Is cyber-security the new lifeboat? An exploration of the employee's perspective of cyber-security within the cruise ship industry

Victoria Knight, Moufida Sadok

University of Portsmouth, Park Building, King Henry | Street, Portsmouth, United Kingdom

Abstract

After the International Maritime Organisation introduced the Maritime Cyber Risk Management in Safety Management Systems Resolution in 2017, with the compliance date set for January 2021, the Maritime industry has displayed an increased focus on its cyber-security. This quantitative research, supported by the socio-technical perspective, explores the employee perceptions of cyber-security onboard cruise ships. The results show that the cruise industry has made an attempt to increase its cyber-security by introducing a formal policy and training their employees. Employees, as a consequence, perceive cyber-security to be important. However, employee perceptions are not reflective of their behaviours onboard. This is because there are various technical and organizational obstacles to their cyber-security practices which have been overlooked. As a result, the cruise industry could do more to prioritise cyber-security on a day-to-day level in order to make sure that the employee experience is in alignment with cyber-security policies.

Keywords

Maritime, cruise ship, cyber-security, socio-technical, employee perspective, quantitative.

1. Introduction

Under the International Management Code for the Safe Operation of Ships and for Pollution Prevention, the International Maritime Organisation (IMO) adopted the International Safety Management Code (ISM) [1]. This requires all passenger ships to ensure safety at sea, the prevention of human injury and avoidance of damage to the environment [2]. Up until recently, this requirement of safety management focused on the mitigation of physical threats. However, in response to the increasing evidence of cyber-attacks within the maritime industry, the Maritime Cyber Risk Management in Safety Management Systems Resolution [3] applies the requirement of Cyber Risk Management to the ISM. This is supported by the Guidelines on Maritime Cyber Risk Management [4]. The compliance date for this was January 2021 [5].

This research applies the socio-technical perspective to the maritime industry and explores an employee perspective of cyber-security within the cruise ship industry by way of a quantitative survey. A total of 155 participants completed the self-administered questionnaire which was distributed via Facebook 'Crew Only' groups and LinkedIn. The participants occupied positions onboard from various cruise companies, in a vast array of job roles and varying levels of authority.

7th International Workshop on Socio-Technical Perspective in IS development (STPIS 2021) 11-12 October 2021, Trento, Italy
EMAIL: up603123@myport.ac.uk (A. 1);moufida.sadok@port.ac.uk (A. 2)

The research shows that the maritime industry could benefit from applying the socio-technical perspective to its cyber-security strategy. Currently, the day-to-day level cyber-security is being ignored by the cruise ship sector. As a result, employees are aware of the threat of a cyber-attack at sea, they perceive cyber-security to be important, they are receiving training and are aware of cyber-security policies. However, there is a disparity between their intentions and their practices which is a result of daily obstacles and challenges preventing them from following cyber-security policies.

This paper will be comprised of three parts. The first, will explain the background and situate this research amongst other relevant literature. Next, an overview of the research methodology will be outlined and its limitations presented. Lastly, the paper will discuss the results, offering recommendations and suggestions for future research.

2. Background

In 2017, the maritime industry was awakened to the importance of cyber-security when Maersk Shipping Solutions was hit with what the White House said to be, 'the most destructive and costly cyber-attack in history' [6]. Since then, the number of cyber-attacks on the maritime industry has risen, exacerbated by the dramatic impact of the COVID-19 outbreak, meaning that the majority of seafarers are working remotely with increased connectivity between devices [7]. Alarmingly, even the International Maritime Organisation (IMO) faced a cyber-attack in October 2020 which disrupted its website and networks [8]. Consequently, such attacks have highlighted the importance of maritime cyber-security and therefore should be highly prioritised [9].

Within the maritime industry, the approach to cyber-security, often focuses on highlighting the various ways that a vessel could be exploited [10] [11] [12], paying frequent attention to the navigational system vulnerabilities due to its reliance on multiple sensory digital technologies to operate [13] [14] [15] [16] [17] [18]. Attention is also often paid to considering the protection of supply chains and ports as a critical infrastructure [19] [20] [21] [22].

However, so far, the cruise ship industry has escaped focus, despite there being evidence of cyber-exploitation within the sector [23]. This needs addressing because any weak link within the maritime industry could be the means for exploitation of critical operations at sea [24]. Therefore it is important that the cruise sector's cyber-security is efficient for the safety of both its crew and passengers as well as its contribution to the maritime industry in general [24].

Furthermore, despite the IMO guidelines highlighting the importance of the adoption of a holistic approach to cyber-security [4], the maritime industry has relied heavily on a technical approach [13] [14] [15] [16] [17] [18]. Although a technological approach to cyber-security is necessary, overly technocentric approaches do not provide effective protection [25] [26] [27]. This is because, as highlighted by the socio-technical perspective, there are many other factors, aside from the technical which influence the cyber-security of an organisation [25] [28].

Currently, there is extremely limited discussion of cyber-security from humanistic approach. However, the human factor is a vital contribution and is in need of attention [29].

The literature provided from the socio-technical perspective adopts an employee perspective in order to try to understand user behaviour. Oftentimes, users are aware of their

role in cyber-security, but their intentions do not match their practices [28]. Therefore, it is important to consider how to maximise the efficacy of training in order to alter their behaviours for the long term. For instance, Bada et al. explains that, 'people must be able to understand and apply the advice, and secondly, they must be motivated and willing to do so' [30]. It is therefore vital to explain why cyber-security practices are important in order for them to be adopted [31]. Furthermore, all humans have different processes of understanding information and decision making regarding cyber-security behaviour, therefore training should reflect this and should be uniquely delivered and matched with the learning style of the individual in order to be most effective [32] [33].

