2021-11-25

Cyber Awareness Raising and Training An Integrated Maritime Cyber Risk Management Approach

Hopcraft, Rory

Cyber Awareness Raising and Training – An Integrated Maritime Cyber Risk Management Approach

R Hopcraft[1], M Canepa[2], S Karamperidis[1], F Ballini[2]
[1] University of Plymouth, [2] *World Maritime University*

Abstract
Ports and their stakeholders are highly interconnected within maritime supply chains. Managing these networks has led to an increasing dependence on information and communication technologies (ICT), opening up the sector to new vulnerabilities from cyber risks. Ports act as the nexus for global trade to move cargo and passengers between land and sea, therefore it is crucial these infrastructures remain secure. Using the EU Horizon's Cyber-MAR platform as an example, this paper will explore the potential disruptions that a cyber incident can cause on a port's power management network. These disruptions can have serious impacts on the maritime sector, especially when considering the multidimensional factors like reputation, insurance and fines. Cyber risk management is currently a major challenge for the maritime sector, and much of the current legislation stipulates training as a way to increase the security of maritime digital infrastructure. This paper will explore how, through the implementation of various training approaches cyber awareness forms a vital part of a company's cyber risk management.

Keywords: *Cyber awareness raising, maritime cyber risk management, hybrid training, maritime transport, digitalisation*

1. Introduction

The amount of digital technology integrated within the maritime sector has risen rapidly over the last decade. Many ports now boast various levels of process automation, in terms of information technology (IT) and operational technology (OT). Much of this new technology is designed to increase efficiency and therefore increase the profitability of operations (Port Technology, 2020). For example, automation in container terminals had enhanced control of containers by providing timely information flow. Thus, increases the quality of service and decision-making within the container yard, that in turn increases growth, profitability, and reputation for the port operator (Kia et al., 2000).

However, the increased integration of technology comes with complications. Much of this technology forms vast networks within maritime infrastructure, and often connects to the public internet. Therefore, the sector is now finding itself increasingly open to cyber risks. The management of these risks have gained increased attention at both national and international levels over the past decade. In 2014, the International Maritime Organization (IMO) first started discussing cyber risk management, with the publishing of interim guidelines in 2016 (International Maritime Organization, 2016b). It was later, in 2017 that the IMO published *Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management System* (International Maritime Organization, 2017), which formalised the need to address cyber risk in the maritime sector.

The IMO is not the only supranational organisation that has realised the risk posed by cyber-enabled systems to the maritime sector. For instance, the European Union, through the NIS Directive (European Union, 2016a), highlights the importance that the maritime sector has on national and global trade. As such, States should be working with key stakeholders within the industry to ensure that these essential services remain safe and secure for the betterment of both the State and the Union.

However, managing cyber risk is not a simple process, and requires detailed exploration by companies to ensure their investment in development is appropriate. One of the first steps to be taken is the development a cybersecurity strategy that can be used to ensure that all devices and users comply with company policy. With regards to the specifics of this policy, there are a number of factors that will come into play. These factors can include the compliance with industry and government regulations and standards, such as GDPR, ISO 27001, and other IMO instruments.

This paper will present the argument that if developed and delivered appropriately, cyber awareness training offers a cost-effective and meaningful cyber risk management approach. As the Gordon-Loeb model illustrates, there is a clear relationship between system vulnerabilities, the resultant potential loss, and the optimum amount of cybersecurity investment (Gordon and Loeb, 2002). Therefore, training should be approached as a comparatively cost-effective way to reduce system vulnerabilities and the potential loss.

The lack of cybersecurity skills within the sector is a real problem. The need for cyber risk management education and training has an impact on many other sectors not just the maritime sector (Security Boulevard, 2019). Vishik and Heisel (2015) (as quoted in Zan and Franco (2019)) commented that even in the EU, where policies follow common objectives, it is challenging to keep similar education approaches. In addition, they explained that there is a "lack of cybersecurity educators, low interaction with the industry, little understanding of the labour market, outdated or unrealistic platforms in education environments, and difficulties in keeping pace with the outside world". Thus, making the implementation of quality cyber security training challenging. However, there are benefits to upskilling, including the fact that highly trained cybersecurity professionals will catch things that automated tools miss.

Using the EU Horizon's Cyber-MAR project as an example this paper will firstly exploring the implications of a cyber-incident on maritime infrastructure. These implications include impacts on the multidimensional factors like reputation, insurance and fines. Secondly, the paper will discuss the important role the human element plays in maritime security more broadly, before exploring the role they play in cyber risk management. Before moving onto discuss the type of training that is most effective, the paper will explore why training should be at the forefront of a company's cyber risk management approach. Developing the argument that training, while only one element of cyber risk management, offers to deliver effective and achievable advancements in a company's cyber risk management.

2. Implications of a Maritime Cyber-Incident

At the end of 2020, the European Union's Horizon 2020 Cyber-MAR project demonstrated the implications of a cyber-incident targeting European maritime infrastructure. The Cyber-MAR project aims to develop an "innovative cybersecurity simulation environment for accommodating the peculiarities of the maritime sector" (Cyber-MAR, 2019a). Through the analysis of data collected from EU member states CSIRTs/CERTs, the project will provide a knowledge-based platform to aid cyber risk management decisions (Cyber-MAR, 2019b).

The scenario chosen by the consortium demonstrated how, through the opening of a malicious email, malware is able to spread throughout a ports digital infrastructure. Eventually the malware propagates through all parts of the ports IT systems allowing an attacker to control the power management system remotely. This level of access allows an attacker to have complete control over the target system, in this case the electrical grid, enabling them to shut it down for a length of time, which results in a variety of subsequent impacts on port operations.

Based on the Port of Valencia (PoV) these impacts would include the loss of power to the cranes across the port, reducing the ability for the port to unload/reload ships, move containers through the port, and finally move goods onwards towards their destination. The loss of power would have also resulted in the loss of administrative systems, where digital manifests and logs become inaccessible. Thus, rendering it almost impossible to determine where each container is within the port and where it needs to go. Moreover, the loss of administrative systems would have also resulted in the loss of emails and other communications, affecting the ability of the port to communicate with other stakeholders of the ongoing incident. Such a scenario will have an impact on the port's profitability as we aforementioned.

While no sector is safe from the consequences of a cyber-incident, this example highlights the importance of ensuring that maritime digital infrastructure remains secure. According to 2019 data, PoV ranked 5th in Europe for total throughput handling 5,441 thousand TEU's (Twenty-foot equivalent unit – container) (Notteboom, 2020). **Error! Reference source not found.** illustrates the statistics from PoV annual report, with 56.38% of container traffic was transhipment (held at PoV as an intermediate destination before transferring onwards), 21.15% was imported and 22.46% exported (Port Authority of Valencia, 2019).

