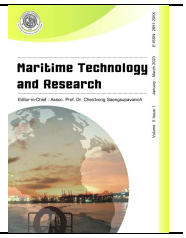
Maritime Technology and Research

https://so04.tci-thaijo.org/index.php/MTR



Research Article

Developing a maritime cyber safety culture: Improving safety of operations

Rory Hopcraft*, Kimberly Tam, Juan Dorje Palbar Misas, Kemedi Moara-Nkwe and Kevin Jones

CyberSHIP Lab, Faculty of Science and Engineering, University of Plymouth, UK

Article information

Received: May 13, 2022
1st Revision: July 25, 2022
Accepted: August 18, 2022

Keywords
Cybersecurity,
Safety culture,
Risk management,
Cyber risk

Abstract

A rise in catastrophic loss-of-life events as a result of poor safety management (e.g., the capsizing of the Herald of Free Enterprise and the Costa Concordia) has driven the maritime sector to improve its safety management practices. This paper will explore the vital role of the human element within safety management, and why, as part of that safety management, organizations must foster a safety culture. This development must be achieved if organizations are to make a significant step forward in preventing similar catastrophes in the future. It is important to note that the development of safety cultures is not new to the maritime sector. However, the increase in connected systems within the sector (e.g., satellite communications) means these safety cultures must now consider the new, or altered, risks posed by digital systems. Therefore, the paper, through a high-level literature review, will consider what the core elements of a cyber safety culture are, and how an organization company can nurture its development, both internally and across the wider sector. The paper will discuss the various benefits of developing a robust cyber safety culture, including demonstrable compliance to the International Maritime Organization's (IMO) cyber regulation, Resolution MSC.428(98). The paper will conclude by arguing the development of a cyber safety culture is not going to remove all risk completely, but rather will allow organizations to be better prepared for when incidents do occur.

1. Introduction

The various, high-profile incidences of the 1980s (e.g., Chernobyl and the Herald of Free Enterprise) were responsible for raising global recognition for the need to develop stringent safety management systems. 193 lives were lost in the Herald of Free Enterprise incident alone, and the health effects of Chernobyl are still being felt today. Through the past half-century, many sectors, including the maritime sector, have made great strides in developing and enhancing their safety management systems after witnessing the damage that could happen if there are not any in place (International Transport Forum, 2018).

As part of the response to these loss-of-life incidents, and others like September 11th (2001) and the USS Cole (2000), the International Maritime Organization (IMO) introduced the International Safety Management (ISM) Code and the International Ship and Port Facility Security

*Corresponding author: *CyberSHIP Lab, Faculty of Science and Engineering, University of Plymouth, UK*
E-mail address: rory.hopcraft@plymouth.ac.uk

(ISPS) Code. Both of these codes, the first focusing on safety, the second focusing on security, brought in to place mandatory provisions in an attempt to raise the minimum level of both safety and security in the maritime sector. One such provision was the development of a safety culture, which the IMO defines as "a culture in which there is consideration informed endeavor to reduce risks to the individual, ships and maritime environment to a level that is 'as low as is reasonably practicable'" (International Maritime Organization, 2003a).

Therefore, in order to reduce risks, organizations must develop a close relationship between their safety culture and Safety Management System (SMS) (American Bureau of Shipping, 2016), and embed this mindset into every operation (Corrigan et al., 2019). This close relationship between safety management and safety cultures is now more critical than ever, as the current state of digital integration mandates that this minimum level of safety needs to be raised yet again. The integration of digital systems into everyday operations has brought with it many benefits, and has been seen as a way to improve both safety and security. These improvements help to reduce the risk posed by operations to the lives of personnel. However, as highlighted in the recent International Association of Classification Societies (IACS) Unified Requirements for Cyber Resilience of Ships (International Association of Classification Societies, 2022a), this digital integration has opened organizations and personnel up to a new range of safety risks, whereby digital systems could be compromised, leading to safety-compromising incidents; for instance, the potential increase in human stress and resulting errors due to the adoption of technology like automation (Tam et al., 2021).

This paper will argue that, to manage these new risks, organizations must now adapt their safety cultures to include elements of cyber risk within them. Otherwise, changes to behavior may not be maintained, and solutions would likely not be implemented properly. It is worth noting the IMO have a distinct differentiation between safety and security, indicating that a safe culture is not inherently a cyber-secure culture, whereby safety is defined as protection from injury due to non-intentional events like accidents, and security is protection from intentional events (International Maritime Organization, 2020). However, recent cyber incidents affecting the maritime sector, most notably the 2017 NotPetya incident that struck shipping giant A.P. Møller-Mærsk, illustrate that technology can affect both safety and security. As argued by the International Atomic Energy Agency (2020), the management of safety and security often occurs at the same time, with organizations dealing with the consequences of an incident in the same way regardless of its initial cause. For instance, the initial response to a failure of a ship's navigation system would be the same, regardless of whether the cause of the outage was a power failure or a cyber-attack.

As will be discussed later, the IMO have adopted the term 'cyber risk management', under the remit of the ISM Code. Therefore, to ensure consistency in terminology with the already established safety cultures, the authors opted for the term cyber safety culture. However, as discussed above, it is important that organizations approach these cyber safety cultures holistically, and include both accidental and deliberate events. Due to the link between cyber risk and safety, failure to include these new risks, especially with more digitalization and automation coming every year, would render the safety culture ineffective, putting the safety of maritime infrastructure and personnel at risk.

This paper will review academic literature and the regulatory requirements of safety cultures and explore how and why maritime organizations need to develop a cyber safety culture. Firstly, the paper will discuss the relationship between safety and risk management. Secondly, the paper will explore the importance of cyber risk management and the role that the human element plays in its continued safety and security. The next section will discuss the importance of developing a cyber safety culture, whilst briefly outlining some of the core benefits of doing so. The final section of this paper will discuss the development of a cyber safety culture and argue the importance of allowing personnel to experience risk as a way to facilitate an improved safety culture.

2. Safety and risk management

Various high-profile incidents during the 1980s demonstrated the need for organizations to implement effective risk management practices to ensure the continued safety of operations. This section will explore this relationship between safety and risk management and how this can now be applied to cyber risk. A series of failures in safety tests in 1986 ultimately led to an explosion in a reactor at the Chernobyl Nuclear Power Plant. Early investigation reports argued that human error had been a major contributor to the disaster (International Nuclear Safety Advisory Group, 1986), with the initial response to the safety incident deemed inadequate (Nuclear Energy Institute, 2019). Later reports have argued that the company failed to articulate, and circulate, safety policies and procedures appropriately with personnel (World Nuclear Association, 2021), leading operators to make their own interpretations of the best course of action. However, without possessing an adequate understanding of safety, and its consequences, operators were unable to make informed decisions. The year following Chernobyl, the ferry *the Herald of Free Enterprise* capsized shortly after leaving Zeebrugge, Belgium. The inquiry into the incident commented that the company, from top to bottom, was "…infected with the disease of sloppiness" (Department for Transport, 1987), where proper consideration had not been given to the safety systems in place.