Similarly, it is not sufficient to just train employees because workplace cyber-security practices degrade overtime [34].Therefore, it is important that cyber-security awareness is maintained, most effectively through actively involving users with training and awareness as opposed to passive forms of maintenance [35].

Aside from understanding and changing user behaviour, the socio-technical perspective highlights that there are other factors which influence employee's practices. Oftentimes there are many social and organisational factors acting as an obstacle to employee's cyber-security which are overlooked. For instance, the needs of the designers, compared to the needs of the users are not in alignment [36]. Similarly, managerial expectations, and organisational policies are frequently out of touch with workplace routines [37]. Employees, as a result, are not able to balance the needs of the organisation with the demands of cyber-security policies, meaning that they do not highly prioritise cyber-security practices or workaround them [37] [38]. By adopting a socio-technical approach, a shift can be made from humans as a problem, to humans as a solution [39]. Therefore, in order to be successful, cyber-security practices must be influenced by the employees who are affected by security controls [37].

It is also important that the organisational culture is in alignment with the cyber-security policies in order to encourage good cyber-security practices. This helps to communicate the importance of cyber-security to employees and promote compliance with cyber-security policies [40].

There is evidence that the maritime industry could greatly improve its cyber-security by considering the socio-technical in its strategy. Interestingly, after the Maersk attack, the U.S. Coast Guard discovered that crew members were aware that computers onboard had been compromised, they avoided using them for personal tasks out of fear of being compromised but disregarded the threat when conducting professional tasks. It was therefore said that "simple cyber hygiene would have prevented this issue… it's in the day-to-day that these things happen" [41]. This evidence highlights the dangers of relying heavily on a technical approach to cyber-security and ignoring the humanistic elements of cyber-security. Consequently, the maritime industry should adopt a holistic approach to cyber-security, considering people, processes and technology combined [42].

This research therefore seeks to apply the socio-technical perspective to the maritime industry to see if this environment could also gain the benefits of adopting the perspective to its cyber-security strategy. The research assumption is that staff members onboard are conducting common practices which could be putting cruise ships at risk of a cyber-attack. These behaviours are the result of daily challenges which are acting as an obstacle for staff members. This research therefore aims to gain an employee perspective of cyber-security

onboard cruise ships and apply the socio-technical perspective in order to understand the reasons behind their behaviour.

3. Methodology

Using a quantitative method, this research was conducted via the use of a computerised self-administered questionnaire design [43] which was formed mostly of closed-ended questions [44]. The justification for the appropriateness of this method, is that cyber-security is generally something that not everyone is particularly knowledgeable about. Many people consider it to be an expert subject and are intimidated about discussing the topic. Additionally, given that cruise ship employees come from all over the world and speak many different languages, using qualitative research to explore the perceptions of someone whose first language is not English would potentially discourage participants from taking part. Instead, asking participants to simply select a number as a response, rather than requiring them to attempt to express their answer about an expert subject in their second language, was considered more appropriate. Consequently, in order to gain responses which were useful, a quantitative design was adopted to give structure and support to the participants' responses. To provide explanation for the selected responses, an interpretivist epistemology [45] was used with inductive reasoning.

The questions were answered on a five-point Likert Scale [46] in order to assess the level of agreement with the statement proposed [47] ranging from 'Strongly agree' to 'Strongly disagree'. Open-ended questions, producing qualitative data, were also used in the questionnaire, giving participants the chance to offer a subjective response based on their own experience and support the inductive reasoning.

The sample of cruise ship employees was obtained through a nonprobability purposive sampling method [48] obtained through Facebook 'Crew Only' groups and LinkedIn. The researcher was already a member of many of these closed groups on Facebook but selected specific groups based on the diversity of the members, ensuring it was comprised of employees in differing job roles and varying cruise ship companies. This enabled a wider exploration of the perceptions and also was an attempt to avoid reputational damage to any one company in particular. Once permission was obtained from the group administrators, the researcher posted a message in the groups, informing members of the research, containing a link to the questionnaire if the participant wanted to participate.

Those who were in a job role that had access to an IT system between 2018-2020 were invited to take part. The IMO guidelines were released in 2017, so the time frame selected enabled companies the chance to respond, and ensured that the exploration of the perceptions of employees was from the time which there was cyber-security awareness within the maritime industry.

According to the Facebook group descriptions, there was approximately 50,000 group members combined. However, it is difficult to determine how many of these members were actively engaging in the group at the time. It is also important to highlight that these groups are for social purposes and so, many members are no longer employed, nor have been in a long time. As a result, they may not have been working for a cruise company when cyber-security was a priority and therefore not eligible to partake in the research.

A total of 155 participants completed the questionnaire. The responses from the closed-ended questions were analysed using descriptive statistics [49]. IBM SPSS software was used to facilitate this to avoid human error. Confidence intervals of the proportion were also calculated using the modified Wald method [50].

3.1. Limitations

The researcher will now briefly outline the limitations of this research so that the results within their given context. Due to the quantitative method adopted and questionnaire design, the exploration of employee perceptions was limited in scope. Therefore inductive reasoning, supported by the answers from the qualitative questions, was used to give further explanation to results. This therefore means that the research is not completely objective and has an element of researcher influence.

The questionnaire was also conducted in English by many participants who are not fluent speakers. Given that cyber-security is considered a complex subject, there is a chance that some participant's comprehension of the questions may have been reduced. Some staff members who were not entirely comfortable with partaking in the research due to it being conducted in English may have even been put off taking part.

