# Reducing the Cyber-Attack Surface in the Maritime Sector via Individual Behaviour Change

Konstantinos Mersinas
Information Security Group
Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, UK
Email: konstantinos.mersinas@rhul.ac.uk

Chupkemi Divine Chana
Information Security Group
Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, UK
Email: divine.chupkemi.2019@live.rhul.ac.uk

***Abstract* — The maritime sector has been a target for cyber-attacks during the past years. Humans play a significant role in cyber security in a dual fashion; on the one hand, human error allows for the majority of attacks to be successful, as in the case of ransomware attacks via phishing, and on the other hand, appropriate security behaviours can serve as a strong line of defence. We advocate that security needs to transcend awareness and materialise as behaviour of individuals. The question that we attempt to answer is which conditions are necessary for individuals to follow specific information security behaviours, and how to translate these conditions into a tool of practical value for the maritime industry with the intention of minimising the attack surface. Our suggestion comprises of a) identifying the characteristics of the maritime sector with regards to cyber security behaviour, b) introducing and adapting models of behaviour change from behavioural economics and psychology into maritime cyber security, and c) in the next stage of the research, creating an Artificial Intelligence (AI) based tool for individual cyber behaviour change for enterprise centres, ports and ships.**

***Keywords – maritime security, cyber security, behaviour change, security training.***

## I. INTRODUCTION

Cyber-attacks evolve and spread worldwide becoming an increasingly crucial issue in the maritime industry, resulting in individual and organisational impact; these threats have been documented within the sector [4][15][37]. Emerging recommendations aim at unifying and enhancing the security posture of the maritime industry [18][27]. This endeavour includes a focus on training; for example, the International Maritime Organization (IMO) develops model courses for various seafarers' competencies, including maritime cybersecurity related digital skills, under the International Convention on Standards of Training, Certification and Watchkeeping (STCW) [23]. It is also being recognised that human errors and behaviours are related to the majority of cybersecurity and security incidents. Therefore, personnel training is crucial for security hygiene.

There are three main obstacles, however, in achieving security hygiene via training. First, the maritime sector status quo, by large, does not provide the necessary training conditions or the training opportunities needed for personnel. Second, the sector has inherent complexity due to the interconnectivity of various systems, often including legacy ones, along with being a regulation-dense field. And third, training via traditional approaches has questionable effectiveness long-term, due to the way of delivery (e.g., a classroom setting), the frequency of occurrence (e.g., taken once or annually), its generalised nature, i.e., that it is usually not tailored to individuals' needs, and most importantly, the fact that human and circumstantial limitations are not taken into consideration.

The combination of the aforementioned environmental, sector-specific, and training factors indicates the need to investigate the underlying reasons for security awareness training ineffectiveness and to propose an innovative means for training personnel and achieving policy compliance. In this paper, we provide the theoretical basis upon which a practical solution for behaviour change will be built. The authors have developed a prototype which leverages artificial intelligence to automate security awareness and behaviour change as well as ensure personnel can easily access, assimilate, and comply with the many different regulations inherent to the industry. The finalisation of the AI-based tool comprises the next step of our research.

We advocate that the measurable and important factor in creating security hygiene is behaviour. That is, awareness on its own does not necessarily translate into corresponding (secure) actions. Thus, the goal needs to be how to shape behaviours and form secure and safe habits amongst personnel. The rest of the paper is organised as follows. In Section II, we present the challenges which relate to secure behaviours in the maritime sector. Section III presents challenges for changing security behaviours and Section IV provides the proposed solution along with the future steps needed. We conclude in Section V.

## II. CHALLENGES IN THE MARITIME SECTOR

The majority of cybersecurity incidents including human errors are generally considered to be a result of behavioural and other factors, such as lack of knowledge, human cognitive limitations, and the lack of time and motivation (World Economic Forum, [28]). To that end, it is only natural to expect cybersecurity professionals to ensure, as high priority, the effective management and mitigation of cyber threats related to human actions. In the following sections we take a closer look at some of those threats in the context of the maritime industry.