These high-profile safety-related incidents led to the IMO formally recognizing the importance of improving safety of operations within the maritime sector. To this end, the IMO adopted various resolutions which stipulated stronger safety management practices on ships (International Maritime Organization, 1988, 1989). These culminated in the development and ratification of the ISM Code (International Maritime Organization, 2014) as a mandatory part of the Safety of Life at Sea Convention (SOLAS) (International Maritime Organization, 2020). The adoption of the ISM Code was to ensure all governments and companies took the necessary steps to ensure the implementation of risk management practices that improved the safety of maritime personnel. In conjunction with these codes, people in the sector also started creating risk management frameworks. These helped people understand, visualize, and meet new safety codes in day-to-day operations.

One way to view risk management is Reason's *Swiss Cheese Model* (Reason, 1997), where risk management relies on the development of different layers of mitigations (see **Figure 1** for an example). These mitigations can include hardware, software, or policies and procedures. However, like its namesake, these layers have weaknesses (holes). The aim of an effective SMS is to ensure that those holes do not align. Since its creation, this has been a very popular risk view, as readers tend to find it easy to comprehend. Therefore, the authors use this model to illustrate a gap in today's risk management, the gap of cyber-security.

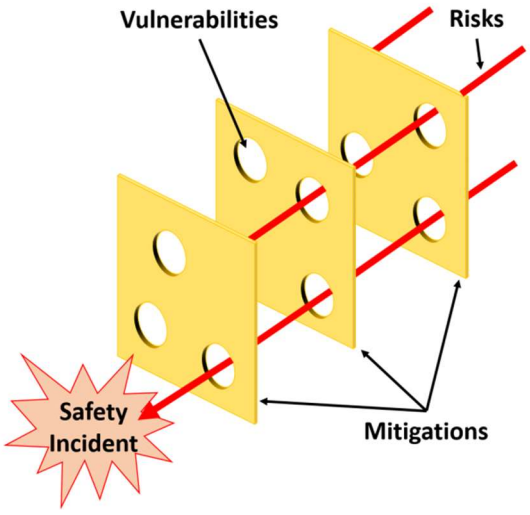


Figure 1 Reason's Swiss Cheese Model (Source: Reason (1997)).

However, as the loss-of-life incidences given above highlight, operational safety is contingent on the interactions between man and machines, which Emery and Trist describe as a socio-technical system (Emery & Trist, 1960). As Baxter and Sommerville (2011) argue, system performance relies on the optimization of both the technical and social elements. However, risks can arise within the system, due to ill-structured or mismanaged interactions between these elements (Pidgeon & O'Leary, 2000). For example, if the technological or procedural solution is too cumbersome, personnel may find workarounds that, again, affect safety, e.g., using generic passwords.

Figure 2 demonstrates how the *Swiss Cheese Model* can be used to visualize critical elements involved in the safety of socio-technical systems like ships. Firstly, the governance layer, which represents the regulations and laws that organizations must abide by. The second layer is the management layer, which is the internal policies and practices that govern an organization's specific risk profile. The third layer is the technical layer. This layer comprises the technical and, often, digital safety management and mitigation systems. The final layer within the maritime safety system is the human element, the people who are responsible for operating within the safety constraints of the company.

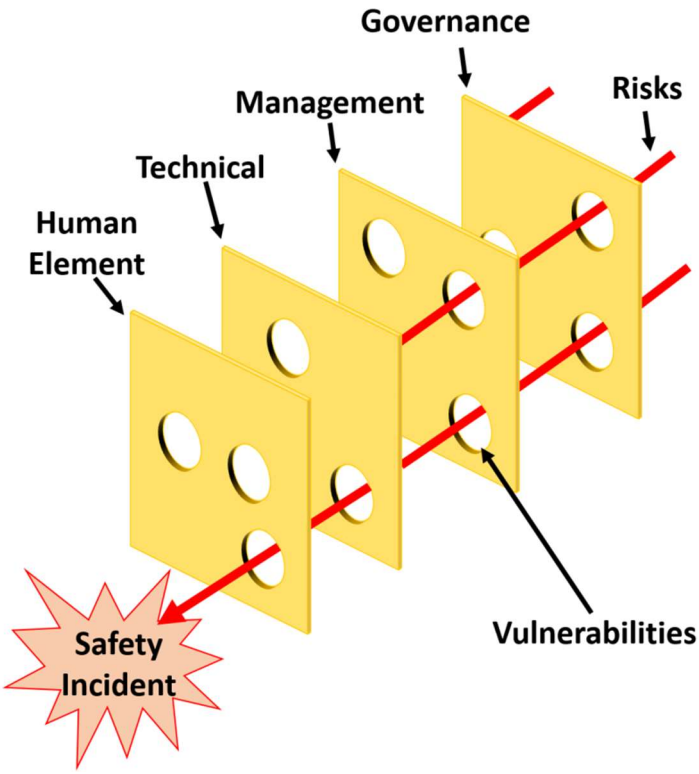


Figure 2 Maritime Risk Management Swiss Cheese, developed by the authors.

By applying this multi-layer approach to the *Herald of Free Enterprise* incident, it becomes clearer how a combination of failures in each layer led to the capsizing of the ferry (see **Table 1**). It is important to note that, in isolation, it is unlikely that any of these failures would have led to the catastrophic event occurring. However, when coupled together, a risk penetrated all the layers of mitigations, allowing the safety incident to occur. As will be discussed next, cyber risks often differ from accidents, whereby risks do not transverse these mitigations in a traditional manner.

Table 1 Factors leading to the capsizing of the Herald of Free Enterprise (adapted from Department for Transport (1987)).

Failure in…			
Governance	**Management**	**Technical**	**Human Element**
Bow and stern loading doors were only required to be weathertight (a lesser watertightness level).	Memorandum sent to operators pressuring them to load and leave Zeebrugge 15 mins ahead of schedule.	Lack of foolproof system to indicate to bridge that the doors have been closed.	The Captain accelerated rapidly, causing water to flood the car deck.

2.1 Managing cyber risk

The management of cyber risk can differ from the management of traditional risks on board, like fire. As illustrated by *the Herald of Free Enterprise*, these catastrophic safety events are 'black swan' events, whereby a certain set of circumstances align, allowing the incident to occur. However, in the case of a cyber-attack, the risks can transverse the layers within the safety system, as attackers actively look for vulnerabilities in both systems and people. Therefore, in comparison to **Table 1**, an accident, the authors will now go through the stages of a common attack chain. This demonstrates how an attack does not leave things to chance (i.e., a straight line on the Swiss cheese model), but actively seeks vulnerabilities at each layer in a flexible, often intelligent way.