Embracing the use of the internet to conduct the research was a useful aid during a pandemic. Without such a tool, it would have been extremely challenging to obtain the perceptions of employees who were scattered around the globe. However, not all employees are connected to the internet, nor are necessarily on social media, or a part of Crew Groups on Facebook. Therefore, by embracing this method of sampling, the generalisability of the results to the entire population is reduced.

Furthermore, the sample obtained was a size which enabled an exploration to be obtained into the perceptions of employees. However, the results represent a snap-shot of the number of staff members employed in total across the entire industry.

The researcher would also like to highlight that the cruise industry has paused its operations for over a year. Therefore this research required employees to recall their experiences. This means that their responses may have been influenced by lack of memory. Furthermore, in the year that has passed, the cruise industry may have taken more steps to improve its cyber-security which has yet to be rolled out to employees.

4. Findings

The key findings of the research are:

1. The cruise ship industry is raising cyber-security awareness amongst employees

   This explains the employee awareness of cyber-security policies, their experience of training onboard and the maintenance of their awareness.

2. Employee cyber-security intentions do not match their behaviour

This explains employee perceptions of a cyber-attack/the importance of cyber-security. It then proceeds to discuss employee's onboard behaviour.

3. Day-to-day level cyber-security is being ignored

   This explains the various obstacles which are influencing employee's cyber-security practices onboard.

This section will be comprised of three parts, presenting a discussion of each of these key findings.

4.1. Key Finding One: Cyber-security awareness amongst employees

This finding will be discussed in three parts. The first part will present the findings from the exploration of the employee's experience of training. The second part will focus on the maintenance of their training and awareness. The third part will discuss the impact of the current approach to training and awareness maintenance.

The results show that the cruise industry appears to be attempting to improve its cyber-security in accordance with the IMO guidelines. A formal cyber-security policy has been introduced, which 68.4% of employees confirmed had already been established (90% CI [0.6197, 0.7418]). Alongside this, 67.7% of employees received cyber-security training (90% CI [0.6130, 0.7358]). which was given to employees occupying the full range of job roles onboard. However, there are limitations to the cruise ship industry's efforts which will be outlined below.

The training was not always conducted prior to the employee using an IT system onboard, due to employees being left to 'settle in' before being given cyber-security training. Employees also explained that the cyber-security training was 'not taken seriously'.

Furthermore, not all employees who are using an IT system are being trained; those in job roles that are more centred around IT are more likely to receive training at 71.4% (90% CI [0.5471, 0.6748]), compared to those who said that they used an IT system as part of their role but not centrally, with only 45.5% receiving training (90% CI [0.0381, 0.1058]).

Furthermore, although the training was given to those in varying levels of authority, those with increased authority were more likely to receive cyber-security training, as displayed in the bar graph below.

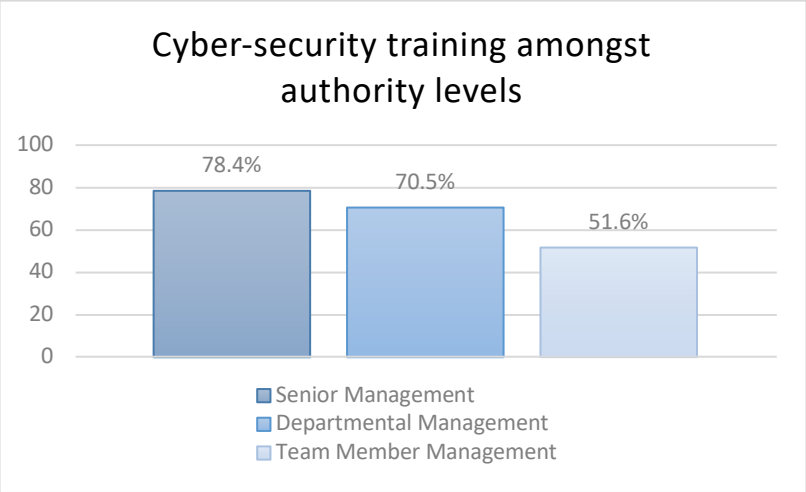

Figure 1: Bar chart showing training levels compared to level of authority

Employees also explained that oftentimes the training was not job specific and 'quite generic'. An employee explained:

> 'each position has different levels of access (a media manager has open access to the internet - entertainment hosts is an intranet so closed access) the risks for these 2 roles for example would be different'.

This meant that only 45.8% (90% CI [0.7212, 0.8305]) of employees strongly agreed that cyber-security was important for their job role. Therefore, the standardised training given to employees in varying job roles, meant that they disregard it and considered it irrelevant to their role onboard.

Similarly, given that cyber-security is considered a complex subject for most, and that the cruise ship environment is made up of employees speaking many different languages, it was also suggested that the training not only be more job specific, but also employee specific. For instance, an employee explained:

> 'Have important training like cyber security be offered in multiple languages for easier understanding. Cyber security training uses specific vocabulary that may be difficult for crew members who speak English as an additional language'.

Therefore, the exploration of the employee experience of training, shows that there is more work to be done to make it as efficient as it could be.

Next, the researcher will discuss the maintenance of training and awareness. The results show that only 16.1% of participants received any further additional training to maintain their knowledge (90% CI [0.1182, 0.2160]). Instead, passive forms of cyber-awareness, such as publications were the main source of maintenance. The bar graph below presents the various methods that were used to keep employees up-to-date with cyber-security.