 ISBN: 978-1-61208-996-6 

### A. The maritime training environment

Human behaviour, typically in the form of unintentional actions by individuals without sufficient security training or awareness has been identified as the most significant security incident cause [28, p. 45], and human weaknesses are reported to cause more than three-fourths of data breaches in organisations, in general [20]. For example, clicking on phishing links in emails or accessing false websites despite warnings from an anti-virus have been usual ways for attackers to install malware. Similar percentages hold for shipping accidents caused by human errors directly or indirectly [13]. The authors are not aware of maritime-specific studies on human-generated cybersecurity breaches. Sen analyses the vulnerability of cybersecurity in the maritime industry and reports the over-reliance on outdated technology and security tools as a major issue [32]. The global fleet has an average ship lifespan of more than 20 years [21][45] and Information Technology (IT) and Operational Technology (OT) systems are usually not upgraded regularly, if at all, resulting in, e.g., legacy operating systems which are no longer supported.

The focus on technology, outdated or not, also diminishes the importance and increases the risk of human-related security incidents. In particular, the traditional view that firewalls, antivirus software and other technical controls are sufficient to deal with cyber-attacks, is still existent across sectors, including the maritime sector. The disproportionate focus on technical controls has indeed, on the one hand, significantly enhanced the effectiveness of these controls and, to an extent, possibly diminished the role of humans in security. On the other hand, it has driven attackers to target human weaknesses. For example, it is highly unlikely that attackers target the underlying cryptographic algorithms to gain access to a system, but most likely they would utilise social engineering attacks [7].

The sector has a heavily operational nature which does not provide a conducive environment with enough opportunities for personnel training [35]. Training usually takes place at ports, or is expected from personnel at the expense of their leisure time [24]. Importantly, seafarers are reported to have excessive workloads, lack of sleep and job-related worries [40]. In combination with being away from their families, these factors contribute to suboptimal decision-making, subjective risk perceptions and increased susceptibility to social engineering attacks. Therefore, the nature of the maritime environment can increase the attack surface and a higher level of susceptibility to human error.

### B. Sector characteristics and challenges

The maritime sector is becoming digitised, with increasing interconnectivity of ship and port systems. A first issue, however, is that ships tend to have long life cycles estimated to be on average between 20.3 years [45] and about 30 years (25 years life expectancy and 5 years build time) [21], which result in legacy systems that are difficult to maintain and patch [32]. Moreover, legacy systems need additional controls in place to compensate, e.g., for the lack of support to outdated versions, which add complexity and cost overheads. Additionally, the different life cycles of IT and OT systems result in company overheads in managing risks.

Companies which operate internationally are known to face a significant compliance challenge, due to multiple region-related requirements [27], as in the case of the Maritime Transportation Security Act of 2002 (MTSA) in the U.S. which required that ports and vessels perform a number of vulnerability assessments, access control, screening and other procedures [6]. Another example of country-specific stricter-than-IMO requirements is that of ballast water treatment, where although the IMO deferred the implementation of the requirements to 2019, at the time, the U.S. issued their own regulations and implementation schedule [3].

As defined by the IMO, maritime cyber risk relates to the extent to which a technology asset could be endangered by a potential circumstance or event, resulting in operational, safety, or security failures due to corrupted, lost or compromised information or systems [23]. However, in the maritime sector there is a combination of navigational, IT and OT critical systems, threats to which can also be detrimental. To that end, the maritime industry recognises the need for cybersecurity compliance measures for effective mitigation of evolving threats, some of which include the IMO resolution MSC.428(98) maritime cyber risk management in safety management systems [42], ISA/IEC 62443-4-2 security for industrial automation and control systems [43], and ISO/IEC 27005 information security risk management [44].

The case of the A.P. Møller-Maersk ransomware attack which incurred losses approaching $300m [12] is well known in the sector. The Evergreen container ship that blocked the Suez Canal hindered international trade and impacted the world economy. The Suez Canal Authority demanded $916m for compensation, salvage costs and reputational losses from the shipping company (later lowered the demand to $550m) [5]. Although the Evergreen case was not a cyber-attack, it illustrates the impact of maritime incidents and the potential impact of cyber incidents [39].

Compliance challenges and the interconnectedness of cyber physical systems, that is, the intersection of IT, OT and the human interface, increase the complexity of maritime security. Indicative of OT systems are cargo, fuel and utility management, vessel propulsion, mooring and docking, operations for cranes and equipment; IT systems include all navigation, communication and monitoring systems and sensors. Finally, the human interface angle includes port and vessel operators, deck and engine crew, support officers, office employees, technical superintendents and various service providers [31].