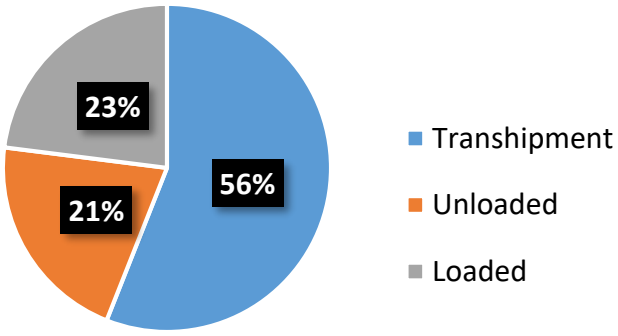

Figure 1: 2019 Valencia Port Authority Container Traffic *(Port Authority of Valencia, 2019)*

Goods handled by PoV (as in most container ports) are split in two categories: 1) time critical and 2) non-time critical. Non-time critical goods such as construction materials are the majority of cargo being lifted in PoV in terms of volume. That is the case as usually those goods are high volume and low value. PoV exported more than 5mil tons of construction materials in 2019 (Notteboom, 2020).On the other hand, time critical cargo is usually low volume high value goods. PoV exported approximately 2mil tons of food products (Port Authority of Valencia, 2019). Food products are usually transported with refrigerated containers. Delays, or damage to the refrigerator units, caused by the cyber-incident affecting the power supply, would have a catastrophic impact to the freshness of these goods.

This impact could be in terms of both reputation and monetary as companies whose goods were in those containers would sue the port for damaging the cargo. That will affect the overall Spanish Economy, as Spanish food production is 12.6% of the total Spanish GDP (European Commission, 2020). Therefore, if the port damage such an important sector the impact of the damage will be spread to the overall Spanish economy. In addition, the local region comprises of a large manufacturing industry, delays in the transfer of machinery and iron products will have a knock-on impact on the local region. Thus, the impacts of these delays become more widespread directly affecting the port, the local region and the Spanish economy.

Another factor that demonstrates the multidimensional factors of a cyber-disruption is the ports ability to mitigate and recover effectively in a short-time frame. A slow recovery will ultimately affect

the throughput of the port. As first reaction, shipping companies may redirect their cargo to another local port to help reduce the impact. However, this might not be possible for all goods coming through the PoV. The PoV has a proportion of goods arriving and departing on fixed infrastructure, like rail (7.27%), which other ports do not have direct access too (Port Authority of Valencia, 2019). Secondly, much of the PoV's operations are transhipment, other ports are reliant on the transfer of goods from Valencia to the wider region. These ships could travel to other ports in the region, for example, Barcelona. Needing to travel to another port would extend the shipping time of products. Moreover, these other ports will still be servicing their normal operations, leaving limited capacity available to deal with the extra demand for cargo handling.

Thus, the Port of Valencia offers a snapshot into the increasingly complex multidimensional factors that determine the severity of an incidents impact. While the specific geographical, technical, and societal elements of this example are unique to the PoV, all other ports offer similar complex situations. While the shutdown of the PoV would have a limited lasting impact, other ports like Port of Pireaus, where there are no alternative ports with enough capacity, the consequences of a cyber-incident would be higher. Therefore, companies, with the support of their States (as any impact in ports operations could heavily affect States), need to be giving maritime cyber risk management serious consideration. The consequences of a cyber-incident will not be limited to a single company. Rather an incidents impact will be more widespread, causing greater disruption.

2.1. Other Consequences

Alongside the resultant business disruption, the impacts of a power failure are just some of the threats companies may face because of a cyber incident. One such impact is the cost to replace, or repair equipment damaged during the incident. From research carried out by the UK Government's Department for Digital, Culture, Media and Sport, they found that in 2020 the average cost of cyber-incidents on UK businesses was around £3,230 (Department for Culture Media and Sport, 2020). While not a significant financial impact, these losses are due to mundane cyber incidents. On the more extreme side of events, (i.e. the black swan incidents) the 2017 NotPetya incident at A.P Møller-Mærsk destroyed 55,000 client computers and 7,000 servers (Ashford, 2019). Estimates suggest that the company's total loss of revenue was in the region of $300million (Ritchie, 2019). Whereas the recovery cost of the incident was around $40million (A.P Møller-Mærsk, 2019).

The Mærsk incident illustrates that there are other financial impacts of cyber-incidents aside from the cost of disruption and recovery. While not the case for Mærsk, companies also face the threat of subsequent litigation, fines and reputational damage (Pearson, 2014). Many of these could have a significant financial impact on the company, both in the short and long term.

As mentioned earlier, the IMO is only one of the supranational organisations considering cybersecurity. The EU is one of primary organisations driving companies to consider their cyber risks. To do this they have ratified a range of Directives that legally obligate companies to improve cybersecurity, failure to do so can result in fines. In an attempt to combat the rise in high profile data breaches the EU ratified the General Data Protection Regulation (GDPR) (European Union, 2016b). GDPR stipulates that companies that fail to ensure the security of personal data they hold are liable to pay considerable fines of up to €20,000,000 or 4% of global annual turnover.

In 2018, British Airways experienced a cyber-attack that affected 380,000 transactions (BBC, 2018). In the Information Commissioner's Office Penalty Notice, the authority charged with enforcing GDPR compliance, originally proposed a penalty of £183.39m (Information Commissioner's Office, 2020). While the Notice goes onto explain how the Covid-19 pandemic led to the reduction in this fine to £20m, this example illustrates that a GDPR breach can have serious financial implications.

However, unlike the financial implications for regulatory compliance failure, cyber incidents, due to their increased publicity and widespread impacts can have a greater impact on a company's reputation. This impact is multi-faceted with the damage of customer confidence, and the loss in market share. It has noted that a strong reputation can yield better market performance. However, it is challenging to quantify the true impacts of a damaged reputation (Ireland, 2018).

In their study, Fontnouvelle and Perry (2005) found that there was limited too no reputation damage if the losses were triggered by external factors. Rather companies suffered a bigger loss in reputation if the loss was caused by internal factors. Thus, if a company suffers a cyber-incident originating externally their reputation should fare better than if the incident was caused by internal factors. However, there are examples where failings in the internal cybersecurity procedures have had a lasting impact on a company's reputation, regardless of the origin of the incident.