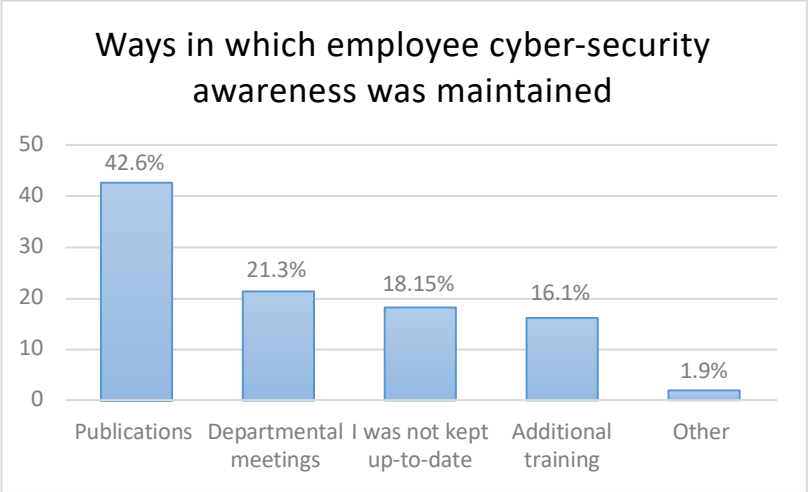

Figure 2: Graph showing cyber-security awareness maintenance

Lastly, this section will discuss the impact of the current approach to training and awareness maintenance. The implications of the sporadic training, conducted with a

standardised, generic session, suggests to the employees that cyber-security is, at present, not something which is considered as everyone's responsibility onboard. As a result, employees perceived cyber-security as an IT department responsibility only. When asked how they would respond to a suspicious threat, participants most commonly selected that they would contact the IT department. This resulted, in some instances, with the IT department becoming overburdened. For instance, an employee explained:

> '…IT was prompt with fixing the issue when reported but it was hard to get a hold of them via either phone or email. Typically I did not come across security problems but if I had, not much was promoted in terms of equipping managers with the tools they'd need to combat or prepare against'.

Furthermore, the lack of maintenance of cyber-security awareness is implying that cyber-security training is a tick box exercise. As a result, employees are disregarding their training on a practical day-to-day level, and putting the trust in the IT department to mitigate threats.

4.2. Key Finding Two: Employee's cyber-security perceptions compared to cyber-practices

This finding will discuss the perceptions of the employee and their practices onboard. Employee perceptions surrounding cyber-security and cyber threats appear to be reflective of the increased concerns of the maritime industry in general. 76.1% of employees strongly agreed or agreed that a cyber-attack on a cruise ship is a threat (90% CI [0.7006, 0.8130]) and 92.9% of the employees believed that cyber-security onboard is important (90% CI [0.8865 to 0.9569]).

The employee's perceptions surrounding cyber-security appear to be influenced by the training that they received, as demonstrated in the table below.

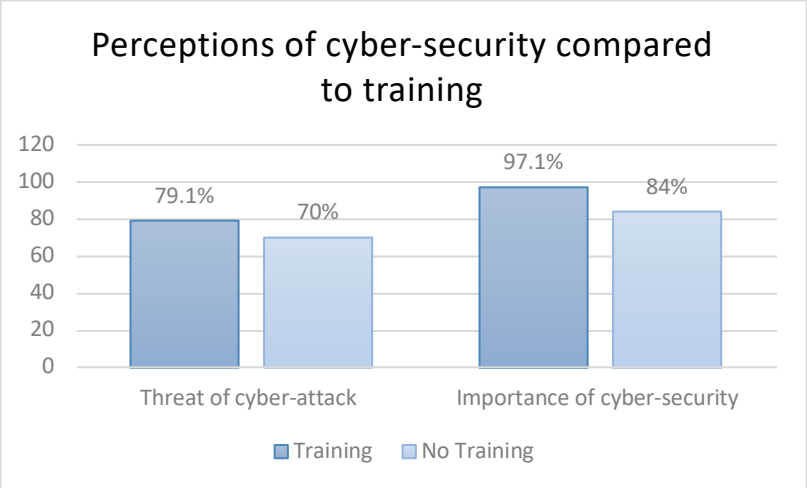

Figure 3: Graph showing the perceptions of cyber-security compared to training

However, when examined more closely, the results show that the employees seem to be more concerned about cyber-security than is evident from their practices. Despite these perceptions, 81.8% of employees conducted practices onboard that could result in a cyber-attack (99% CI [0.5485, 0.7423]), therefore showing that there is a disparity between the

intentions of the employees and their conduct onboard, which supports the findings of Albrechsten [28]. The graph below shows the type of behaviours and the level of commonality.