Consider the initial stages of a well-established intruder cyber-attack chain (see (SANS Institute, 2016) as an example). Firstly, the majority of digital attackers will deploy reconnaissance attacks on the target system, looking for weaknesses in the system, its integration, or its operators. Those that do not carry out these attacks are less likely to find and exploit vulnerabilities, making them less of a threat. If an attacker is persistent, they will look for multiple vulnerabilities. Secondly, armed with that knowledge, an attacker can then craft an attack chain that best exploits these vulnerabilities, across people and systems. This could include zero-day exploits, which utilize unknown weaknesses in the systems code. Thirdly, the attacker will deliver the attack. If the first attempt fails, for example, the recipient does not click on the malicious link, then the attack could try another route, e.g., a USB drive loaded with malicious code.

This ability for cyber intruders to actively look for vulnerabilities often makes the human element the last barrier of defence within the cyber risk management system (Barnett & Pekcan, 2017). Therefore, the human element must be able to make decisions that do not introduce new vulnerabilities to the model. An example of such would be writing a password down and sticking it to the terminal it is used to login with. Here, the management mitigation is to have a password policy, and the technical mitigation is the system requiring a password with certain characteristics, and yet the human element has introduced a vulnerability by writing it down for all to see.

Despite the fact that there are many layers to the safety/security issue, as seen in **Figure 2**, it has been argued that the human element remains one of the biggest internal threats facing the cybersecurity of organizations (Boletsis et al., 2021; Meshkat et al., 2020). Findings from BIMCO's latest cybersecurity white paper support this assertion, with 52 % of respondents identifying people as their organizations' biggest cybersecurity vulnerability (IHS Markit, 2020). Moreover, Verizon's 2020 Data Breach Investigations Report found that 20 % of all reported breaches were caused by human error (Verizon, 2020).

To this date, the maritime sector is still reliant on the human element, meaning that the human is an accepted risk, which has often led to a complex relationship between safety and human activity (Barnett & Pekcan, 2017). Human activities within the sector are a complex multi-dimensional issue, as these include "the entire spectrum of human activities performed by ships'

crews, shore-based management, regulatory bodies, recognized organizations, shipyards, legislators, and other relevant parties…" (International Maritime Organization, 2003b). While digital technology is changing the sector and the role the human element plays in it significantly, operations are still reliant on people (Kia et al., 2000).

The use of risk management methods, such as good management policies, training, and the attainment of suitable qualifications and experience, can reduce the risks posed by the human element (Berg, 2013). Therefore, an approach is needed that ensures personnel are equipped with the right knowledge and skills to ensure that, as operators or custodians of digital systems, their actions and the actions of others do not compromise the safety of operations. As such, the human element must be aware of the safety risks, digital and non-digital, during operations, and of appropriate management practices. The nurturing of a safety culture offers a framework in which an organization's personnel can effectively implement a risk management system.

3. Safety cultures and the inclusion of the human element in risk management

To manage the safety risks of these complex systems of humans, machines, and policies effectively, the IMO stipulates organizations should be developing "a framework for understanding the complex system of interrelated human element factors, incorporating operational objectives, personal endurance concerns, organizational policies and practices… in order to facilitate the identification and management of risks in a holistic and systematic manner" (International Maritime Organization, 2003b). One such way to embrace this holistic approach is through the development of a safety culture, which is one of the primary aims of the ISM Code (Anderson, 2003). However, it is worth noting that Kongsvik et al. (2013) argue that one of drawbacks of this approach to safety is that it is too prescriptive, and seafarers see safety mitigations as a set of detailed rules with little room for interpretation or improvisation. In comparison, as will be discussed below, the development of a safety culture empowers personnel to make informed safety-related decisions, allowing for a degree of improvisation in response to risk. What is more, there are other benefits to the organization in adopting a holistic approach to safety cultures, including the demonstration of compliance, the reduction of human risk, and potential insurance benefits.

Looking to the nuclear energy sector, who have been at the forefront of safety culture development, the International Safety Advisory Group stated a safety culture is "that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear power plant safety issues receive the attention warranted by their significance" (International Nuclear Safety Advisory Group, 1991). Therefore, while now dated, this definition remains relevant, arguing that safety should be understood to be, and is accepted as, the number one priority for all organizations.

Changes to risk management post-9/11 has also helped to distinguish the role of a safety culture in security. As such, the US Federal Aviation Administration argue that a positive safety culture is built upon five behavioral principles: informed culture, flexible culture, reporting culture, learning culture, and a just culture (Quezadra, 2016). An informed culture ensures personnel are knowledgeable about the human, technical, and organizational factors that determine safety. A flexible culture allows personnel to adapt organizational process when facing certain kinds of risks, especially those that are unexpected. A reporting culture goes hand-in-hand with a just culture, where personnel are prepared to report their errors without fear of reprisal. Finally, a learning culture is demonstrated when people have the willingness and the competence to draw conclusions from safety information systems. Thus, personnel engagement is a key element within a safety culture.

The findings of Clark (2020) divides personnel engagement with organizational safety culture into four stages. In the first stage, *inclusion safety,* personnel feel safe in belonging to the team, whereby they feel their practices and behaviors align well with the group. In the second stage, *learner safety,* personnel feel able to learn through asking questions of others within the group.

These questions can help develop an understanding of how the group does 'safety', and why it does it in this way. In the third state, *contributor safety,* personnel feel safe in contributing their own ideas without risk of embarrassment, ridicule, or punishment. This enhances the engagement and empowerment of all personnel in safety practices. The fourth and final state, *challenger safety,* involves members questioning others' (in particular those in authority) ideas or suggesting significant changes to safety; thus, demonstrating that, through actively encouraging personnel engagement with risk management, a more effective safety culture can be developed.

It is worth reiterating that one of the central tenets of the successful development of a safety culture is the idea of a just culture, which has been recognized as an important attitudinal change within the maritime sector. The IMO (2011) argue that a just culture is founded on two principles: 1) human error is inevitable, and 2) everyone is accountable for their actions if they knowingly violate safety procedures. A just culture, therefore, should not punish people for genuine mistakes. With management actively engaging with and encouraging others to step forward, it allows lessons to be learnt from mistakes and for development to occur. For example, the Nautical Insititute (2020) discusses how safety practices can be improved considering information gained from an official accident report. What is more, this managerial investment ensures personnel feel empowered to come forward, discuss risk in a safe environment, and have an invested interest in the development of better risk management practices.