One example of these internal factors affecting reputation is the UK-based telecommunications company TalkTalk's data breach in 2015. The company failed to notify thousands of customers about a data breach affecting them (Ashford, 2016). This internal failure of the incidents handling, and lack of reassurance led to a loss of consumer confidence (Maddocks, 2015). Figure 2 shows how the company's reputation score changed following the announcement of the breach (1). Due to the poor internal handling of the data breach, the company's reputation continued to dip over the proceeding months as more details were announced (2-5). This media coverage included the court case of one of the perpetrators, as well as the announcement of the fine.

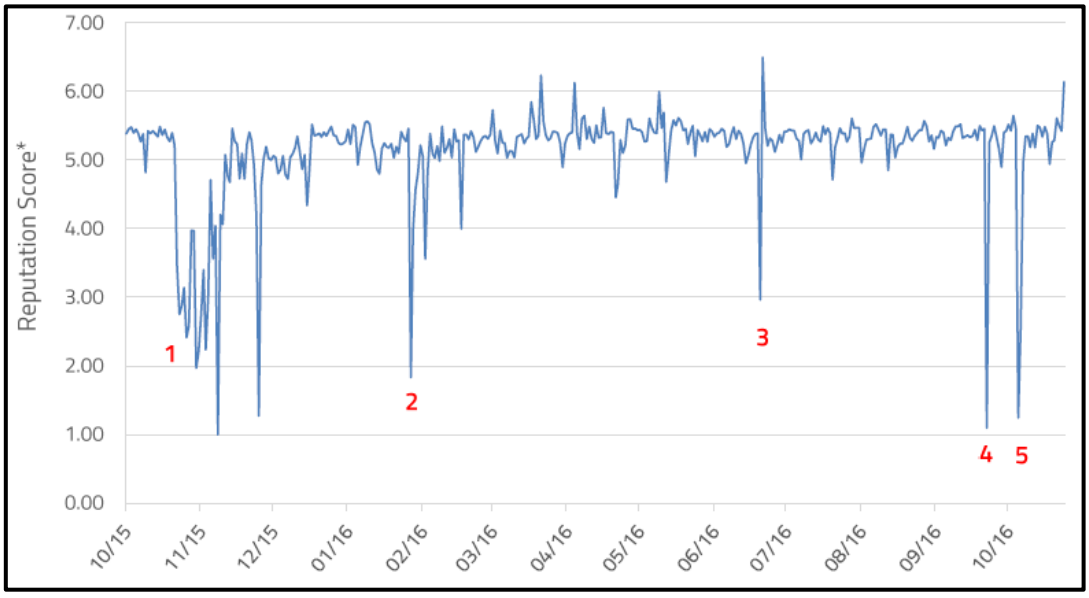

Figure 2: TalkTalk's Reputation Score Change After 2015 Breach *(Ashford, 2016)*

Moreover, Gillet et al. (2010) argue that when the loss amount is not know there is often an overreaction by the market, compared to when the actual loss figures are known. This overreaction by the market due to the uncertainty is clearly demonstrated in the wake of the Colonial Pipeline cyber-attack. In May 2021, the US-based pipeline providing 45% of oil to the East Coast was hit by a ransomware attack (The Guardian, 2021). Due to the uncertainty over the severity of the attack, and the shutdown of the pipeline, the cost of oil increased by 0.6% (Offshore Technology, 2021). This increase pushed US petrol prices above $3 a gallon, representing its highest level since 2014 (Brower and McCormick, 2021).

For our example of the PoV, oil would be less of a concern than the time-critical products like fresh fruit and vegetables. Spain has the highest production share of Oranges (54%), small citrus fruit (67%),

avocados (91%), among others, in Europe (Ministry of Foreign Affairs, 2020). Thus, a delay in the transportation of these perishable goods would affect both the local region and Europe more broadly.

3. The Human Element in Cyber Safety Management

The maritime sector has always relied upon human involvement from sailing the ships to operating the port cranes (Kia et al., 2000). While these roles may have changed or been replaced with the integration of technology, maritime operations are still reliant upon human operators [ibid]. **Error! Reference source not found.** illustrates the major fields on employment in the maritime sector. Many of these roles are directly related in the safety of maritime operations.

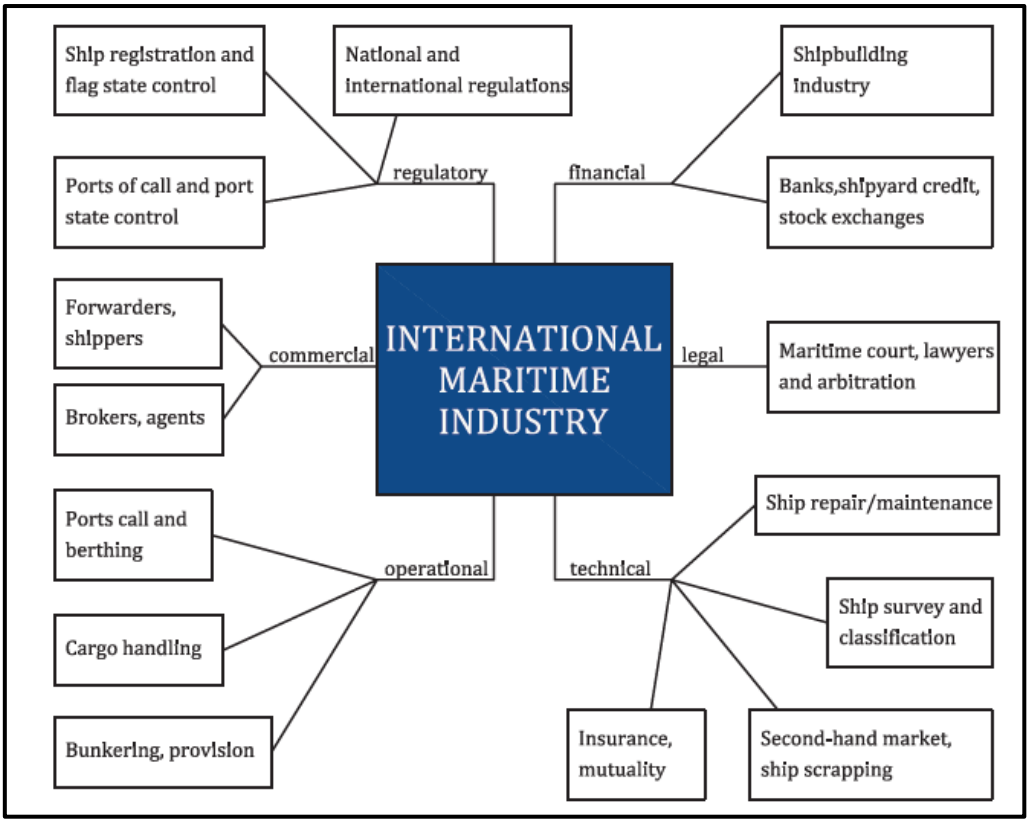

Figure 3: Major fields of employment in the maritime industry *(International Organization for Standardization, 2020)*

What is evident from the variety of employment fields in the maritime sector is that each personnel will have a different role to play in safety. For instance, those personnel involved in cargo handling will have different safety responsibilities to brokers working in offices. This varying degree of responsibility for safety is noted within the training guidance of other industries. For example in nuclear safety, personnel who work more closely with nuclear material require a greater extent of training to those personnel who perform tasks less sensitive to maintaining nuclear safety (International Organization for Standardization, 2021).