These factors pose challenges for personnel, some of which include managing multiple projects simultaneously in limited time [24] with an increased risk of errors and managing a continuously rotating personnel. The question, thus, is how to ensure that staff understand and comply with the various standards and codes of practice, participate in effective training, and behave accordingly. The combination

 ISBN: 978-1-61208-996-6 

of the aforementioned characteristics and challenges, make the maritime sector a unique cyber security environment.

### C. Security behaviour change

The IMO identifies that the human element is a significant and complex multidimensional and that 'consideration of human element matters should aim at decreasing the possibility of human error as far as possible' [22]. Additionally, insights from other sectors expand the scope of the human element by combining security with safety, as in the case of the International Atomic Energy Agency practices [14]. However, the way to minimise human error is not straightforward and is largely context-dependent. Limitations of training and practices to be avoided, for example, a blame culture towards seafarers and shore-based personnel, are identified in maritime; indicatively, the IHS Markit and BIMCO report highlights the need to 'look deeper' into the human element [16]. The behaviour change interventions that we propose are in line with this needed 'deeper look'.

There are specific reasons for traditional training not being as effective as policy-makers and security professionals would like it to be; some of these reasons are inherent in human nature while others are environmental or circumstantial. First, as humans, we have limited cognitive capacity and we can absorb, remember and utilise certain amounts of information. Second, only a fraction of the information is available to an individual when they have to make a decision; that is, access to information is partial, or worse, information is unknown. Finally, the available timeframes for making a decision or collecting information is limited by definition. These limitations were identified by the economist Herbert Simon and were termed as 'bounded rationality' [33].

The criticality of time is amplified in the maritime and other sectors, where often personnel have to make fast operational, security and safety related decisions. The aforementioned factors are not to diminish the influence of knowledge and understanding in optimising decision-making, and more so in organisational contexts [34]. However, they portray the inherent issues related to training and whether this training can have significant long-term effects.

We can think of a behaviour change mechanism (or intervention) as having a messenger, a message and a receiver. The message includes a particular threat (including likelihood and impact) and a suggested solution to be accepted or rejected by the receiver (including the level of difficulty of the solution or the skills of the receiver and how effective the solution is expected to be). For example, a threat could be typosquatting the URL used by ship operators to access live ship traffic maps and the solution could be providing a set of actions that ship crews need to undertake, in order to avoid such attacks.

The receiver, e.g., personnel, have a subjective perception of the threat, of their ability (self-efficacy) to follow the suggested solution, and of the solution itself (response efficacy). The so-called 'intervention design' needs to utilise the individual's strengths and be customised to the individual's competence level, professional role, and even cultural background, so that the individual is convinced about the importance of the threat and is subsequently persuaded about the efficacy of the proposed solution. Depending on the context, *who* conveys the message (e.g., senior management, officers etc.) also influences receivers' acceptance decision. The goal is to consider and balance these factors in a way that individuals accept messages and comply with the proposed security behaviour, e.g., adhering to a security policy.

One of the main approaches to change behaviour in psychology and health sciences, and one that has recently been introduced to cybersecurity, is fear appeals. A definition of fear appeals is that they are *'persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends'* [41, p. 329]. Overall, responses to fear depend on two main factors. On the one hand, we have context-dependent stimuli, which are objective. On the other hand, we have behavioural responses which – to an extent – depend on individual traits and characteristics [1], possibly both cognitive and physiological. The latter point reinforces our initial argument that any behaviour change intervention should be individualised to match the subject's needs and characteristics. *Figure 1* depicts an abstraction of conveying a message to, for example, personnel.