One such example of this type of practice is in intent-based leadership. Intent-based leadership was first developed by David Marquet, whilst Captain of the Santa Fe Submarine (Marquet, 2015). The concept involves passing decision-making to those closest to the information, rather than those with the highest rank or authority. In this way, all personnel feel involved within the decision-making process, and are able to contribute their ideas based on their own experiences and practices, as illustrated in Fernandez-Salvador et al. (2017). This example, along with the highlighted elements of an effective safety culture, reiterates the importance of developing a safety culture. What is more, they highlight the important role that the human element plays in the development of an effective safety culture and subsequent risk management.

3.1 Benefits of a cyber safety culture

With the ratification of MSC.428(98), as of January 1st 2021, a company's SMS must now consider cyber risk management (International Maritime Organization, 2017). The inclusion of cyber risk into the SMS ensures that there is a commitment to its effective management, as well as for practical benefits, and that it is not merely a 'paper exercise'. Without the inclusion of cyber risk management in the SMS, there is a risk that, in a complex organization, safety management becomes inconsistent, under-resourced, and not business driven (Gordon, Perrin, & Kirwin, 2007). Successfully developing a safety culture that is considerate of cyber risk will have many benefits to an organization.

Demonstrates compliance

As Golay (2000) argues, the traditional prescriptive regulatory approach to safety often constitutes a checklist exercise, which fails to promote uniform levels of safety amongst different elements within the same sectors. As highlighted by May (2007), there should be a move towards a risk-informed approach, which allows regulation to ensure safety is managed appropriately by each organization, without being limited to prescriptive requirements. One such way to do this is through the development of compliance to a safety culture. This approach to safety management reiterates the need for companies to engage with, understand, and mitigate the risks their operations face, in order to remain compliant with regulations.

Furthermore, a successful cyber safety culture must provide demonstrable understanding of cyber risk to ensure compliance with Resolution MSC.428(98). The US Coast Guard's Work Instruction CVC-WI-027 argues that, if under questioning, crew are not able to demonstrate a

general level of cyber risk management, this could constitute a failure of the SMS, leading to the detention of the ship (United States Coast Guard, 2020). As such, due to the hierarchical nature of command on-board, safety considerations depend upon the actions of the master and officers (Räisänen, 2009). The development of a cyber safety culture ensures that these personnel are able to make informed decisions about safety. Furthermore, the encouragement of a cyber safety culture that encourages the empowerment of all personnel will allow lower-ranking crew to feel comfortable discussing safety practices with their superiors (Drouin, 2010), a process that actively strengthens the safety culture throughout the organization.

Reducing the human risk

Secondly, the development of an effective cyber safety culture will reduce the risk that the human element poses to safety, and allow employees to "become robust human firewalls" against cyber incidents (European Union Agency for Network and Information Security, 2017). The strengthening of the human element will have a significant impact on cyber risk management across the organization. As illustrated by the 2017 NotPetya incident at A.P. Møller-Mærsk, the consequences of a cyber incident can be non-trivial. While events of this scale are rare, and the likelihood of the human element being able to stop them is low, they illustrate that, if personnel are prepared for these events, they may make decisions that limit the incident's impacts. The NotPetya incident destroyed 55,000 computers and 7,000 servers (Ashford, 2019) owned by Mærsk, costing around $40million to recover (Møller-Mærsk, 2019).

It has been argued that the cause of most safety-related incidents can be traced back to inadequate training, instruction or attention (Singleton, 1973). What is more, the latest Verizon Data Breach report highlights that 85 % of all data breaches involve the human element (Verizon, 2021). This, coupled with studies by various academic institutions, suggests that more focus needs to be paid to developing humans as robust firewalls. One of the major takeaways from those studies is to get personnel to question their actions and consider the implications of them on safety. For instance, the social experiment carried out by Tischer et al. (2016) found that, when dropping memory sticks randomly on campus, up to 98 % were plugged into a computer. Encouragingly, the later experiment by Bullée et al. (2015) found that interventions that form part of a company's safety culture, like posters, emails, or warning labels, helped to reduce the success rate of attacks. This study also raises the need for personnel to question the presumed authority of individuals approaching them. In a maritime context, this would involve crew questioning and verifying the presence of external personnel (e.g., engineers) on board.

Financial implications

Thirdly, the improvement of a company's cyber safety culture will also help to avoid other financial implications like regulatory fines or reputational damage. If doing business within Europe, companies must comply with the EU's General Data Protection Regulation. Failure to ensure adequate date security could lead to a hefty fine of €20 million or 4 % of global turnover. The 2018 British Airways data breach that affected over 380,000 transactions (BBC, 2018) illustrates the consequences of poor data protection. While the final fine was reduced because of the global pandemic, the initial fine was expected to be around £183.39 million (Information Commissioner's Office, 2020). The negative publicity from these types of incidents and their handling often damages a company's reputation. Consequently, there can be a fall in customer or investor confidence, which ultimately has an impact on the financial stability of the company. Through the improvement of a cyber safety culture, a company is more aware of the risks digital technology poses to its data, and its personnel are better prepared to mitigate those risks. A company that implements a high-level of cyber security can, in the event of a major incident, assure customers that cyber security is taken seriously, thus, helping to mitigate some of the negative implications of the incident.

Insurance value

The final benefit of a developed cyber safety culture that this paper explores is the reduction in insurance premiums. Many of the Classification Societies, who are responsible for ensuring ships are up to code, have now introduced some form of cyber notation (e.g., Lloyd's Register's CyberSAFE notation (Lloyd's Register, 2021)). The notation acts as verification that a ship and its crews are managing cyber risk adequately onboard. This notation can then be used as proof with insurers to illustrate the company is:

1) Compliant with current international regulations;
2) Aware of their cyber risks;
3) Have adequate safeguards in place to mitigate those risks.

This reduction in risk means they could be offered better insurance premiums, because the likelihood of a cyber-incident occurring is reduced. Furthermore, as the US Coast Guard illustrates in its enforcement of MSC.428(98), being able to show appropriate cyber risk management practices also demonstrates compliance.

4. Developing a cyber safety culture

This article has outlined the importance and potential benefits for organizations to develop a cyber safety culture. However, it is also important to consider how an organization can develop such a culture. Therefore, it is important to consider the definitions used to describe these cultures. Within the literature, there is often a distinction between a safety culture, a cybersecurity culture, and an information security culture. In their detailed analysis of information security cultures, Veiga et al. (2020, p2) offer two clear definitions. A cybersecurity culture "relates to the manner in which people perceive cybersecurity and the resultant behaviour in cyberspace that impacts on the protection of the digital information, systems and people", whereas an information security culture focuses on the way in which personnel process information, and how this has an impact on its protection.