It is worth noting that there are many different elements to cyber risk management, with humans being just one of those. However, as argued by Reason (1997) the safety practices and processes put into place often create what is termed a *Swiss Cheese Model*. This model is where there are various safety elements, including hardware, software and humans that create layers. However, like its dairy counterpart, these layers have weaknesses (the holes) these represent the limitations in that processes capabilities. This visualisation illustrates why safety management consists of various layers of elements to ensure as many of the holes are covered.

However, the last and final barrier normally involves the operator of the system, so when the incident exceeds the operators limitations, the risk penetrates through all the safety barriers leading to an incident to occur (Barnett and Pekcan, 2017). The human element is sometimes referred to as the biggest internal threat facing the cybersecurity of companies (Boletsis et al., 2021, Meshkat et al., 2020). The latest Verizon Data Breach Investigations report asserts that 30% of reported data breaches involved internal actors, and that 22% of all breaches were caused by human error (Verizon, 2020). As argued by Aytes and Connolly (2004) personnel are often rewarded for not following good cyber risk management practices. For instance, the sharing of passwords is seen as helpful or not scanning documents before opening them saves time.

Following the argument that humans are often the last barrier to stop an incident occurring, Singleton (1973) argues that the cause of almost any incident can be traced back to inadequate design, inadequate training, inadequate instruction or inadequate attention resulting in a human error. Barnett (2005) illustrates the different types of human error (see Figure 4).

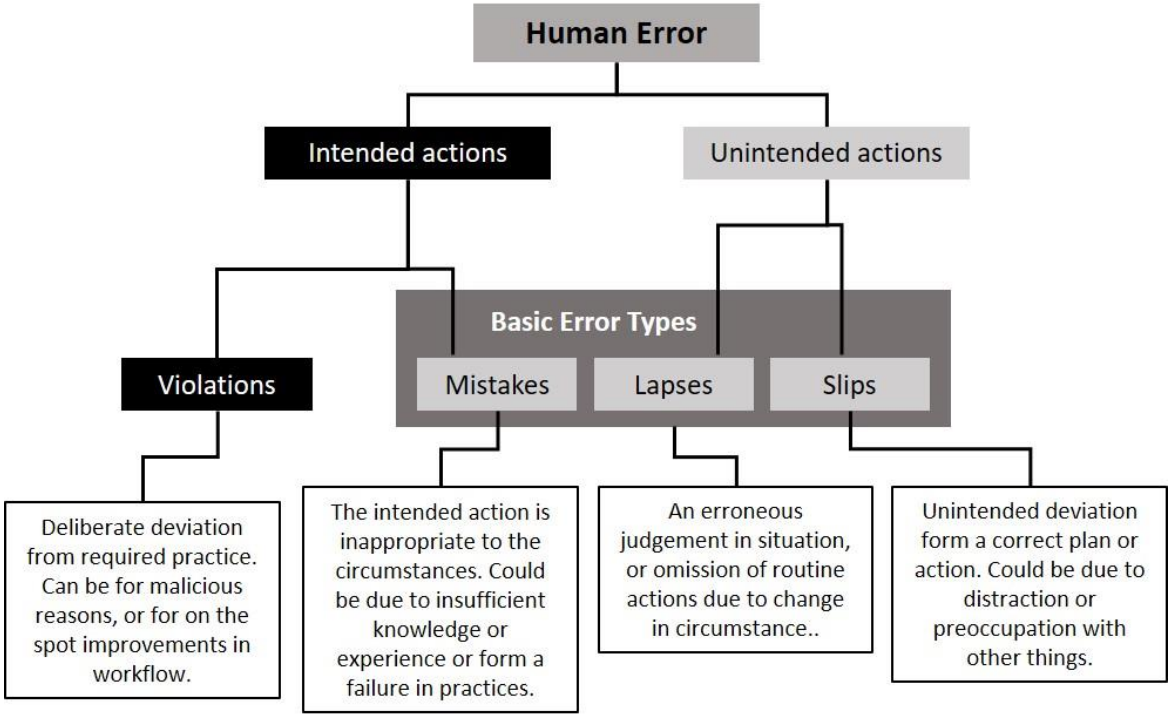

Figure 4: Summarised Sources of Human Error *(adapted from Barnett (2005))*

Therefore, regardless of the various layers of safety that have been built into a system, human error, accidental or deliberate can allow an incident to occur. Thus, demonstrating the important role that humans play in the safety of system, and the importance on ensuring they attain the right skills and knowledge to perform their safety function. Moreover, this safety function differs between operational responsibilities, meaning the safety training provided needs to be appropriate to these roles.

3.1. Humans in Maritime Safety Management

Within the maritime sector, the IMO has a long history of emphasising the link between the human element and safety. This relationship was formalised in 1993 (International Maritime Organization, 1993), where the IMO argue that safety is based on many complex interacting variables including training, skill level and experience (International Maritime Organization, 2003). Thus, arguing that for humans to fulfil their safety roles they must be equipped with the right skills to do that.

While Hetherington et al. (2006) summarises that it is often difficult to collate the true number incidents caused solely by human error, there is still a significant number of examples. Examples like the capsizing of the Herald of Free Enterprise (1987) or Costa Concordia (2012) demonstrate the significant consequences that human error, or misjudgement can have on the safety of maritime infrastructure.

The IMO has often been accused as being a reactive Organization, where it learns from incidents and develops governance that reduces the likelihood of events reoccurring (Pomeroy and Earthy, 2017). However, what is evident over the last decade is the IMO's drive to place the human element at the centre of the safety management discussion. This placement was achieved through the introduction of the International Management Code for the Safe Operations of Ships and for Pollution Prevention (ISM Code) (International Maritime Organization, 2014). To ensure compliance, companies had to overhaul their organisation and management practices to formalise many of the safety management process already in place (O'Neil, 2003). This restructuring of the role of the human element in safety management ensures that personnel are equipped with the right skills to recognise when unsafe operations are occurring, and proactively respond to them.