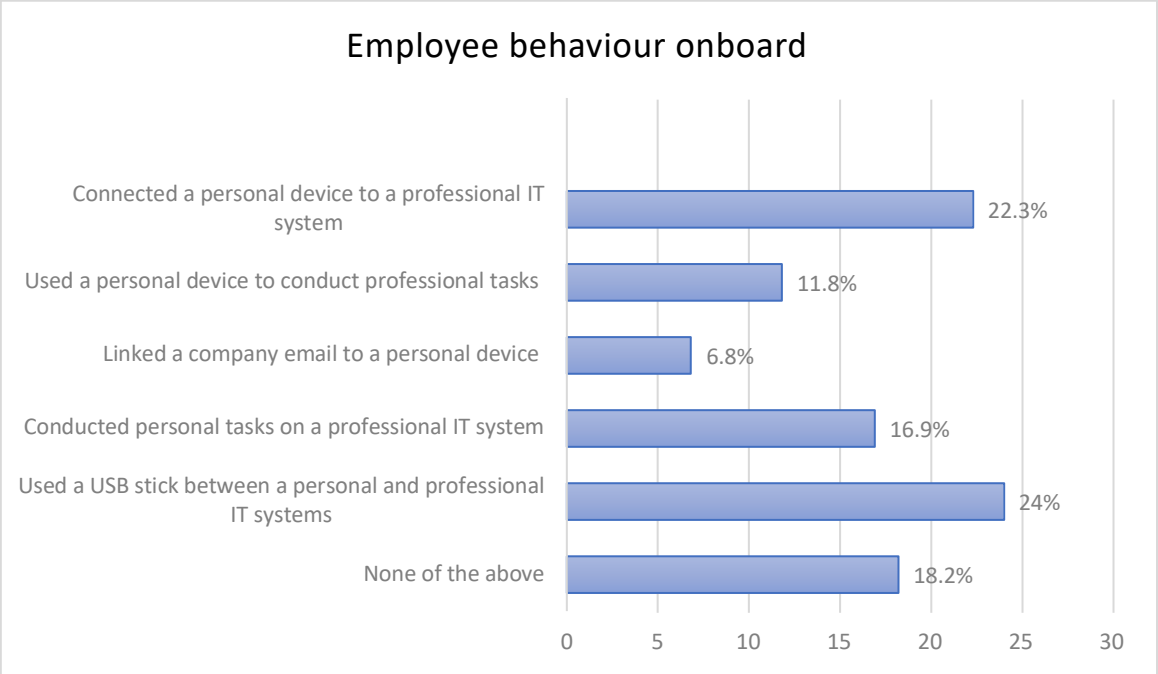

Figure 4: Graph showing common cyber-security behaviours onboard

It was found that the training did have some level of impact on the employee's conduct. Of the participants who received training, 78.6% selected behaviours (90% CI [0.3190, 0.4464]), compared to 87.5% of participants selecting behaviours who did not receive training (90% CI [0.8380, 0.9601]). However, due to the limitations of the training which were discussed above, the influence of training on the employee's practices is limited.

4.3. Key Finding Three: Day-to-day level cyber-security

The results show that despite the indication of an attempt to increase cyber-security onboard, cyber-security on a day-to-day level is not being prioritised. This is resulting in many organisational obstacles for the employees. This section will present a deeper understanding of the factors which are influencing their practices.

Firstly, there is a misalignment between cyber-security practices, and the needs of the employees in executing their job role. This is consistent with the work of Hooper & McKissask [36]. Only 41.3% of employees strongly agreed that the cyber-security rules were easy to follow when carrying out their daily tasks (90% CI [0.3499, 0.4789]), and only 31% of employees strongly agreed that cyber-security rules were useful within their job role (99% CI [0.2232, 0.4118]). As a result, in support of Koppel et al. [38], employees would often workaround cyber-security practices, opting for efficiency and convenience over security.

Similarly, a lack of connectivity onboard meant that employees were left with no choice but to work around cyber-security policies. For instance, an employee explained:

> ‘I was also required to take company electronics off of the ship into insecure internet connections in order to complete program updates as the ship internet was not strong enough to do so’.

This suggests that the cruise ship companies are not prioritising cyber-security on a practical level. This is supported by the fact that another significant reason for employee workarounds onboard was simply, a lack of resources. Employees were left with no choice but to use their own, potentially insecure devices, to conduct professional tasks because they did not have the resources needed.

Lastly, a cruise ship is an environment which encompasses employees living and working in the same space whilst being detached from the outside world. This presents obstacles to employees which need to be considered when forming cyber-security policies. For instance, a lack of connectivity both in port and onboard, as well as the high cost of Wi-Fi for crew, meant that employees commonly explained that they used onboard, professional devices and networks to conduct their personal correspondence. For instance, a participant explained:

> ‘I was in the middle of a house purchase and needed to scan and send documents over- there is often no time or appropriate place in ports we visit to do this.’

Therefore, it is not just the professional tasks of employees which are encouraging workarounds, but also personal factors, that have not been considered as part of the cyber-security strategy, which are forcing them to disregard cyber-security policies.

There is also a misalignment between the corporate policies and the workplace routines, consistent with the findings of Sadok et al. [37]. For instance, oftentimes, employees explained that their behaviours onboard were at the request of shoreside management who had assigned them tasks that were not achievable unless they ignored cyber-security rules.

Furthermore, although employees knew that their practices were jeopardising the cyber-security of the vessel, they explained commonly that they were ‘normal’. For instance, an employee explained:

> ‘I can't say I have ever really thought twice about the security risk factor in doing so and everybody does it so it seems like the normal thing to do.’

In some instances, these behaviours were even encouraged, or considered a benefit to the position onboard. For instance, an employee explained:

> ‘I also used my office computer to do personal things, yet was never told not to do so on it. I was actually advised by head office that it was one of the “perks” of my job.’

Consequently, the misalignment between the organisational cyber-security policies and the culture onboard, implies to employees that on a day-to-day basis, breaking cyber-security rules is normal and acceptable.

4.4. Recommendations

Overall, although the results outlined above indicate that the cruise ship industry has attempted to improve its cyber-security strategy with increased training and awareness amongst

employees, there is still progress to be made. The researcher recommends that training is given more thoroughly across departments to every employee, and is more job specific, to communicate the relevancy of cyber-security to each crew member. IT is also strongly recommended, that the training sessions are delivered in various languages for those who do not speak English as their first.

It is also the recommendation of the researcher that the training sessions and awareness of employees onboard is maintained. As per Albrechsten & Hovden, this should be most beneficially conducted through the use of interactive methods of cyber-security awareness [35], such as refresher training sessions or drills (which will be discussed below). This would encourage employees to continually be aware of cyber-security and enhance the change in behaviour over a longer period of time.