Individually, these definitions do not cover the full concept of a cyber safety culture within a socio-technical system. The cybersecurity culture definition limits the behaviors to personnel within the company, and fails to address those externally aiming to do harm. The information security culture is limited to the information. From the understanding that safety cultures must be developed from within a socio-technical framework, these definitions do little to incorporate the multifaceted relationships between the various elements of a socio-technical system. These definitions also do not address the risks that operations pose to the safety of digital systems. For example, extreme weather, like ice or fog, can have a detrimental impact on digital systems. These operational factors pose risks to safety, and have nothing to do with the human element, aside from the fact that they are expected to continue to operate safely when these systems are compromised.

In his review of Australian cyber security culture initiatives, Alshaikh (2020) argues that little is known about how organizations can develop effective cyber security cultures. Zhang et al. (2002) highlights there are some common features of a successful safety culture that can be used to understand how one might be developed. Firstly, safety cultures are a concept defined at a group level, i.e., at an organizational level. Secondly, they are developed through the contribution of all individuals within the organization. Thirdly, once developed, these safety cultures are relatively enduring, stable, and somewhat adaptable to change.

The release of Resolution MSC.428(98) by the IMO in 2017, whilst mandating the inclusion of cyber risk in a ship's SMS, also provides a definition of cyber risk. Covering both accidental and deliberate events, cyber risk refers to a "measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures…" (International Maritime Organization, 2021). Thus, companies, as part of their risk management processes, should be developing a safety culture that includes the identification, assessment, and mitigation of cyber risks.

Looking at the maritime sector specifically, Drouin (2010) outlines the core elements of a well-developed safety culture (**Figure 3**). Firstly, there is engagement from all levels of the organization, from shore-based leadership to the crew, thus allowing the safety culture to be informed and defined at a group level. Secondly, all individuals within the organization have a responsibility for informing safety. For instance, the crew at the very top of the pyramid are expected to contribute and question the risk discussions with the aim to bring about improvements, whilst shore-based leadership are expected to provide the overarching risk management objectives that are considerate of the organizational structure and operations. All of these elements remain true in the development of a cyber safety culture.

The safety culture structure presented by Drouin (2010) places shore-based leadership as the foundation of an organization's safety culture, and is responsible for engaging with others within the organization and experts external to synthesize the understanding of risks with the day-to-day operational requirements. However, in one report, respondents raised concerns that ashore personnel lack at-sea experience, which erodes their ability to make key safety decisions which could affect the ship (Maritime & Coastguard Agency, 2004). With the integration of highly complex systems onboard ships, these tensions are likely to worsen. In particular, engineers ashore are likely to have a better understanding of the digital systems, yet lack a maritime awareness. The reverse is true for shipboard leaders, where they lack the digital awareness, but have an abundance of maritime experience. Therefore, a balance between these experiences is required, and a company should be aware of the tensions that can manifest, while actively mitigating them to ensure they do not have a detrimental impact on the cyber safety culture.

Figure 3 Safety Culture Pyramid- adapted from Drouin (2010).

As one of the largest Classification Societies, representing 18 % of the world's fleet, the American Bureau of Shipping (ABS) are key drivers in the development of a safety culture within the maritime sector (American Bureau of Shipping, 2019). To see these improvements, organizations must identify areas of strength, weaknesses in defenses and opportunities for improvement against incidents (American Bureau of Shipping, 2014). As such, ABS have developed the core safety features they believe need to be present and enhanced to ensure the development of an effective safety culture (see **Table 2**).

Table 2 Core safety factors of an effective safety culture (adapted from American Bureau of Shipping (2014)).

Safety factor	Definition
Communication	Vertical and horizontal communications channels are open and effective.
Empowerment	Individuals feel empowered to fulfil their safety requirements, which are clearly defined by the organization.
Feedback	Priority is placed on the communication and response to safety issues and concerns
Mutual Trust	Individuals trust that managers do the right thing to support safety, and take on their responsibilities
Problem Identification	All individuals have experience and training to recognize unsafe acts and take avoidance measures.
Promotion of Safety	Management leads the way in promoting safety as a core value to the organization. Not just seen as a for-profit exercise.
Responsiveness	Individuals are responsive to the demands of their jobs, including unexpected events and emergencies.
Safety Awareness	All individuals have a strong awareness of their responsibilities for their safety and the safety of co-workers, organization, and the environment.

The elements within this table are fully transferable to cyber risk and, as such, can act as a starting point for the development of a strategy to enhance the cyber safety culture of an organization. For example, with communication, it is vital that organizations understand their communication channels and how these might pose challenges to communication during a cyber-attack, particularly if they utilize Voiceover IP. Furthermore, the organization should be developing communication strategies that allow the fast and effective communication of information pertaining to a cyber-incident, allowing for rapid and appropriate responses. As a broader strategy, the organization could be considering the development of cyber risk awareness training. Through this training, personnel are provided with the awareness of the risks that digital technology poses to safety, the tools to identify potential problems, and the skills to respond to them.

Thus, by an organization embedding these core safety factors into everyday practices, and encouraging all levels of an organization to be involved, a safety culture can be developed and enhanced. Keeping these factors as central tenets in safety culture development will allow cyber risk to be included. For example, having clear and effective communication channels about cyber risks ensures that all personnel know who to talk to if they have any concerns or issues. The promotion of cyber safety, by demonstrating and implementing best practices, will ensure all are aware of the correct processes for digital safety. Finally, the delivery and enhancement of cyber safety awareness will raise the knowledge base and skillsets of all personnel, and ensure that they understand their roles and responsibilities in terms of cyber safety.

4.1 Practical implications of developing a cyber safety culture

It is important to remember that organizations should already have well-established safety cultures in place, and the inclusion of cyber risk into these are just an adaption. However, it is important to consider the practical implication of including cyber risk within a developed safety culture.

Within cyber security, there are three important principles- usability, security, and functionality- that all interrelate, and which form what is often called the security triangle. Good

security measures should have a good balance between these three elements; if an imbalance occurs, an erosion in the security posture can ensue. In some circumstances, this could have a negative impact on the security culture.

For example, consider the application of a strict password policy for logging into bridge equipment. Firstly, technical settings could require users to create passwords with certain requirements (length, type and formation of characters, etc.). This would increase the security of those devices, as it would reduce unauthorized access. Most people are used to these requirements so, again, the policy will be reasonably functional and will not impact usability. However, consider that the device settings might mean it logs out after a few minutes of activity, and that the device is being used during critical operations (e.g., berthing). As the crews only visually interact with the data displayed on the device, and do not interact with it as expected, the device could log out at a critical moment as a part of its programmed security policy. The loss of this information could have an impact on the safety of the crew, and expecting the crew to consciously interact with this device to stop it logging out is not practical. Therefore, the usability of strong passwords and automatic logging out logic on that device is reduced, creating an imbalance. This, in turn, could lead the crew to develop workarounds for this security measure, i.e., completing those operations without that device's information, which is an erosion of the safety culture.