As a part of the ISM Code companies should develop and implement a safety management system (SMS). As part of their SMS, companies should include instructions and procedures to ensure the safety operation of ships that is compliant to international regulations and guidance. What is more, as part of the SMS, personnel should be able to carry out the safety processes and practices outlined. Thus, placing the human at the very centre of maritime safety management.

Further to the ISM Code, the IMO also uses the International Convention on Standards of Training and Watchkeeping, to highlight the safety role personnel play (International Maritime Organization, 2016a). For instance, the STCW Convention stipulates that personnel must be able to make a knowledgeable and informed contribution to the safety operation of the ship. Thus, companies are obligated to consider their operation-specific safety requirements and ensure their personnel can demonstrate appropriate skills to fulfil them.

Thus, demonstrating that the IMO, through the application of various instruments, have acknowledged that each company, and role within that company, faces unique safety risks. As such, these safety risks should be addressed by the company, as they are better positioned to determine the appropriate course of action to mitigate each risk. Furthermore, this position of knowledge means the companies are better placed to determine the appropriate type of training that their personnel needs to receive to ensure they can fulfil their safety functions.

Thus, with the IMO placing cyber risk management within the confines of the ISM Code, it explicitly requires maritime personnel to be made aware of the risks posed by cyber, just like any other maritime risk. To manage risk the maritime sector utilises a wide variety of physical, technical and procedural mitigations. Their handling of cyber risk will be no different. However, as outlined above the human element, has always been a central part of the maritime sectors risk management practices. What is more, the human element has demonstrated both its ability to be a weakness and strength in the management of cyber risk. Thus, focus should be given to developing the human elements ability to implement cyber risk management processes, as a way to compliment the technical and procedural mitigations.

4. Training as a Cyber Risk Management Approach

To ensure that the human element is best able to provide a valuable addition to cyber risk management practices they must be have the appropriate skills and experience. The only way to

deliver these skills is through appropriate training. There are many compelling reasons why cyber training should be implemented as a risk management practice. These include:

1) **Attacks are on the rise as more employees are working from home** – Up to 30% of workforce will be working from home at least two days a week in 2021 (Lister, 2021). Hackers are opportunistic and are now using this shift in remote work to prey on unsuspecting and unsecured devices.
2) **Humans are a considered a weakness in an organizations cybersecurity** – 52% of respondents on a recent BIMCO survey consider the humans the most risky part of their cyber risk management practices (IHS Markit, 2020).
3) **Compliance requirements for businesses and operations are increasingly focused on employee training -** Regulatory agencies (NIST for example) emphasize the necessity of not only developing security policies but also ensuring that all users are fully trained in those policies and understand the responsibilities they hold.
4) **Providing basic training once is not enough to educate employees -** Creating regular training that is interactive, and covers multiple topics like phishing, ransomware, business email compromise and physical security is the best way to provide employees with the knowledge to effectively respond to cyber threats.
5) **Anyone can become the victim of a phishing attack -** It is important to remember that no member of any organization is immune from a cyberattack if they are not trained to spot it. Comprehensive cybersecurity training is important for all members of an organization

The concept of including cyber awareness training as part of cyber risk management is not unique to the maritime sector. The International Organization for Standardization (ISO) have been a key driver behind this concept. More broadly, the ISO, through *ISO31000:2009 – Risk Management – Principles and Guidelines* reiterates the importance of implementing adequate training sessions and programs to ensure that personnel are able to adhere to risks management strategies (International Organization for Standardization, 2009). More importantly, the ubiquitous ISO/IEC27001:2013 – Information Technology – Security Techniques applies this risk management logic and applies it to cybersecurity (International Organization for Standardization, 2013). Thus, ISO/IEC27001 asserts that to achieve compliance all personnel shall receive appropriate awareness, education, and training on information security that is relevant to their job role. Furthermore, as seen in the recent version of BIMCO's *Guidelines on Cyber Security Onboard Ships* (BIMCO, 2021), which is held in high regard by the sector, training should cover a broad level of cybersecurity activities, which are both generic and unique to specific operations.

A risk-based approach to cyber security ensure organizations can identify which of their assets or operations represents the highest risk of compromise, and priorities resources accordingly. What is more, this prioritisation should be evaluated regularly as various factors change, including criticality of the system, value of the asset, new known attacks or vulnerabilities etc. When an asset priority list has been created, it is then necessary to assess the vulnerabilities of each.

In this way cyber risk is included within an organizations business risk management. Due to the integration of technology, and overlap in operational and business networks within organizations, this ensures they are considering cyber risk holistically and not as a standalone form of risk. As discussed above, a large part of this risk management includes personnel behaviour, where training needs to be provided to ensure they are able to operate systems safely and securely. Again, this is not a new concept as training is provided to cover all manner of operational risks e.g. fire, evacuation etc.

With the publication of *Resolution MSC.428 (98),* the IMO has drawn a clear link between the development of maritime cyber awareness skills and cyber risk management. The *Resolution* reiterates the "urgent need to raise awareness on cyber risks threats and vulnerabilities to support

safe and secure shipping…" (International Maritime Organization, 2017). What is more, the *Resolution* ties this cyber risk awareness into the provisions of the ISM Code.

The ISM Code stipulates that a "Company should establish and maintain procedures for identifying any training which may be required in support of the SMS and ensure that such training is provided for all personnel concerned" (International Maritime Organization, 2014). Through the inclusion of cyber risk within the SMS it ensures that companies are developing, and delivering training that ensures personnel are able to following instructions and procedures when using on board systems. These training will provide personnel with the skills required to ensure they do not inadvertently compromise the safety or security of the systems they operate.

The requirement for companies to include cyber awareness within their cyber risk management processes is as far as the IMO, as a regulator, goes. Within the various IMO instruments that outline maritime personnel competencies, there is no explicit guidance on what cyber awareness competencies should consist of. Therefore, it is necessary for companies to look further afield and assess what training is appropriate to their operation-specific risks.

One such example is the USCG Work Instruction *CVC-WI-027(1)*, that outlines how cyber risk management will be assessed during the routine inspection of a vessel (United States Coast Guard, 2020). The Instruction argues that if, under questioning, personnel are not able to demonstrate a general level of cyber risk management this could constitute a failure of the ships safety management system. Therefore, to avoid the risk of detention, companies must be providing crews with the appropriate training on cyber risk management processes.

