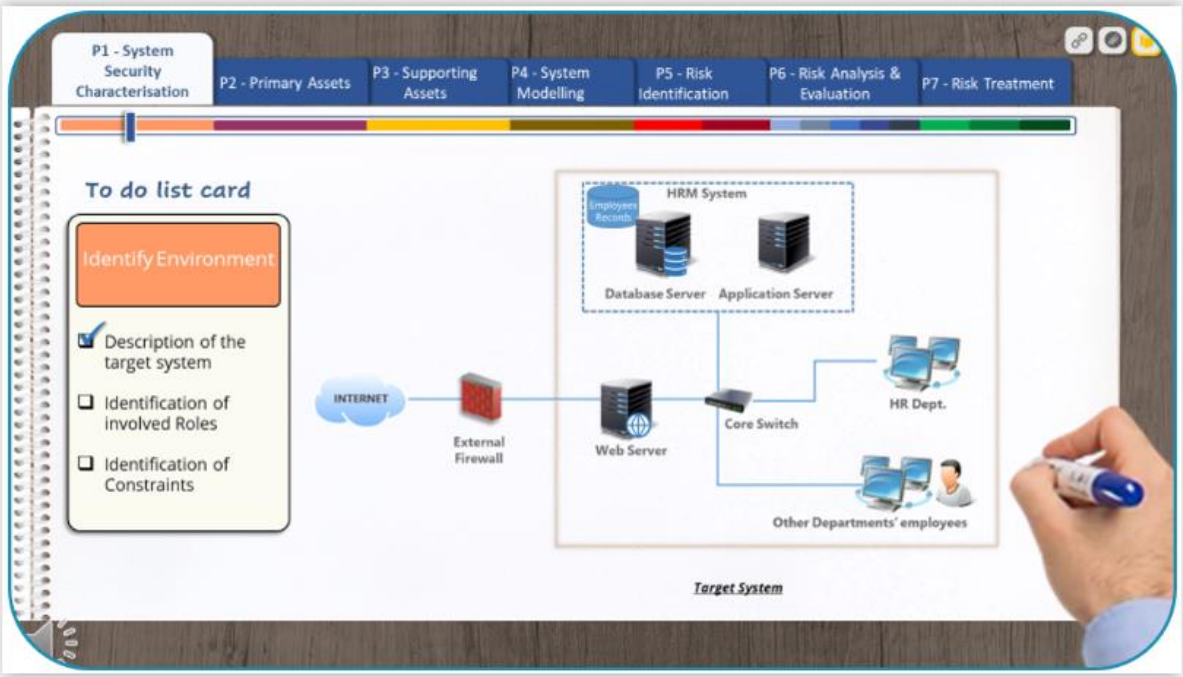

Figure 28: Example of game-based material

14 Glossary

ACL	Access Control List
AI	Artificial Intelligence
AIS	Automated Identification Systems
AT	Attack Tree
BIMCO	Baltic and International Maritime Council
BYOD	Bring Your Own Device Policy
CIA	Confidentiality, Integrity, Availability
CISA	Cybersecurity & Infrastructure Security Agency
CISE	Common Information Sharing Environment
CNG	Compressed Natural Gas
CSP	Cyber Security Plan
CYREN	Cyber Resilient North Sea Canal Area
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
ECDIS	Electronic Chart Display and Information Systems
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
ESP	Endpoint Security Protection
EU	European Union
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation

GNSS	Global Navigation Satellite Systems
IDS	Intrusion Detection System
IIOT	Industrial Internet of Things
IMS	Integrated Management System
INS	Integrated Navigation System
IoT	Internet of Things
IPS	Intrusion Prevention System
IP/Sec	Internet Protocol Security
ISO/IEC	International Organization for Standardization
IT	Informational Technology
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LPG	Liquified Natural Gas
MFA	Multi-Factor Authentication
MV-HARM	Maritime Vessel-Hierarchical Attack Representation Model
NAC	Network Access Control
NGFW	Next-Generation Firewall
NIST	National Institute of Standards and Technology
OS	Operating System
OT	Operation Technology
PDU	Protocol Data Unit
PAM	Privileged Access Management
PDCA	Plan-Do-Check-Act
RDP	Remote Desktop Protocol

RDS	Remote Desktop Services
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SE	Social Engineering
SecCM	Security Configuration Management
SIEM	Security Information and Event Management
SMS	Safety Management System
SOC	Security Operation Center
SSP	Ship Security Plan
STCW	Standards of Training, Certification and Watchkeeping
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
ZTNA	Zero Trust Network Access

15 Table of Figures

16 References

K. Tam, K. Jones. (2019). MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment. *WMU Journal of Maritime Affairs*, 129-163.

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

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

A. Goudossis, S.K. Katsikas. (2019). TOWARDS A SECURE AUTOMATIC IDENTIFICATION SYSTEM (AIS). *Journal of Marine Science and Technology*, 410-423.

A.Dimakopoulou, N.Nikitakos, I. Dagkinis, Th. Lilas, D.Papachristos, M.Papoutsidakis. (2019). The New Cyber Security Framework in Shipping Industy. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*.

Aldawood, H. (2019). *An Academic Review of Current Industrial and Commercial Cyber Security Social Engineering Solutions.* Kual Lumpur: ICCSP.

Allianz. (2021). *Safety and Shipping Review 2020.* Allianz.

B. Svilicic, D. Brčić, S. Žuški, D. Kalebić. (2019). Raising Awareness on Cyber Security of ECDIS. *the International Journal on Marine Navigation and Safety of Sea Transportation*.

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

Baldauf, M., Kitada, M., Mehdi, R.A., Al-Quhali, M.A., Chong, J.C. (2018). WILL THE FUTURE OF SHIPPING BE BASED ASHORE? *VTS, NAVIGATION, MOORING AND BERHING*, 100-103.