The various cyber risks to modern ships include spoofing of GPS signals received by the ship. Over the past five years, there have been several high-profile reports suggesting state-level actors have used GPS spoofing intentionally. Firstly, Russia was accused of using spoofing as a tactic to fool GPS-guided weaponry. However, as a consequence, the navigational equipment of ships displayed wildly inaccurate positions, which could have an impact on the safety of crews (Hambling, 2017). The second example saw Iran accused by the US of jamming GPS signals so that vessels inadvertently sailed into Iranian territorial waters so they could be detained (Bockmann, 2019). Again, this geopolitical motivation could have an impact on the safety of crews.

The development of a cyber safety culture, whilst not completely removing the risks of GPS spoofing, could allow the risks it poses to safety to be managed. For instance, empowering those at the top of the safety culture pyramid to question when something does not look right might enable earlier notification of the issue. What is more, providing ongoing training on how to mitigate these types of incidents so that they become habitual, for example, using a secondary device for position, will reduce the impact of the incident.

Another type of attack that a developed cyber safety culture might help mitigate, or at least reduce the impacts of, is phishing and ransomware. The US Coast Guard, through their Marine Safety Information Bulletin, have drawn attention to several such cases impacting the maritime sector (United States Coast Guard, 2019a, 2019b). The UK's National Cyber Security Centre (NCSC) argue that eradicating the risk from phishing is difficult, and can only be done through implementing technical, procedural, and social measures (Centre, 2020); for instance, installing and updating anti-virus software to manage the consequences of opening a phishing email, or provide means for users to respond appropriately if they receive such an email. The development of these measures, along with the behavioral aspects, will enhance the cyber safety culture of the organization. Again, empowering individuals to question the communications they receive leads them to feeling valued in reporting those they feel are not legitimate. What is more, enforcing the just culture mentality, along with instilling trust in technical mitigations, will enable personnel to feel confident in reporting instances where they have clicked on a link in a phishing email.

IACS has released two new documents outlining various new cyber risk management requirements for all ships constructed on, or after, 1 January 2024. E26 and E27 both consider the cyber resilience of ships and their on-board equipment. Through the requirements laid out in E27, organizations will need to provide detailed system documentation, which includes key information such as recovery plans (International Association of Classification Societies, 2022b). E26 clearly identifies the key systems that could pose a safety risk to crew if they became victims of cyber

incidents, and lays out various technical and procedural measures through which cyber resilience can be improved; for example, physical access control or manual control capabilities. Through these two sets of requirements, IACS obligates companies to develop and implement an effective cyber risk management system which helps crew Identify, Protect from, Detect, Respond to, and Recover from cyber incidents. The development of these measures, and the provision of training and awareness of the risks and mitigation measures, will help to enhance not only the cyber resilience of ships, but also help improve the cyber safety culture. For example, through companies investing the time and effort to provide adequate documentation for systems, it will show their high-level commitment to cyber safety. The provision of training, information, and tools to manage these risks will increase crew trust in systems. As this paper has reiterated, companies need to listen to and work with crews to develop these documents, as this helps improve commitment to cyber safety from all levels of the organization.

4.2 Experiencing the safety culture in action

A vital process of ensuring the development of an effective safety culture is for seafarers to experience safety management practices in action. As stipulated in the STCW Convention (International Maritime Organization, 2016), *Sea going service* is a fundamental component of maritime training. Without the required amount of time spent at sea, an individual will not be certified competent to sail. The UK's Maritime & Coastguard Agency (2004) regard competency as a combination of the following factors:

- Knowledge
- Skills
- Experience
- Training

This mandated period at sea offers practical experience to cadets, allowing them to transfer the skills learnt ashore to seagoing operations. It is during this time that cadets will experience many of the operational risks and their mitigations, which are discussed during land based training. Further to this, the route from a cadet to a Master is again contingent on the factors above, which is achieved through time spent onboard; in the UK, this equates to 36 months of seagoing time (Maritime & Coastguard Agency, 2015). Thus, the ability to experience and practically implement skills and knowledge in real operations is a core component of competency at sea.

It is, therefore, vital that cadets experience risk during their operations, and feel they are a positive and proactive part of the company's safety culture. This engagement with the safety culture consists of two elements. The first is the opportunity to experience risk. This means that cadets should not be shielded from risk, and should be encouraged to take appropriate risks, to both learn and experience how these are managed and mitigated. Having this opportunity to experience risk, and the safety culture in action, leads to the second element. As illustrated in **Figure 3**, all members of an organization have a responsibility to engage with the development of a safety culture. Therefore, allowing cadets to experience risk appropriately will allow them to understand why certain procedures are how they are, whilst allowing them to potentially offer their own thoughts and experiences to the safety process.

However, it is important to note that Dickety et al. (2002) found that established workers can often be the worst offenders for cutting corners in safety. Therefore, it is important to ensure that, just because personnel are experienced, they are not encouraging those with less experience to disregard the safety processes that form part of the safety culture. What is more, the safety culture should empower others to challenge those practices.

As has been alluded too throughout this article, communication is a key component of a safety culture. Glendon & McKenna (1995) suggest that organizations with positive safety cultures all share the same characteristic of effective communication. The Health & Safety Laboratory (2002) argue that good communication consists of three elements. The first is, through the visible

behaviors of discussing safety, others will adopt these behaviors. Secondly, organizations should be writing and publishing safety policies and statements, as well as report findings. Thirdly, organizations should be encouraging face-to-face discussions between personnel, to encourage engagement with safety.

Thus, by allowing new seafarers the opportunity to gain real-world practical experience working within a safety culture, it will better prepare them for when they form a permanent part of that team; allowing cadets to get first-hand experience of what an informed and just culture feels like, whilst helping develop the skills to be able to enhance both the flexible and learning elements of that safety culture. What is more, the short forays into operations will also demonstrate to cadets the digital systems, and the risks these face, which they may have previously never seen in training situations. This will facilitate the transition of theoretical knowledge of the risks of these systems into actual operations and their associated safety risks.

5. Conclusions

This paper has presented evidence that safety cultures are a fundamental part of maritime risk management. With more digital systems being integrated into every ship and into every operation, crew safety is becoming more reliant upon those systems. It is then no surprise that safety cultures should now include cyber risks. However, as seen with other risks, it takes time for these cultures to develop and become established (Parker, Lawrie, & Hudson, 2006). This paper has explored various ways in which organizations can facilitate the development of their cyber safety cultures. Further research needs to be completed to consider the practical implications of developing a cyber culture, and how organizations will facilitate their adoption. One such challenge is the development of appropriate training for personnel, which provides them with enough knowledge to have the confidence and understanding to engage with the cyber safety culture.