Again, this only provides a brief insight into what is to be expected in one country, which is still a long way from becoming the norm. To address the disparity in implementation of cyber risk management the IMO recommends companies utilise the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2018). Utilising this framework adds enhances the development of processes that are both relevant to the companies risk profile, and consistent across the global sector.

As Gordon et al. (2020) argue, the NIST Framework drives companies to develop cyber risk management practices that are both relevant and cost-effective. Thus, companies must consider all options that maximise the impacts of their investments in cyber risk management. The NIST Framework highlights awareness and training as one of the fundamental elements of the Protect function. Thus, suggesting that training offers a cost-effective method of developing a company's cyber risk management.

Even a small investment in security awareness and training has a good chance of significantly reducing the business impact of a cyber-attack. However, many studies show that the use of multiple methods of training produced the highest correlation to perceived security effectiveness in employees. These different methods can include both face-to-face training or e-learning, this could also include practical session allowing a hands-on approach to training.

Regardless of the method/s selected for delivering training, to ensure that it remains cost-effective it must be appropriate to the personnel its delivered too. This means that when developing training it is important to consider the level of responsibility each personnel has for risk management. For example, the Master has more responsibility than the chief engineer, who in turn has more responsibility than a deck cadet. The EU's Cyber-MAR project provides a good example of how these levels of responsibility can be decided. As illustrated in Table 1**: Description of Cyber-MAR Training Levels** (Authors own elaboration), each level requires more knowledge but helps to ensure a better understanding of the risks that digital technology poses.

Developing this style of hierarchical structure to training delivery, which is based upon a company's specific risk profile, ensures each personnel receives the most appropriate training. Allowing personnel to work their way up through the levels is also important as it ensures they have attained the appropriate skills and experience required before moving to the next level. This will ensure a cost-effective approach to the delivery of appropriate cyber training.

Table 1: Description of Cyber-MAR Training Levels *(Authors own elaboration)*

Complexity level	Details	Requirements	General aims
Entry level	Entry-level users who are not familiar with cyber security **Theoretical**	Nothing officially required since the training will take them into that space for the first time and will be used to grant access to the second level	Training is a basic introduction to cyber security and the concept of Cyber-MAR. The goal is to raise awareness among identified users (very large audience). To give the participant the opportunity to understand cyber security threats and the basic concepts for reducing risk in the maritime sector.
Mid level	Users who are familiar with cyber security and wish to increase their skills to a higher level **Theoretical and hands on**	Middle level : it's a must that they have at least 3 years of experience into networking and security and to have got entry level certificate	The course aims to provide an overview of cybersecurity risks in maritime domain, introducing the **Cyber-MAR concept** and platform (familiarization)
Advanced	Users with high IT security skills, at theoretical and practical level. High security specialists may work as senior positions in IT departments. **Theoretical and hands on**	Mid-level certification plus direct experience on specific security environment , nice to have certifications on cybersecurity and vertical skills like CEH, Comptia Security +, CCDA and ISACA CISM and/or CRISC, but nice to have, not a must have	The course aims to provide a more detailed overview of cybersecurity risks and how good risk assessment will have a positive impact in reducing threats and vulnerabilities in the maritime sector also through the Cyber-MAR approach. The course will be updated with the latest tools on the use of the Cyber-MAR CR together with the recent international legislation and guidelines. Deep dive in Cyber-MAR and CR platform

To help improve the cost-effectiveness of the development and delivery of cyber security training it is important to consider the development of a learning management system (LMS). By way of example, the Cyber-MAR LMS will provide an easily accessible training environment that will complement existing qualification pathways offered by public and private entities. Moreover, it will provide a dedicated training cyberspace and a maritime logistics simulation environment for an integrated training and simulation environment. Keeping training in a central management system ensures all staff are able to access the materials and training they require in a timely and cost-effective fashion. Moreover, an LMS allows a company to monitor its personnel's training, ensuring they are completing content as required. This in turn ensures that personnel remain up-to-date with the latest developments in risk management practices, helping to reduce the risks of a cyber incident.

Finally, as above has mentioned, determining the content of this training is a vitally important step. The development of a comprehensive syllabus ensures that training is representative, and appropriate to a company's risk profile. Ensuring the syllabus considers a company's everyday operations, systems, and personnel skillsets. As such, the primary aims of this training is to ensure that personnel are able to respond appropriately to a cyber incident in a way that ensures the continued safety of ship and crew. These personnel also need to be able to respond to these incidents, and know how to communicate important details of the incident to management or specialised companies.

Again, looking to the nuclear industry where safety training is critically important there is some guidance that can be applied (see **Error! Reference source not found.**). What these course contents do is ensure companies are thinking about their risks, and subsequent associated risks, before developing training content. This understanding is then built into the training ensuring that personnel understand not only the mitigation measures but also the cause of the risks. This allows them to make holistic decisions about risk, as they are better prepared to spot when situation is starting to become unsafe. Developing content in this way ensures that the right knowledge about the high-priority risks is passed onto personnel. This ensures that the development and suitability of the training remains cost-effective, where it will have the largest cost to benefit improvements.

Table 2: Content of Nuclear Criticality Training *(International Organization for Standardization, 2021)*

a)	The nature of a nuclear criticality event, how it can be caused, and the hazards associated with a criticality accident.
b)	The factors affecting nuclear criticality safety.
c)	Past accidents relevant to the type of operations to be carried out and the root causes of these accidents.
d)	Local incidents and deviations relevant to nuclear criticality safety, the reasons they arose and root causes.
e)	Local or site-specific nuclear criticality safety limits, controls/instructions and equipment important to safety, to explain why they are needed and to illustrate the importance of following procedures.

The Cyber-MAR project adopted a similar approach to its training development, and from recent feedback, surveys on delivered training the results are positive. For instance, the overall satisfaction score for the training session was 4.6/5.0. The variance in scores was very low (standard deviation of 0.1746) indicating consistent responses. Respondents were asked to give an overall impression of the training taking into account: content, quality, appropriateness and time allocated. Thus, illustrating that delivering the right content to an appropriate audience helps ensure a cost-effective approach to training as a cyber risk management practice.

It is worth noting that the retention of training is a large factor within cost-effectiveness. If personnel engage with training and then forget it after a period of time it becomes ineffective. However, as suggested above, if content is applicable, and different methods are adopted to deliver training this can help to improve retention. In turn keeping the cost-effectiveness of training high.

4.1. Cyber Ranges as a tool for training

Training increases in effectiveness if it is able to simulate situation that may occur in the respective organizations day-to-day operations. This ensures that personnel are considering cyber risk management holistically. This holistic approach ensures they are considering the implications of their actions on other parts of the network, ensuring they do not inadvertently compromise the safety or security of another system.