 ISBN: 978-1-61208-996-6 

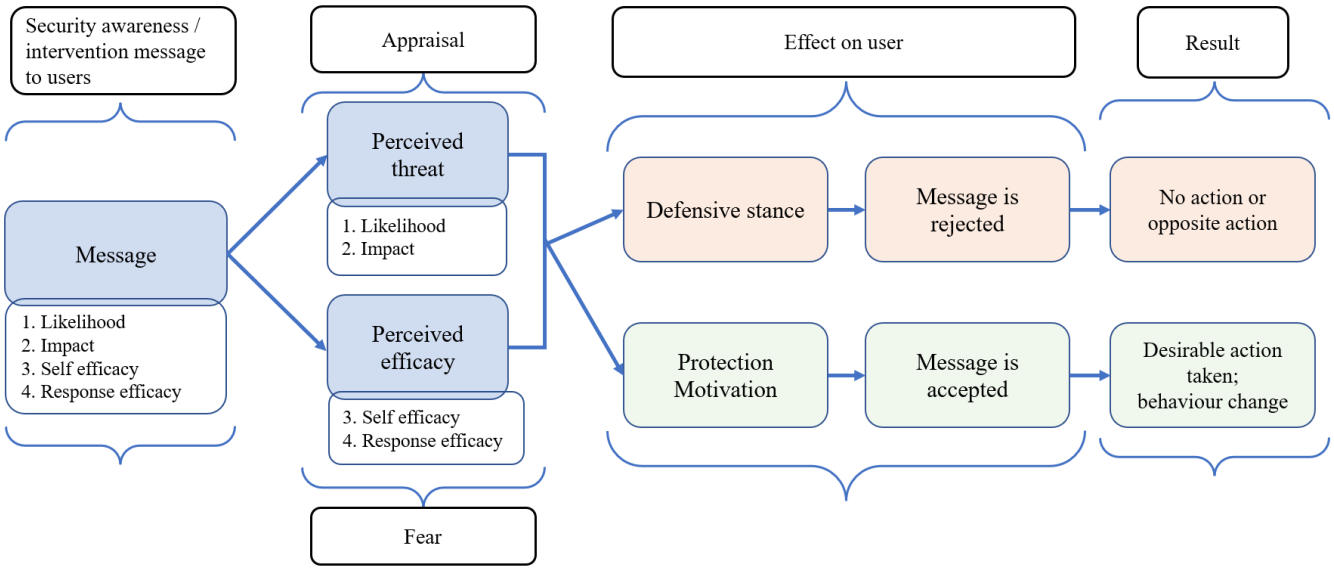


Figure 1. Behavioural intervention model for personnel (adapted from [29] and [38]).

## III. BEHAVIOUR CHANGE CHALLENGES

### A. *Defining secure behaviour*

It is not straightforward what constitutes secure behaviour. As a first step, desired behaviours need to be identified. 'Following IMO's guidelines on maritime cyber risk management on board ships.' is a generic and perhaps not fully constructive goal. Understanding which behaviours work, e.g., for personnel, and why, is a more promising approach. In fact, some of the guidelines might be impractical or not in line with the daily reality of personnel and, thus, full and consistent compliance should not be expected from users, by default, without considering situational circumstances.

For instance, reading and memorising vast amounts of international cyber security standards related to technologies that are crucial to the operation of numerous maritime systems is not necessarily a reasonable expectation. Personnel have a number of tasks to perform, their attention is focused on their own work and cybersecurity is not their priority. So, what is expected of personnel needs careful examination and dissemination.

### B. *Balancing and utilising emotion and reason.*

The balance of emotion and reason in appeals to individuals is key for conveying a message. And, equally, considering the individuals' responses is important. For example, [38] suggests that cognitive responses are the desired reactions to communicated threat messages, rather than emotional ones. However, defining 'reason', 'rationality' and adjusting the level of emotional appraisals is not an easy endeavour [2]. Indicatively, the factor of fear plays an important role, as well as the various types of rationality [26].

Additionally, in the maritime sector, we have critical OT systems and safety risks, which can attract the attention of individuals more, if contrasted to cyber security risks. Thus, fear appeals, unless they are linked to safety and OT risks, might not be sufficiently salient in the perception of personnel.

### C. *Selecting and weighing the behavioural intervention variables to be modelled.*

According to [30], the perceived level of threat, along with the individual's perceived efficacy to cope with this threat, are the main predictors of whether people take protective actions or not. Additionally, [10] proposes motivation, appropriate triggers, simplicity of solutions, peer pressure and social acceptance as the main factors which influence behaviour change, and the Hook model also utilises triggers, along with rewards for personnel and their investment in an action [9]. The majority of research literature on behaviour change originates from health sciences, e.g., studies on alcohol consumption, smoking, poor nutrition or lack of exercise, and people fail to change their behaviour even when facing life-threatening conditions. The core variables for behaviour change in a maritime security setting are yet to be identified empirically.