The primary aim of a safety culture is to stop events, like the sinking of the Costa Concordia, due to deliberate negligence or poor decision-making from happening (The Guardian, 2013), and reduce the impacts of accidents that, unfortunately, do happen. However, it is important to conclude that the development of a cyber safety culture will not make a company immune to all cyber risk. A quick look at the news headlines will highlight that accidents still happen, but they are just that, accidents. However, with the development of an effective cyber safety culture, the few times incidents do happen, response and recovery can be much quicker, as the organization and its personnel are better informed about these risks.

Acknowledgements

This paper is partly funded by the research efforts under Cyber-MAR. The Cyber-MAR project has received funding 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

Alshaikh, M. (2020). Developing cybersecurity cutlure to influence employee behavior: A practice perspectice. *Computers & Security, 98*, 1-10. https://doi.org/10.1016/j.cose.2020.102003

American Bureau of Shipping. (2014). *Safety culture and leading indicators of safety*. Retrieved from https://maritimesafetyinnovationlab.org/wp-content/uploads/2016/03/abs-safety-culture-and-leading-indicators-of-safety.pdf

American Bureau of Shipping. (2016). *Ergonomic & safety discussion paper*. Retrieved from https://ww2.eagle.org/content/dam/eagle/innovation-and-technology/safety-and-human-factors/Discussion-Paper-MSRI-Safety-Culture.pdf

American Bureau of Shipping. (2019). *Annual review 2019*. Retrieved from https://ww2.eagle.org/content/dam/eagle/publications/annual-review/ABS-Annual-Review-2019.pdf

Anderson, P. (2003). *Cracking the code - The relevance of the ISM code and its Impacts on shipping practices*. London: The Nautical Institute.

Ashford, W. (2019). *NotPetya offers industry-wide lessons, says Maersk's tech chief*. Retrieved from https://www.computerweekly.com/news/252464773/NotPetya-offers-industry-wide-lessons-says-Maersks-tech-chief

Barnett, M. L., & Pekcan, C. H. (2017). *The human element in shipping* (pp. 1-10). Encyclopedia of Maritime and Offshore Engineering: Wiley Online.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From deisgn methods to systems engineering. *Interacting with Computers, 23*(1), 4-17. https://doi.org/10.1016/j.intcom.2010.07.003

BBC. (2018). *BA investigation into website hack reveals more victims*. Retrieved from https://www.bbc.co.uk/news/technology-45953237

Berg, H. P. (2013). Human factors and safety culture in maritime safety. *TransNav, 7*(3), 343-353. https://doi.org/10.12716/1001.07.03.04

Bockmann, M. W. (2019). *Seized UK tanker likely 'spoofed' by Iran*. Retrieved from https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran

Boletsis, C., Halvorsrud, R., J B Pickering, S. P., & Surridge, M. (2021). *Cybersecurity for SMEs: Introducing the human element into Socio-tehnical cybersecurity risk assessment.* In Poceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: Reducing the success of social engineering attacks. *Journal of Experimental Criminology, 11*(1), 97-115. https://doi.org/10.1007/s11292-014-9222-7

Centre, N. C. S. (2020). *Phishing - still a problem, despite all the work*.

Clark, T. R. (2020). *The 4 stages of psycholigical safety*. Oakland: Berrett-Koehler Publishers.

Corrigan, S., Kay, A., Ryan, M., Ward, M. E., & Brazil, B. (2019). Human factors and safety culture: Challenges and opportunities for the port. *Safety Science, 119*, 252-265. https://doi.org/10.1016/j.ssci.2018.03.008

Department for Transport. (1987). *Herald of free enterprose formal investigation*. Retrieved from https://assets.publishing.service.gov.uk/media/54c1704ce5274a15b6000025/FormalInvestigation_HeraldofFreeEnterprise-MSA1894.pdf

Dickety, N., Collins, A., & Williamson, J. (2002). *Analysis of accidents in the foundry industry*. London: Crown Press.

Drouin, P. (2010). *The building blocks of a saafety culture. Seaways*. Retrieved from http://www.safeship.ca/uploads/3/4/4/9/34499158/safety_culture_pauldrouin.pdf

Emery, F. E., & Trist, E. L. (1960). *Socio-technical systems* (pp. 83-97). In Churchman, C. W., & Verhulst, M. (Eds.). Management Science Models and Techniques (Vol. 2). Oxford: Pergamon.

European Union Agency for Network and Information Security. (2017). *Cyber security culture in organisations*. Retrieved from https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Fernandez-Salvador, C., Oney, R., Song, S. A., & Camacho, M. (2017). From nuclear submarines to graduate medical education: Applying David Marquet's intent-based leadership model. *Military Medical Research, 4*(1), 31. https://doi.org/10.1186/s40779-017-0140-7

Glendon, A., & McKenna, E. (1995). *Human safety and risk management*. London: Chapman and Hall.

Golay, M. W. (2000). Improved nuclear power plant operations and safety through performance-based safety regulation. *Journal of Hazardous Materials, 71*(1-3), 219-237. https://doi.org/10.1016/s0304-3894(99)00080-1

Gordon, R., Perrin, E., & Kirwin, B. (2007). Measuring safety culture in a reaserch and development centre: A compaison of two methods in the Air Traffic Management domain. *Safety Sciece, 45*(6), 669-695. http://dx.doi.org/10.1016/j.ssci.2007.04.004

Hambling, D. (2017). *Ships fooled in GPS spoofing attack suggest Russian cyberweapon*. Retrieved from https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon

Health & Safety Laboratory. (2002). *Safety culture: A review of the literature*. Retrieved from https://www.hse.gov.uk/research/hsl_pdf/2002/hsl02-25.pdf

IHS Markit. (2020). *Safety at sea and BIMCO cyber security white paper*. Retrieved from https://ihsmarkit.com/Info/0819/cyber-security-survey.html

Information Commissioner's Office. (2020). *Penalty notice - British Airways*. Retrieved from https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf

International Association of Classification Societies. (2022a). *E26 - Cyber resilience of ships*. London: International Association of Classification Societies.

International Association of Classification Societies. (2022b). *E27 - Cyber Resilience of on-board systems and equipment*. London: International Association of Classification Societies.

International Atomic Energy Agency. (2020). *Safety culture practices for the regulatory body*. Retrieved from https://www-pub.iaea.org/MTCD/Publications/PDF

International Maritime Organization. (1988). *Resolution A.596(15) - Safety of passenger Ro-Ro ferries*. London: International Maritime Organization.

International Maritime Organization. (1989). *Resolution A.647(16) - IMO guidelines on management for the safe operation of ships and pollution prevention*. London: International Maritime Organization.

International Maritime Organization. (2003a). *MSC.77/17 - Role of the human element*. London: International Maritime Organization.