One way to deliver this type of training is by using a Cyber Range, where trainees will access a simulated network environment in which they can practice and improve their skills. A simulation environment is a representation of an organization's ICT, OT, mobile and physical systems, applications and infrastructures (NIST, 2020). It includes the simulation of attacks, of users and of their activities and of any other Internet, public or third-party services that the simulated environment may depend upon. An exhaustive survey on Cyber range architectures in relation to training can be found (Priyadarshini, 2018). Cyber Ranges offer the capability to employ tools, attacks and procedures safely without risk to the organisations digital infrastructure.

As discussed above personnel often form the last line of defence in a cyber-attack and experience and practice enhance teamwork and provide the necessary background for smart decision-making during a real cyberattack. Cyber ranges are one of the best ways to run real attack scenarios and immerse the team in a live response exercise. These simulated environments personnel can witness first-hand what a cyber-attack feels like, and how to respond to, and recover from the event. What is more, companies are becoming increasingly aware that their risk management practices, and response plans need to be developed and tested on real-world conditions.

It has become apparent that the all-remote working situation brought about by the Covid-19 pandemic has elevated the priority of digital collaborative platforms when preparing for cyber incidents. More importantly, the rapid increase in high-profile attacks, with large financial implications and subsequent reputational impacts has led to an increase interest in cyber ranges. Damaging attacks, like data breaches and ransomware, have cemented the criticality of effective incident response to prevent worst-case outcomes and rapidly contain eventual ones.

The most compelling reason for building a cyber range is that it is one of the best ways to improve the coordination and experience level of cyber security team. Experience and practice enhance teamwork and provide the necessary background for smart decision-making during a real cyberattack. Cyber ranges are one of the best ways to run real attack scenarios and immerse the team in a live response exercise. As a tool for training and development, a cyber range is then economical investment for a company, with the benefits outweighing both the time and financial investment or purchase and setup.

What is more, may compliance certifications and insurance policies cite the delivery of mandatory various levels of cyber training. These are driven by mandates and compliance standards established by the International Organization for Standardization (ISO). Using a cyber range will not only free up the budget to provide the required training, but also increase the effectiveness of the training.

5. Conclusions

As this paper has discussed the rapid technological advancements and the digital evolution of companies is likely to increase the number of cyber incidents that they face. What is more, the disruption caused by these incidents are likely be wide spread, affecting both the tangible and no-tangible assets of the organisation (CyberWISER, 2019). Protective barriers either in the form of technical protection or human awareness are necessary to prevent attack from impacting companies

business, operations and integrity, which could have a significant impact on the effectiveness and viability of a company.

This paper has argued that the human element within the maritime sector, even though their role may have changed because of technology, remain as a vital part of operations. One of their roles within operations is risk management, and with technology, this includes cyber risk management. As illustrated by the given examples, humans are fallible and their decisions can make all the difference between a well-managed incident and a disaster. To ensure that the human factor are able to make informed decisions involving, and work collaboratively with, technology they must have the appropriate skills.

To provide these skills companies should be considering develop detailed training programmes whose syllabuses consider the specific risk profile of the company. Approaching training in this way, alongside alignment with the variations in responsibility, will ensure effective training is developed and delivered. What is more, the reduction in risk offered by training that is effective and considerate of the company's specific will represent a positive cost-benefit investment.

It is generally recognized that cyber ranges may be one of the most effective ways to train IT professionals in defending against cyber-attacks. The virtual environments deliver simulated real-world attacks that test multiple dimensions and stakeholders within diverse environments (Stone, 2020). As cyber ranges are interactive, simulated platforms and representations of networks, systems, tools, and applications, they provide a safe and legal environment to gain hands-on cyber skills. What is more, the use of these environments stimulates cooperation and confidence growth, which in turn can lead to benefits in cyber risk management.

The adoption of a hybrid approach to training is more effective than a single method approach. In this way, conventional education and training models are insufficient to fill the cybersecurity skill gap present in the sector. As put into evidence cyber ranges provide enabling technology to operationalize, predict, and monitor the training and performance of cybersecurity professionals. Therefore, investments in the development of the right training and the right tools for the job will ensure that training remains a cost-effective risk management practice.

Acknowledgements

This paper is part of the research efforts under Cyber-MAR. The Cyber-MAR project has received finding from the European Union's Horizon 2020 research and innovation program under grant agreement No, 833389. Content reflects only the authors' views, and the European Commission is not responsible for any use that may be made of the information it contains.

References

A.P Møller-Mærsk 'Cyber Security in the Maritime Sector'. *International Maritime Organization - Maritime Safety Committee 101*, London.

Ashford, W. 2016. What is the long-term reputational impact of a cybersecurity breach? - TalkTalk 12 months later. Alva.

Ashford, W. 2019. NotPetya offers industry-wide lessons, says Maersk's tech chief. ComputerWeekly.com.

Aytes, K. and Connolly, T. (2004) 'Computer security and risky computer practices: a raional choise perpectice', *Journal of Organization and End User Computing,* 16(3), pp. 22-40. doi:

Barnett, M. L. (2005) 'Searching for the Root Causes of mariitme Casualties', *WMU Journal of Maritime Affairs,* 4(2), pp. 131-145. doi:

Barnett, M. L. and Pekcan, C. H. (2017) 'The Human Element in Shipping', *Encyclopedia of Maritime and Offshore Engineering*: Wiley Online, pp. 1-10.

BBC 2018. BA investigation into website hack reveals more victims. BBC News.

BIMCO (2021) *The Guidelines on Cyber Security Onboard Ships*, Copenhagen: BIMCO.

Boletsis, C., Halvorsrud, R., J B Pickering, S. P. and Surridge, M. 'Cybersecurity for SMEs: Introducing the Human Element into Socio-tehnical Cybersecurity Risk Assessment'. *Poceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*.

Brower, D. and McCormick, M. 2021. Coloinal pipeline resumes operations following ransomware attack. Financial Times.

Cyber-MAR 2019a. Cyber-MAR - The Project at a Glance.

Cyber-MAR 2019b. Cyber-MAR Fact Sheet.

CyberWISER (2019) *D3.4 EU Cybersecurity legal and policy aspects: Preliminary recommendations and road ahead*: European Union. Available at: https://www.cyberwiser.eu/content/what-cyber-range (Accessed: 30th May, 2021).

Department for Culture Media and Sport (2020) *Cyber Security Breaches Survey 2020*, London: Uk Government. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf.