The researcher also recommends that the cyber-security culture onboard also needs to be addressed. As per Alshaikha, this has been seen to improve cyber-security for a sustained amount of time. There are various ways that the culture could be achieved [40]. Firstly, it must be communicated to employees that cyber-security is everyone's responsibility and not just the role of the IT department. Ultimately, at sea, every crew member's supreme priority is safety. For instance, an employee explained:

> 'Safety is our number one priority it is very important that we see different aspect on how we can deal on such incidents. This training should be considered as very important as this is a safety issue.'

Currently onboard, employees often experience safety drills to maintain their knowledge of safety procedures, as well as keep safety as a forefront priority. The cruise industry should seek to treat cyber-security as just as important, by consistently reinforcing employee's awareness that vessels are made up of complex, interlinking cyber-physical systems [51] and adopting good cyber-security practices is vital to protect the overall safety of the vessel. It should also be communicated often to employees that adopting good cyber-security practices is a necessity of every crew member onboard to prevent harm coming to all those onboard. Employees should also be informed often of what could be suspicious and how they should act if they see such occurrences. This could be done on a large scale with a drill in order to reinforce not only the importance, but also the notion that it is everyone's responsibility onboard.

As suggested by Alshaikha another way that the cyber-security culture onboard could be improved could be through the use of incentives, similar to 'employee of the month' which would reward individuals who have raised awareness of a threat or conducted good cyber-security onboard [40]. This would ignite a collective call to action, acting as a reminder to be cyber-security mindful, and alter the perceptions that poor cyber-security practices are 'normal' and acceptable onboard.

The researcher also recommends that the organisational approach to cyber-security adopts a more employee centric approach in order to mitigate some of the challenges that they face which are ultimately impacting their cyber-security practices. As per Sadok et al., it is vital that cyber-security practices are influenced by the employees who are affected by security controls [37].

Time and time again, employees blamed a lack of resources, and inconvenience as a reason for their behaviours onboard. This could be mitigated by increasing the number of secure portable devices which are available to employees so that they do not opt to use their personal device.

Lastly, it is important not just to mitigate the misalignments in the employees professional experience, but also their personal conduct also. The cost of crew Wi-Fi, and poor connectivity, is deterring employees from using the correctly assigned network. Employee's must have the ability to contact home and carry out personal tasks onboard, easily and affordably. If this is not the case, their personal needs will take priority over cyber-security measures.

5. Conclusion

To conclude, employees are aware of the importance of cyber-security onboard, yet they are conducting practices onboard which are putting cruise ships at risk of exploitation. Although employees appear to be the weak link in the cyber-security onboard, their behaviours are influenced by many, humanistic and organisational factors. Their practices are therefore the product of organisational weaknesses which have arisen because the employee perspective, and the practical day-to-day level cyber-security, have not been considered. Therefore, the cruise ship industry could take cyber-security more seriously.

Although employees are receiving training, it is rolled out amongst employees sporadically, delivered through sessions which are standard and generic across many different job roles. This means that employees consider cyber-security as irrelevant to them. Furthermore, after the training has been conducted, it is not maintained, meaning that there has been little consideration about how to actually change the behaviour of employees in the long term. This means that employees are trusting the cruise ship companies and IT departments to maintain the cyber-security of the vessel, without fully considering their role, and the potential impacts of their behaviours.

There are also misalignments between the corporate cyber-security policies, the manager's expectations and the experience of employees when trying to balance their tasks and the cyber-security practices. This means that employees are working around them or disregarding them. Furthermore, the organisational cyber-security culture does not mirror the culture onboard. This communicates to employees that cyber-security does not really matter.

This research highlights the dangers of relying heavily on a technical approach to cyber-security within the maritime industry. Applying the socio-technical perspective to the maritime environment produces results which are consistent with the perspective's previous research. Therefore, this research shows that there are many benefits, discussed throughout, which could be gained from applying the socio-technical perspective to the cyber-security of the cruise ship sector, and the maritime industry more generally. By adopting a socio-technical perspective within the maritime industry, a more holistic cyber-security strategy will be formed, which will ultimately provide more efficient protection.

The findings of this research were mostly as expected, particularly surrounding the level of common behaviours that are conducted onboard, potentially putting cruise ships at risk. However, particularly surprising was the perceptions of employees. The researcher assumed that employees were unaware of the threat of a cyber-attack/did not perceive cyber-security to be important, which would explain why frequent common bad practices were being conducted

onboard. This research suggests the opposite, which although, initially was alarming to discover, upon reflection, was actually reassuring. This therefore means that it is the obstacles which are impacting employee behaviour, which ultimately can be addressed more easily than altering people's perceptions.

This research hopes to encourage the application of the socio-technical approach within the maritime industry more so in the future. There are many areas to pursue, the avenues of which can vary depending on the corporate level. For instance, on a higher level, the researcher would suggest that an exploration of the designer perspective would be useful. Are they aware of the lives of crew members onboard and do they take it into account when they are designing the policies?

Similarly, an exploration into the efficiency of the corporate approach to training and awareness could be conducted. For instance, given that the cruise ship industry, and the maritime industry in general is made up of employees from all over the globe, future research could consider cyber-security perceptions across varying nationalities. This research suggests that employees speaking different languages may find it more difficult to comprehend the training. Therefore, the researcher would recommend future exploration surrounding the efficacy of conducting cyber-security training in various different languages for the employees who do not speak English as their first language. If cyber-security awareness and training was not only more job specific, but more tailored to the employee's learning needs, would their practices improve?