### D. *Considering security culture.*

Including security culture as an 'environmental' factor in the equation is another angle. Security culture can be considered as the set of shared values, beliefs and practices relating to cyber security in an environment, e.g., in an organisation [8]. The benefits of cyber security and safety culture have been reported in the literature [19]. Situational circumstances can affect message acceptance; e.g., social norms, peer pressure or herding behaviours, say, in a ship environment. A new employee observes her colleagues' behaviour and will most likely follow aspects of this behaviour. It is, thus, important to consider security culture and environment-dependent factors, and model them to a

 ISBN: 978-1-61208-996-6 

sufficiently adaptable level, so that a generic model and a context-specific implementation are balanced.

## IV. PRACTICAL BEHAVIOUR CHANGE FOR THE MARITIME SECTOR

Taking into consideration context, technology and personnel-related challenges in the maritime sector and the underlying psychological and behavioural reasons for people's non-compliance we propose a practical solution. Namely, the authors propose an AI-based individualised assistant which a) is customised to the particular environment of implementation, e.g., by analysing and codifying the existing – and being updated with new – guidelines on maritime cyber risk management, security policies and standards, and b) learns the individual's personal characteristics, behaviours, and knowledge gaps, and directs them to relevant information in a focused fashion. For example, the tool will know which policies and procedures are required for the person's role and rank and will learn which knowledge gaps the person has; it can then prompt the individual with targeted information.

The idea of our solution aims in minimising the susceptibility of individuals to security (and safety) errors by providing training and support with practical information, and prompting hints to maritime staff, in a timely manner. In this paper, we provide the theoretical basis upon which the idea of this digital assistant will be built. The current state of the solution achieves an AI-based analysis of maritime security policies, guidelines, and standards, and can be trained through them to direct individuals and assist with their security-related enquiries. Next steps include a constant training of the tool, based on maritime security policies, guidelines, and standards, user behaviour and user characteristics (with user consent), so that a holistic 'understanding' is achieved by the tool, and the tool can consequently assist in complex and emerging situations and needs of the individual and the company.

### *Limitations, technical details and future research*

The goal of this part of the research is to set the basis for the future development of our intervention technologies for security behaviour change. However, the approach has its limitations; as a matter of fact, a significant part of the literature in this area has similar limitations and in particular, a lack of experimental verification of certain aspects of models and theories [29]. This is an open problem which we plan to tackle through our future research, in two ways. First, via lab-based experiments where we can measure individuals' reactions in a 'clean' environment, with clear conditions to be tested; and, thus, examining both individual traits and situational circumstances. Second, with field experiments in maritime context, where we will be able to measure the specific characteristics of individuals, but also of the environmental and the social conditions, i.e., aspects of the security culture. The aforementioned research activities will inform and shape the development and finalisation of the AI-based tool.

In more detail, there is a need for large-scale gathering and analysis of security policies, standards, and guidelines of interest. With the aim of developing agents that are capable of systematically identifying, extracting, and quantifying sentences and paragraphs, these documents will be prepared and trained using techniques such as clustering, semantic analysis, and similarity analysis from Natural Language Processing (NLP). In parallel, in collaboration with industry partners, further research will be conducted to identify Key Monitoring Points (KMPs), as well as potential Threat Entry Points (TEPs), in such an OT dominated environment.

The identification of KMPs (e.g., a ship's satellite-related software) and TEPs (e.g., a connection point that allows for malware to be injected) will serve as a baseline and paradigm on which behavioural protocols are designed (similarly to traditional protocols, but aimed at affecting users' actions through statements, reminders, advice, extracts from policies, and other interventions). Algorithms are derived from translating measurable behaviours and are fed with selected actions (events or group of events) to trigger targeted behavioural interventions based on the protocol's threshold or trigger point. The algorithm's output will, in most cases, be determined with the help of trained Machine Learning (ML) agents from NLP training of available documents (policies, procedures and standards of interest). These agents are able to extract the most appropriate text or point personnel to the right document.

Many additional questions emerge from this study. Namely, fear is an evolutionarily useful emotion, initially related to survival. We would like to further explore the degrees of fear in relation to less-strong individual traits like risk aversion, uncertainty avoidance and loss aversion. Moreover, another goal is the experimental testing of behavioural responses to fear in a maritime security context. There are also ethical considerations of having human participants in experimentally tested fear conditions. Beyond these considerations, the 'fear-level matching' that simulates a real-world threat, e.g., data loss due to ransomware attacks, is a challenge on its own. Another aspect of future work is the empirical identification of behavioural interventions best-suited for maritime environments.