European Commission 2020. Agriculture and Rural Development Statistical Factsheet - Spain. Brussels: European Commission.

European Union (2016a) *Directive (EU) 2016/1148 - Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (NIS Directive)*, Brussels: European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (Accessed: 15th April, 2021).

European Union (2016b) *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)*, Brussels: European Union.

Fontnouvelle, P. d. and Perry, J. (2005) *Measuring Reputation Risk: The Market Reaction to Operational Loss Announcements*, Boston: Federal Reserve Bank of Boston.

Gillet, R., Hubner, G. and Plunus, S. (2010) 'Operational risk and reputation in the financial industry', *Journal of Banking & Finance,* 34(1), pp. 224-235. doi:

Gordon, L. A. and Loeb, M. P. (2002) 'The Economics of Information Security Investment', *ACM Transactions on Information and System Security,* 5(4), pp. 438-457. doi. Available at: https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P. and Zhou, L. (2020) 'Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model', *Journal of Cybersecurity,* 6(1), pp. 1-8. doi:

Hetherington, C., Flin, R. and Mearns, K. (2006) 'Safety in Shipping: The Human Element', *Journal of Safety Research,* 37, pp. 401-411. doi:

IHS Markit (2020) *Safety at Sea and BIMCO cyber security white paper*. Available at: https://ihsmarkit.com/Info/0819/cyber-security-survey.html (Accessed: 10th May, 2021).

Information Commissioner's Office (2020) *Penalty Notice - British Airways*: Information Commissioner's Office.

International Maritime Organization (1993) *Resolution A.77s(18) - Fatigue Factors in Manning and Safety.* London: International Maritime Organization.

International Maritime Organization (2003) *Resolution A.947(23) - Human Element Vision, Principles and Golas for the Organization.* London: International Maritime Organization.

International Maritime Organization (2014) *International Management Code for the Safe Operation of Ships and for Pollution Prevention.* London: Internation Maritime Organization.

International Maritime Organization (2016a) *International Convention on Standards of Training, Certification and Watchkeeping.* London: International Maritime Organization.

International Maritime Organization (2016b) *MSC.1/Circ.1526 - Interim Guidelines on Maritime Cyber Risk Management.* London: International Maritime Organization.

International Maritime Organization (2017) *Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems.* London: International Maritime Organization.

International Organization for Standardization (2009) *ISO31000:2009 - Risk Management - Principles and Guidelines*: International Organization for Standardization.

International Organization for Standardization (2013) *ISO/IEC27001:2013 - Information Security - Security Techniques*: International Organization for Standardization.

International Organization for Standardization (2020) *ISO 24438 - Ships and Marine Technology - Maritime Education and Training - Maritime Career Guidance*: International Organization for Standardization.

International Organization for Standardization (2021) *ISO23122 - Nuclear Criticality Safety - Nuclear Criticality Safety Training for Operations*: International Organization for Standardization.

Ireland, A. 2018. Here's Why Putting a Price on Reputational Damage Is So Hard — But Totally Worth It. Risk & Insurance.

Kia, M., Stayan, E. and Ghotb, F. (2000) 'The Importance of Information technology in port terminal operations', *International Journal of Physical & Logistics Management,* 30(3/4), pp. 221-344. doi: 10.1108/09600030010326118

Lister, K. 2021. Work-At-Home After Covid-19—Our Forecast. Global Workplace Analytics.

Maddocks, T. 2015. Lessons from the TalkTalk crisis. Media Training Associates.

Meshkat, L., Miller, R. L., Hillsgrove, C. and King, J. 'Behavior Modeling for Cybersecurity'. *2020 Annual Reliability and Maintainability Symposium (RAMS)*.

Ministry of Foreign Affairs 2020. The Spanish market potential for fresh fruit and vegetables. Ministry of Foreign Affairs.

National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity - version 1.1*: National Institute of Standards and Technology.

NIST (2020) *The Cyber Range: A Guide*: NIST. Available at: https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf (Accessed: 1st June, 2021).

Notteboom, T. 2020. Top 15 container ports in Europe in 2019: TEU volumes and growth rates. Port Economics.

O'Neil, W. A. (2003) 'The Human Element in Shipping', *WMU Journal of Maritime Affairs,* 2(2), pp. 95-97. doi:

Offshore Technology 2021. Oil prices surge as cyberattack prompts critical US fuel pipeline closure. Offshore Technology.

Pearson, N. (2014) 'A larger problem: financial and reputational risks', *Computer Fraud & Security,* 2014(4), pp. 11-13. doi:

Pomeroy, V. and Earthy, J. V. (2017) 'Merchant shipping's reliance on learning from incidents? A habit that needs to change for a challenging future', *Safety Science,* 99, pp. 45-57. doi:

Port Authority of Valencia (2019) *Statistical Report Port Authority of Valencia*, Valencia: Port Authority of Valencia. Available at: https://www.valenciaport.com/wp-content/uploads/Statistical-Report-December-2019.pdf.

Port Technology 2020. What is the future of automation?

Priyadarshini, I. (2018) *Features and Architecture of The Modern Cyber Range: A Qualitative Analysis and Survey.*

Reason, J. (1997) *Managing the Risks of Organisational Accidents.* Aldershot: Ashgate Publishing.

Ritchie, R. 2019. Maersk: Springing back from a catastrophic cyber-attack. I-Global Intelligence for Digital Leaders.

Security Boulevard 2019. Why the Cybersecurity Skills Shortage is a Real Nightmare.

Singleton, W. T. (1973) 'Theoretical Approaches to Human Error', *Ergonomics,* 16(6), pp. 727-737. doi: 10.1080/00140137308924563

Stone, M. 2020. Why Cyber Ranges are Effective to Train your Teams. Security Intelligence.

The Guardian 2021. Shutdown of US pipeline after cyber-attack prompts worry over gas prices. The Guardian.

United States Coast Guard (2020) *CVC-WI-027(1) - Vessel Cyber Risk Management Work Instruction*: United States Coast Guard.

Verizon (2020) *2020 Data Breach Investigations Report*: Verizon. Available at: https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf (Accessed: 20th May, 2021).

Vishik, C. and Heisel, M. (2015) *Cybersecurity Education snapshot for workforce development in the EU*: ENISA. Available at: https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/cybersecurity-education-snapshot-for-workforce-development-in-the-eu/at_download/file (Accessed: 30th may, 2021).

Zan, T. D. and Franco, F. D. (2019) *Cybersecurity skills development in the EU*: ENISA. Available at: https://data.europa.eu/doi/10.2824/525144 (Accessed: 30th May, 2021).