International Maritime Organization. (2003b). *Resolution A.947(23) - Human element vision, principles and golas for the organization*. London: International Maritime Organization.

International Maritime Organization. (2011). *MEPC 62/17/2 - Human and organizational factors - The critical role of "Just Culture"*. London: International Maritime Organization.

International Maritime Organization. (2014). *The International Safety Management Code*. London: International Maritime Organization.

International Maritime Organization. (2016). *International Convention on Standards of Training, Certification and Watchkeeping*. 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 Maritime Organization. (2020). *International convention for the safety of life at sea*. London: International Maritime Organization.

International Maritime Organization. (2021). *Maritime cyber risk*. Retrieved from https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

International Nuclear Safety Advisory Group. (1986). *INSAG-1 - Summary report on the Post-accident review meeting on the chernobyl accident*. Retrieved from https://www.iaea.org/publications/3598/summary-report-on-the-post-accident-review-meeting-on-the-chernobyl-accident

International Nuclear Safety Advisory Group. (1991). *Safety series No.75-INSAG-4 - Safety culture*. Retrieved from https://www-pub.iaea.org/MTCD/publications/PDF/Pub882_web.pdf

International Transport Forum. (2018). *Safety management systems*. Retrieved from https://www.itf-oecd.org/sites/default/files/docs/safety-management-systems.pdf

Kevin, D. J., Kimberly, T., & Papadaki, M. (2016). Threats and impacts in maritime cyber security. *Engineering & Technology Reference, 1*, 1-11. https://doi.org/10.1049/etr.2015.0123

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

Kongsvik, T., Antonsen, S., & Størkersen, K. V. (2013). *The relationship between regulation, safety management systems and safety culture in the maritime industry* (pp. 467-473). In Steenbergen, R. D. J. M., van Gelder, P. H. A. J. M., Miraglia, S., & Vrouwenvelder, A. C. W. M. (Eds.). Safety, Reliability and Risk Analysis: Beyond the Horizon. London: Taylor & Francis Group.

Lloyd's Register. (2021). *Cyber safe for marine*. Retrieved from https://www.lr.org/en-gb/cyber-safe-for-marine

Maritime & Coastguard Agency. (2004). *Drving safety culture*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/288336/rp521_final_report-4.pdf

Maritime & Coastguard Agency. (2015). *MSN 1856 (M+F) UK requirements for master and deck officers*. UK Government. Retrieved from https://www.gov.uk/government/publications/msn-1856-mf-uk-requirements-for-master-and-deck-officers

Marquet, D. (2015). *Turn the ship around!: A true sotry of turning followers inro leaders*. London: Penguin.

May, P. J. (2007). Regulatory regimes and accountability. *Regulation & Governance, 1*(1), 8-26. https://doi.org/10.1111/j.1748-5991.2007.00002.x

Meshkat, L., Miller, R. L., Hillsgrove, C., & King, J. (2020). *Behavior modeling for cybersecurity.* In Proceedings of the 2020 Annual Reliability and Maintainability Symposium.

Møller-Mærsk, A. P. (2019). *Cyber security in the maritime sector.* In Proceedings of the International Maritime Organization. Maritime Safety Committee 101, London.

Nuclear Energy Institute. (2019). *Chernobyl accident and its consequences*. Retrieved from https://www.nei.org/resources/fact-sheets/chernobyl-accident-and-its-consequences#:~:text=Key%20Facts,design%2C%20combined%20with%20human%20error

Parker, D., Lawrie, M., & Hudson, P. (2006). A framework for understanding the development of orgniasational safety culture. *Safety Culture, 44*, 551-562. https://doi.org/10.1016/j.ssci.2005.10.004

Pidgeon, N., & O'Leary, M. (2000). Man-made disasters: Why technology and organizations (sometimes) fail. *Safety Science, 34*(1), 15-30. https://doi.org/10.1016/S0925-7535(00)00004-7

Quezadra, R. D. L. (2016). *Introduction to "Just Culture".* In Proceedings of the ATS Incident Analysis Workshop.

Räisänen, P. (2009). *Influence of corporate top management to safety culture: A literature survey.* Turku University of Applied Sciences. Retrieved from https://www.merikotka.fi/wp-content/uploads/2018/08/isbn9789522161048.pdf

Reason, J. (1997). *Managing the risks of organisational accidents*. Aldershot: Ashgate Publishing.

SANS Institute. (2016). *Leveraging the human to break the cyber kill chain*. Retrieved from https://www.sans.org/blog/leveraging-the-human-to-break-the-cyber-kill-chain

Singleton, W. T. (1973). Theoretical approaches to human error. *Ergonomics, 16*(6), 727-737. https://doi.org/10.1080/00140137308924563

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

Tam, K., Hopcraft, R., Crichton, T., & Jones, K. (2021). The potential mental health effects of remote control in an autonomous maritime world. *Journal of International Maritime Safety, Environmental Affairs, and Shipping, 5*(2), 51-66. https://doi.org/10.1080/25725084.2021.1922148

The Guardian. (2013). Five Costa Concordia staff convicted over shipwreck in Italy. Retrieved from https://www.theguardian.com/world/2013/jul/20/five-costa-concordia-guilty-shipwreck-italy

The Nautical Insititue. (2020). *202063 - Assumptions can lead to bad outcomes*. Retrieved from https://www.nautinst.org/resources-page/202063.html

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). *Users really do plug in USB drives they find.* In Proceedings of the 2016 IEEE Symposium on Security and Privacy.

United States Coast Guard. (2019a). *MSIB 04-19 - Cyber adversaries targetting commercial vessels*. United States Coast Guard. Retrieved from https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_004_19.pdf

United States Coast Guard. (2019b). *MSIB 10-19 - Cyberattacks impacts MTSA facility operations*. United States Coast Guard. Retrieved from https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf

United States Coast Guard. (2020). *CVC-WI-027(1) - Vessel cyber risk management work instruction*. Retrieved from https://www.dco.uscg.mil/Portals/9/CVC-WI-27%282%29.pdf

Veiga, A. D., Astakhova, L. V., Botha, A., & Herslemann, M. (2020). Defining organisaational information security culture: Perspectives from academia and industry. *Computers & Security, 92*, 1-23. https://doi.org/10.1016/j.cose.2020.101713

Verizon. (2020). *2020 data breach investigations report*. Retrieved from https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf

Verizon. (2021). *2021 data breach investigations report*. Retrieved from https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf

World Nuclear Association. (2021). *Chernobyl accident 1986*. Retrieved from https://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx

Zhang, H., Wiegmann, A., Thaden, T. L. V., Sharma, G., & Mitchell, A. A. (2002). *Safety culture: A concept in chaos?* In Proceedings of the 46th Annual Meeting of the Human Factors and Ergonomics Society, Sanat Monica.