## V. CONCLUSION

The vulnerability and susceptibility of the maritime sector can be significantly minimised via investing in the human factors of cybersecurity. Humans can become a significant 'line of defence' in the sector, if equipped and trained appropriately. In order for this approach to be successful, both the individual traits of personnel and the environmental, contextual factors need to be considered. In this paper, we present the theoretical background and propose a practical approach for effective behavioural interventions, at a high level. A combination of adapted behavioural theories and collected data can inform the creation of a practical tool to reduce personnel time and effort for accessing knowledge, and which can gradually form security behaviours, reducing the cyber-attack surface in the sector.

 ISBN: 978-1-61208-996-6 

## REFERENCES


[1] R. Adolphs, The Biology of Fear. Current Biology, 23(2): p. R79-R93, 2013.

[2] D. Ariely, Predictably irrational: The hidden forces that shape our decisions. New York, 2008.

[3] P. Benecki, *"Compliance Challenges," The Maritime Executive*, 22 March 2018. [Online]. Available from: https://maritime-executive.com/magazine/compliance-challenges 2022.09.22

[4] BIMCO. *The guidelines on cyber security onboard ships*, 2017. [Online]. Available from: http://www.icsshipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cybersecurity-onboard-ships.pdf?sfvrsn=16 2022.09.27

[5] BBC. *Ever Given: Ship that blocked Suez Canal sets sail after deal signed*, 2021. [Online]. Available from: https://www.bbc.com/news/world-middle-east-57746424 2022.09.22

[6] C. E. Carey, Maritime Transportation Security Act of 2002 (Potential Civil Liabilities and Defenses). Tul. Mar. LJ, 28, p.295, 2003.

[7] P. Carpenter and K. Roer, The Security Culture Playbook: An Executive Guide To Reducing Risk and Developing Your Human Defense Layer. John Wiley & Sons, 2022.

[8] A. da Veiga and J. H. P. Eloff, A framework and assessment instrument for information security culture. Computers & Security, 29(2), pp. 196–207. doi:10.1016/j.cose.2009.09.002, 2010.

[9] N. Eyal, Hooked: How to build habit-forming products. Penguin, 2014.

[10] B. J. Fogg, A behavior model for persuasive design. In Proceedings of the 4th international Conference on Persuasive Technology (p. 40). ACM, April 2009.

[11] Gov.uk. *Ship security*, 2022. [Online]. Available from: https://www.gov.uk/guidance/maritime-security 2022.09.24

[12] A. Greenberg, *"The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired.com. 22 August* 2018. [Online]. Available from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world 2022.09.24

[13] C. Heij and S. Knapp, "Predictive Power of Inspection Outcomes for Future Shipping Accidents – An Empirical Appraisal with Special Attention for Human Factor Aspects." Maritime Policy and Management, 2018, 45 (5), 604-621, 2018.

[14] International Atomic Energy Agency. *IAEA, Safety Culture Practices for the Regulatory Body*, 2020. [Online]. Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/TE-1895web.pdf 2022.09.28

[15] Institute of Engineering and Technology, IET, Code of practice – cyber security for ports and port systems, 2016.

[16] HIS Markit, Safety at Sea and BIMCO cyber security white paper. Safety at Sea, p.15, 2019.

[17] R. Hopcraft, Developing Maritime Digital Competencies. IEEE Communications Standards Magazine, 5(3), pp.12-18, 2021.

[18] R. Hopcraft and K. M. Martin, Effective maritime cybersecurity regulation–the case for a cyber code. *Journal of the Indian Ocean Region*, 14(3), pp.354-366, 2018.

[19] R. Hopcraft, K. Tam, J. D. P. Misas, K. Moara-Nkwe, and K. Jones, Developing a Maritime Cyber Safety Culture: Improving Safety of Operations. Maritime Technology and Research, 5(1), 2023.

[20] ENISA, ENISA threat landscape report 2018: 15 Top Cyber-Threats and Trends. Heraklion: European Network and Information Security Agency (ENISA). doi: 10.2824/622757, 2019.