Bateman, T. (2013, 10 16). *Police warning after drug traffickers' cyber-attack*. Retrieved from BBC: https://www.bbc.com/news/world-europe-24539417

Beaumont, P. (2018). *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution.* Hershey: IGI Global.

BIMCO. (2020). *The guidelines on Cyber Security Onboard Ships v.4.* BIMCO.

Bosworth, S. K. (2014). *Computer security handbook.* New York: Wiley.

Brewin, B. (2013, 7 29). *University of Texas Team Hijacks $80 Million Yacht With Cheap GPS Spoofing Gear*. Retrieved from Nextgov: https://www.nextgov.com/cio-briefing/2013/07/university-texas-team-hijacks-80-million-yacht-cheap-gps-spoofing-gear/67625/

Bronk, C. (2013, 4 3). The Cyber Attack on Saudi Aramco. *Survival*, pp. 81-96.

Dingeldey, P. M. (2022, 4 12). *The Maritime Executive*. Retrieved from Port Automation and Cybersecurity Risks: https://www.maritime-executive.com/editorials/port-automation-and-cybersecurity-risks

Duck, D. (2017, 2 23). Global Threats: Cybersecurity in Ports. *Hemispheric Conference on Port Competitiveness & Security: Finding the Right Balance*. Miami: University of Miami: Center for International Business Education & Research (CIBER) .

E.P. Kechagias, G.Chatzistelios, G.A. Papadopoulos, P. Apostolou. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*.

Engbers, J. (2016, 8 16). *Pratum*. Retrieved from Security Awareness, Training, and Education - A Learning Continuum: https://www.pratum.com/blog/331-security-awareness-training-and-education-learning-continuum

ENISA. (2022, April 4). *Cyber Risk Management for Ports.* Retrieved from ENISA: https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports/@@download/fullReport

(2021). *ENISA THREAT LANDSCAPE 2021.* ENISA.

H. Boyes, I. Roy, L. Alexandra. (2016). *Code of practice, Cyber Security for Ports and Port Systems.* London: Institution of Engineering and Technology.

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking.* Indianapolis: Wiley Publishing Inc.

I.P. Zarzueloa, M.J.F. Soeanea, B.L. Bermúdez. (2020). Industry 4.0 in the port and maritime industry: A literature review. *Journal of Industrial Information Integration*.

IACS. (2020). *Recommendation no. 166 on Cyber Resilience.* IACS. Retrieved from https://www.iacs.org.uk/download/10965

Iakovleva, E. V., & Momot, B. A. (2017, October). Development of technology for creating intelligent control systems for power plants and propulsion systems for marine robotic systems. *IOP Conference Series: Earth and Environmental Science*.

ICS. (2021). *Seafarer Workforce Report, 2021 Edition.* ICS.

IMO. (2017). *Guidelines on maritime cyber risk management.* IMO.

(2018). *ISO/IEC 27000/2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary.* ISO.

(2018). *ISO/IEC 27005/2018 Information technology - Security techniques - Information security risk management.* ISO.

J. Rajamäki, I. Tikanmäki, J. Räsänen. (2019). CISE as a Tool for Sharing Sensitive Cyber Information in Maritime Domain. *Information & Security: An International Journal*, 215-235.

J.I. Alcaide, R.G. Llave. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, 547-554.

K.D. Mitnick, W.L. Simon. (2002). *The art of deception.* Indianapolis: Wiley Publishing.

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

Mäkinen, M. (2016). Autonomous ships: The next step. Rolls-Royce.

McQuade, M. (2018, 8 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Retrieved from Wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

NIST. (2017). *Special Publication 800-63: Digital Identity Guidelines.*

P. Baum-Talmor, M. Kitada. (2022). Industry 4.0 in shipping: Implications to seafarers' skills and training. *Transportation Research Interdisciplinary Perspectives*.

Planning, D. o. (2021). *Cybersecurity Handbook.* Ministry of Digital Governance.

Polemi, N. (2017). *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains.* Elsevier.

Pseytelis, A. (2021). *Cyber security, Human Factor, Maritime Industry.* Piraues: University of Piraeus.

R. Sahay, W. Meng, E. Sepúlveda, A. Daniel, C.D. Jensen, M.B. Barfod. (2019). CyberShip-IoT: A Dynamic and Adaptive SDN-Based Security Policy Enforcement Framework for Ships. *Future Generation Computer Systems*.

Rusch, J. (1999). *The Social Engineering of Internet Fraud.* San Jose: INET.

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., Harnisch, M. (2015). *Industry 4.0: the Future of Productivity and Growth in Manufacturing Industries.* Boston Consulting Group.

S.Y. Enoch, J.S. Lee, D.S. Kim. (2021). Novel security models, metrics and security assessment for maritime vessel networks. *Computer Networks*.

Schneier, B. (2011). *Secrets and lies: digital security in a networked world.* John Wiley and Sons.

Shauk, Z. (2013, 2 23). *Malware on oil rig computers raises security fears*. Retrieved from Houstochronicle: https://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-security-fears-4301773.php

UNCTAD. (2020). Review of Maritime Transport 2020. New York, United Nations: UNCTAD. Retrieved from https://unctad.org/system/files/official-document/rmt2020_en.pdf

Wilson, B. (2018). *INTRODUCING CYBER SECURITY BY DESIGNING MOCK SOCIAL ENGINEERING ATTACKS.* JCSC.

Wilson, M. (2003). *Building an Information Technology Security Awareness and Training Program.* Gaithersburg: NIST.

Zarrzuelo, I. d. (2021). Cybersecurity in ports and maritime industry: Reasons for raising. *Elsevier*, 1-4.