Alternatively, on a more managerial level, it would also be useful to explore the perceptions of the shoreside employees. As mentioned, oftentimes the employee behaviours onboard are the result of a request at shoreside. Future research could investigate whether the perceptions of the two sides are similar, the challenges that shoreside face and how these two elements of the organisation come together in order to reduce the conflict which is currently occurring.

Lastly, this exploration encompasses employees from various cruise lines. However, future research could focus on one single cruise ship and explore the perceptions and experience of employees in greater depth. This would allow a deeper understanding of the cyber-security practices on a more specific level rather than generically across the entire industry.

Ultimately, this research aims to encourage the adoption of a more holistic approach to cyber-security within the maritime industry, particularly with the support of the socio-technical perspective, to not only understand, but also alter user behaviour. Now is the time to take an employee centric approach to understand how to secure vessels. The researcher hopes that this is the start of employees onboard being seen as a solution to cyber-security, rather than part of the problem.

6. References

[1] G.A. Res. A. 741(18). (Nov. 4, 1993). https://www.palaureg.com/product/resolution-a-74118-international-management-code-for-the-safe-operation-of-ships-and-for-pollution-prevention-international-safety-management-ism-code/ [Accessed July 28, 2021].

[2] International Maritime Organisation, The International Safety Management (ISM) Code, 2019. URL: https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx

[3] G.A. Res. 428(98). (June. 16, 2017). https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf [Accessed July 28, 2021].

[4] G.A. Res. 1/Circ.3. (July. 5, 2019). http://www.gard.no/Content/23896593/MSC-FAL.1-Circ.3.pdf [Accessed July 28, 2021].

[5] International Maritime Organisation, Maritime Cyber Risk, 2019. URL: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

[6] White House, Statement from the Press Secretary, 2018. URL: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/ [Accessed July 28, 2021].

[7] B. Shajari, Cyber Risk Series – Emergency Response and Facility Security Perspectives, 2020. URL: https://open.spotify.com/episode/5yU5Da1V2lc1431gx2AtPb?si=bOg74vydSWSpHM321SZpCA

[8] CSIS, Significant Cyber Incidents, 2021. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[9] United States Coast Guard, Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels, 2019. URL: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf

[10] D. Sepulveda Estay, R. Sahay, W. Meng, C. Jensen, M. Barfod, Exploring Cybership Vulnerabilities Through a Systems Theoretic Process Approach, Ocean Engineering Journal (2020). http://dx.doi.org/10.2139/ssrn.3753663

[11] K. Tam, K. Jones, Maritime cyber security policy: the scope and impact of evolving technology on international shipping, Journal of Cyber Policy 3 (2018). doi:10.1080/23738871.2018.1513053.

[12] K. Tam, K. Jones, MaCRA: a model-based framework for maritime cyber-risk assessment, World Maritime University Journal of Maritime Affairs 18 (2019). https://doi.org/10.1007/s13437-019-00162-2

[13] Government Office for Science. (2017). Future of the Sea: Cyber security. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/671824/Future_of_the_Sea_-_Cyber_Security_Final.pdf

[14] M. Lund, O. Sveinung Hareide, Ø. Jøsok, An Attack on an Integrated Navigation System, Necesse 3 (2018). doi: 10.21339/2464-353x.3.2.149.

[15] B. Svilicic, I. Rudan, V. Frančić, M. Doričić, Shipboard ECDIS cyber security: third-party component threats, Scientific Journal of Maritime Research 33 (2019). https://doi.org/10.31217/p.33.2.7.

[16] B. Svilicic, D. Brčić, S. Žuškin, D. Kalebić, Raising awareness on cyber security of ECDIS, TransNav: The International Journal of Maritime Navigation and Safety of Sea Transportation 13 (2019). doi: 0.12716/1001.13.01.24.

[17] B. Svilicic, M. Kristić, S. Žuškin, Paperless ship navigation: cyber security weaknesses, Journal of Transport Security 13 (2020). https://doi.org/10.1007/s12198-020-00222-2

[18] B. Svilicic, I. Rudan, V. Frančić, D. Mohović, Towards a Cyber Secure Shipboard Radar, Journal of Navigation 73 (2020). doi: 10.1017/S0373463319000808.

[19] S. Carnovale, S. Yeniyurt, S. (Ed.), Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions, World Scientific, 2021.

[20] N. Polemi, Port Cybersecurity, Elsevier, Amsterdam, NL, 2018.