[21] International Maritime Organisation. IMO, Resolution MSC.287(87) – Adoption of the International Goal-based Ship Construction Standards for Bulk Carriers and Oil Tankers, 2010.

[22] International Maritime Organisation. IMO, MSC-MEPC.2 – Guidelines for the Application of the Human Element Analysing Process (Heap) to the IMO Rule-making Process, 2013.

[23] International Maritime Organisation. IMO, Resolution MSC.428(98) — Maritime Cyber Risk Management in Safety Management Systems, 2017.

[24] K. D. Jones, K. Tam, and M. Papadaki, Threats and impacts in maritime cyber security. Engineering & Technology Reference, 1(1). doi: 10.1049/etr.2015.0123, 2016.

[25] K. Mersinas, M. Bada, and N. Tzoumerkas, Security behavior change ethics: implications for research and practice [Unpublished manuscript]. Information Security Group, Royal Holloway, University of London, 2022.

[26] K. Mersinas, T. Sobb, C. Sample, J. Z. Bakdash, and D. Ormrod, Training Data and Rationality. In ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics (p. 225). Academic Conferences and publishing limited, October 2019.

[27] Missionsecure, *A Comprehensive Guide to Maritime Cyber Security*, 2020. [Online]. Available from: https://www.missionsecure.com/resources/comprehensive-guide-to-maritime-security-ebook 2022.09.24

[28] World Economic Forum, *The Global Risks Report*, 2022. [Online]. Available from: https://www.weforum.org/reports/global-risks-report-2022 2022.10.01

[29] L. Popova, The extended parallel process model: Illuminating the gaps in research. Health Education & Behavior, 39(4), pp.455-473, 2012.

[30] R. W. Rogers, A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), pp.93-114, 1975.

[31] I. Progoulakis, P. Rohmeyer, and N. Nikitakos, Cyber Physical Systems Security for Maritime Assets. *Journal of Marine Science and Engineering*, 9(12), p.1384, 2021.

[32] R. Sen, Chapter 9. Cyber and information threats to seaports and ships. McNicholas, MA, Maritime Security, 2, pp. 281-302, 2016.

[33] H. A. Simon, Theories of bounded rationality. In C. B. McGuire and R. Radner (eds.). Decision and Organization, pp. 161-176, 1972.

[34] H. A. Simon, Bounded rationality and organizational learning. Organization Science 2(1), pp. 125-134, 1991.

[35] D. Smith, *Cybersecurity challenges for the Maritime Industry. SeaRates*, 2022. [Online]. Available from: https://www.searates.com/blog/post/cybersecurity-challenges-for-the-maritime-industry 2022.09.22

[36] B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, Maritime Cyber Risk Management: An Experimental Ship Assessment. *Journal of Navigation*, 72(5), pp.1108-1120, 2019.

[37] TRANSAS, *Connected ships and cybersecurity. Frank J Coles CEO*, 2016. [Online]. Available from: https://docs.wixstatic.com/ugd/9491c8_5fbc6ff941df40f8a5b90d703de4a64b.pdf 2022.09.22

[38] K. Witte, Fear as a motivator, fear as inhibitor: Using the EPPM to explain fear appeal successes and failures. The Handbook of Communication and Emotion, 1998.

[39] E. Wong, F. Chan, I. Kim, and J. Lee, Canal Blockage: Legal Risks and Liabilities Framework on the Global Supply Chain

from Suez Canal Blockage by Ever Given. *SSRN Electronic Journal*, 2022.

[40] B. Tetemadze, M. Carrera Arce, R. Baumler, and I. Bartusevičiene, Seafarers' wellbeing or business, a complex paradox of the industry. TransNav: *International Journal on Marine Navigation and Safety of Sea Transportation*, 15, 2021.

[41] T. M. Wilkinson, Nudging and manipulation. Political Studies 61, 341–355, 2013.

[42] IMO, Resolution MSC.428(98) — Maritime Cyber Risk Management in Safety Management Systems, 2017.

[43] ISA/IEC 62443 - Industrial Automation and Control Systems Security by the International Electrotechnical Commission

[44] ISO/IEC 27001:2018 – International Organisation of Standards, International Electrotechnical Commission, Information Security Management Systems.

[45] International Chamber of Shipping, Review of Maritime Transport. United Nations Conference on Trade and Development (UNCTAD), Geneva, 2016.

 ISBN: 978-1-61208-996-6 