[21] National Institute of Standards and Technology, Framework for improving critical infrastructure Cybersecurity, 2018. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[22] S. Schauer, N. Polemi, H. Mouratidis, MITIGATE: a dynamic supply chain cyber risk assessment methodology, Journal of Transportation Security 12 (2019). https://doi.org/10.1007/s12198-018-0195-z
[23] S. Cobel, Carnival Confirms Passenger Data Comprimised, 2020. URL: https://www.infosecurity-magazine.com/news/carnival-confirms-passenger-data/
[24] Emergency Risk Brief, Maritime Cyber Threat Intelligence and Vulnerability Landscape, 2021. URL: https://fortressinfosec.com/blog/maritime-cyber-threat-intelligence-report-current-vulnerability-landscape
[25] J. Jeong, J. G. Mihelcic, C. Oliver, Rudolph, Towards an Improved Understanding of Human Factors in Cybersecurity, in: 5th International Conference on Collaboration and Internet Computing (CIC), IEEE, Los Angeles, CA, 2019, pp. 338-345 doi: 10.1109/CIC48465.2019.00047.
[26] M. Malatjia, A. Marnewicka, S. Solmsb, Validation of a socio-technical management process for optimizing cyber security practices, Computers & Security 95 (2020). https://doi.org/10.1016/j.cose.2020.101846
[27] A. Totade, S. Godbole, Culture and Human Factors, in: D. Antonucci (Ed.), The cyber risk handbook: Creating and measuring effective cybersecurity capabilities, 1st. ed., John Wiley and Sons Incorporated, Hoboken, NJ, 2017, pp.243-255. ISBN: 111930972
[28] E. Albrechtsen, A qualitative study of users' view on information security, Computers & Security, 26 (2007). doi:10.1016/j.cose.2006.11.004.
[29] T. Pseftelis, G. Chondrokoukis. A Study about the Role of the Human Factor in Maritime Cybersecurity, Journal of Economics and Business 71 (2021). https://spoudai.unipi.gr/index.php/spoudai/article/download/2887/2724
[30] M. Bada, A. Sasse, J. Nurse. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?, arXiv https://arxiv.org/pdf/1901.02672.pdf
[31] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, C. Jerram, Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), Computers & Security 42 (2014). https://doi.org/10.1016/j.cose.2013.12.003
[32] R. Protcor, J. Chen, The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace, Human Factors 57 (2015). doi:10.1177/0018720815585906.
[33] M. Pattinson, M. Butavicius, M. Lillie, B. Ciccarello, K. Parsons, D. Calic, A. McCormac, Matching training to individual learning styles improves information security awareness, Information and Computer Security 28 (2020). https://doi.org/10.1108/ICS-01-2019-0022
[34] R. McEvoy, S. Kowalski, Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach, Complex Systems Informatics and Modeling Quarterly (CSIMQ) 105 (2019). doi: 10.7250/csimq.2019-18.03
[35] E. Albrechtsen, J. Hovden, Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study, Computers & Security, 29 (2010). doi:10.1016/j.cose.2009.12.005.
[36] V. Hooper, J. McKissask, The Emerging Role of the CISO, Business Horizons 59 (2016). https://doi.org/10.1016/j.bushor.2016.07.004
[37] M. Sadok, S. Alter, P. Bednar, It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs, Information and Computer Security, 28 (2020). https://doi.org/10.1108/ICS-01-2019-0010
[38] R. S. Koppel, S. Smith, J. Blythe, V. Kothari, Workarounds to computer access in healthcare organizations: You want my password or a dead patient? Studies in Health and Technology Informatics 208 (2015) 220-251. doi:10.3233/978-1-61499-488-6-215.
[39] V. Zimmermann, K. Renaud, Moving from a 'human-as-problem" to a 'human-as-solution" cyber security mindset, International Journal of Human-Computer Studies 131 (2019). https://doi.org/10.1016/j.ijhcs.2019.05.005

[40] M. Alshaikha, Developing cybersecurity culture to influence employee behaviour: A practice perspective, Computers & Security, 98 (2020). https://doi.org/10.1016/j.cose.2020.102003
[41] I. Bramson, Cyber Risk Series – United States Coast Guard, 2020. URL: https://open.spotify.com/episode/2hqSRYPsLHo0a2r5D5FUk5?si=PQN0UmIHThCb531DFgJ7kw&nd=1
[42] A. Garcia-Perez, M. Thurlbeck, E. How, Towards cyber security readiness in the Maritime industry: A knowledge-based approach (2017). https://pure.coventry.ac.uk/ws/portalfiles/portal/12219284/Towards_Cyber_Security_Readiness_In_The_Maritime_Industry.pdf
[43] V. Vehovar, K. Manfreda, Overview: online surveys, in: N. Fielding, R. Lee, G. Blank. (Ed.), The Sage Handbook of online research methods. 2nd. ed., Sage Publications Ltd, London, UK, 2017, pp. 143-161. https://www.doi.org/10.4135/9781473957992
[44] C. Leddy-Owen, Questionnaire Design, in: N. Gilbert, P. Stoneman (Ed.), Researching Social Life, 4th ed., Sage Publications, London, UK, 2016., pp. 245-257. ISBN: 9781412946629
[45] V. D. Alexander, H. Thomas, A. Cronin, J. Feilding, J. Moran-Ellis, Mixed Methods, in: N. Gilbert, P. Stoneman (Ed.), Researching Social Life, 4th ed., Sage Publications, London, UK, 2016., pp. 119-139. ISBN: 9781412946629
[46] R. Likert, A technique for the measurements of attitudes, Archives of Psychology 22 (1932) 5-56.
[47] A. Bryman, Social Research Methods, 5th ed., Oxford University Press, New York, NY, 2016.
[48] E. Ruel, W. Wagner III, B. Gillespie, Nonprobability sampling and sampling hard-to-find populations, in: E. Ruel, W. Wagner III, B. Gillespie (Ed.), The practice of survey research, Sage Publications, London, UK, 2016, pp. 149-159. https://www.doi.org/10.4135/9781483391700
[49] P. Stoneman, Analysis Survey Data, in: N. Gilbert, P. Stoneman (Ed.), Researching Social Life, 4th ed., Sage Publications, London, UK, 2016., pp. 389-411. ISBN: 9781412946629
[50] A. Agresti, B. Coull, Approximate Is Better than "Exact" for Interval Estimation of Binomial Proportions, The American Statistician 52 (1998) https://doi.org/10.2307/2685469
[51] V. Bolbot, G. Theotokatos, L. Bujorianu, E. Boulougouris, D. Vassalos, Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review, Reliability Engineering & System Safety, 182 (2019). https://doi.org/10.1016/j.ress.2018.09.004