Cyber Training in Maritime Cybersecurity

Tiemen Ruijgrok & Allard de Haan

Author: Allard de Haan

E-mail: allard.de.haan@student.nhlstenden.com

Author: Tiemen Ruijgrok

E-mail: Tiemen.ruijgrok@student.nhlstenden.com

Education: Minor Hack@Sea

Educational institution: NHL Stenden

Location: Emmen

Academic year: 2023/2024 – 3rd year

Date: 12/01/2024

Table of Contents

1. Summary

The maritime industry faces escalating cybersecurity threats, exposing vulnerabilities in shipping, ports, and offshore activities. Human errors, a significant factor in these vulnerabilities, often result from social engineering attacks. Maritime cybersecurity training, as advocated by MITAGS, proves vital in fortifying industry defenses. However, the effectiveness of such training remains a critical question, especially concerning ingrained habits like clicking on suspicious links. Weak passwords persist as a pervasive issue, exemplified by a 2015 vulnerability in a satellite network. The complexity of new technologies introduces both efficiency and security risks. A chart depicting the percentage of human errors in marine accidents underscores the human factor's role. Beyond training, adherence to cybersecurity protocols, as outlined by ENISA, becomes imperative. Clear rules, comprehensive awareness, and technological safeguards contribute to a robust defense against cyber threats in the maritime sector.

To enhance maritime cybersecurity, organizations should implement comprehensive training programs for both crews and shore staff. Training should be mandatory, utilizing engaging methods such as in-house instructor-led sessions, online live programs, or video-recorded courses. Incentives like gift cards or certificates can enhance participation. General and specific cybersecurity training, aligned with industry guidelines, are crucial. External collaborations with entities like DNV or government-led initiatives, such as the Netherlands' ISIDOOR, offer large-scale training opportunities. Continuous knowledge retention is vital, achieved through platforms monitoring security information, refresher courses, and organizing conferences and webinars. Staying updated is imperative given the evolving cyber landscape. Ultimately, organizations must proactively address cybersecurity awareness to stay ahead of potential threats.

The paper also talks about how people in the maritime industry need to be careful about cybersecurity. It explains that human mistakes, like clicking on suspicious links or not securing passwords, are big problems. The solution is to have special training programs that teach both technical things and how to stay safe online. These programs should be interesting and might give rewards to encourage participation. However, not everyone takes these trainings seriously, so they should be made more fun and mandatory. The key is to focus on how people behave and make sure everyone in the industry understands and does their part to stay safe online. This helps protect important systems and keeps everything working well despite new cyber threats.

The maritime industry faces big problems with cybersecurity because of human mistakes, like clicking on suspicious links or not being careful with passwords. To fix this, special training programs are important, teaching both technical stuff and how people can stay safe. These programs should be interesting and might even offer rewards. But not everyone understands or takes these trainings seriously, so they need to be made more fun and mandatory. The key is to focus on how people behave and make sure everyone in the industry, not just the tech side, understands and does their part to stay safe online. This helps protect important systems and keeps everything working well despite new cyber threats.

2. Introduction

In a perfect world, all shipping industry factors are safe and accident-free. Unfortunately, all over the real world is accepted that human error accounts for 80-85% of all marine accidents. The most important concern of all stakeholders is the safety of ships at sea. That makes sense because the shipping industry accounts for more than 90% of global trade goods. Accidents still happen despite safety rules and a big part of them is due to human mistakes, which could lead to catastrophic losses and disruption of the Maritime Transportation System (MTS).

This paper investigates the human factor's role in maritime accidents and how these influence the effectiveness of cybersecurity measures, such as cyber training. The findings aim to help improve cybersecurity in maritime situations by dealing with the unique challenges posed by human factors with cyber training.

Social importance

Understanding how people behave online is super important for keeping things secure. Sometimes, without meaning to, people can make mistakes that open the door to cyber-attacks, like falling for fake emails. Recognizing this helps organizations train people better, make them more aware of online dangers, and build a culture of security. It also lets us create flexible security plans and deal with threats from inside the organization. In a nutshell, good cybersecurity isn't just about technology. It's about how people and tech work together to stay safe from ever-changing online threats.

Question

The main question to answer is can be made clear as follows: "how does the human factor influence the effectiveness of cybersecurity measures in the maritime industry?"
To address this question, it can be broken down into three sub-questions:

1. Identifying vulnerabilities:
    - What are the key human-related vulnerabilities and challenges that contribute to cybersecurity risks in the maritime sector?
2. Enhancing awareness and response:
    - How can training and education programs be tailored to enhance maritime professionals' awareness and response to cyber threats.
3. Cybersecurity Training Effectiveness:
    - What factors contribute to the varying effectiveness of cybersecurity training among industry professionals?

The objective of this paper is to identify the role of the human factor, organizational culture and cybersecurity effectiveness on marine cybersecurity to find out how effective cybersecurity measures are. Understanding these factors can significantly improve shipping safety through more effective measures. This paper explains the used methods in section 3. Sections 4 identifies key human-related vulnerabilities and challenges contributing to cybersecurity risks in the maritime sector. Section 5 navigates through cybersecurity training and sustainment strategies in the maritime industry. Section 6 focuses on the effectiveness of cybersecurity training.

3. Methodology

Methods were selected based on thorough analysis of past research and real-world cases.

The study involves professionals and employees in the maritime industry, including cybersecurity implementers and stakeholders. As for data collection, the research relies on surveys, interviews, articles, blogs, past research and focus group discussions to gather both quantitative and qualitative data:

1. **Surveys:** Structured to provide quantitative insights.
2. **Interviews:** In-depth discussions with experts and stakeholders.
3. **Focus Groups:** Gathering collective insights from maritime personnel.
4. **Articles, Blogs, and Past Research:** Reviewing existing literature for a comprehensive understanding of maritime cybersecurity (training).

The study used a variety of methods to look at cyber awareness and training. Numbers were studied to find problems and trends. Words from interviews were studied to understand the reason for cyber training. Articles were consulted from studies on cyber incidents and cyber training that have already been extensively conducted. These methods help in understanding the topic from different perspectives and ensure a well-rounded view. Combining numbers and real-life stories makes the findings more reliable.

4. Understanding Cybersecurity Challenges in the Maritime World: Human Errors and Risks

This part dives down at how cybersecurity is affecting people in the maritime industry. The focus lies on several important problems and questions. Such as the human errors that contribute to cybersecurity vulnerabilities and the common human-related factors that lead to security incidents. Those points are very important in today's world because cyber threats are increasing rapidly according to the maritime institute of technology and graduate studies (MITAGS).

The maritime industry not only includes shipping, but also ports and other offshore activities are part of the whole maritime infrastructure. All these parts are highly vulnerable to cyber-attacks with consequences including impact to global trade, huge financial losses, environmental damage, and even loss of life.

According to MITAGS the maritime cybersecurity training for personnel helps to improve the overall cyber security posture of the maritime industry. It is the responsibility of the industry to provide training to the workforce. Employees will gain an understanding of possible cyber threats and acquire skills to prevent them. Training helps with the recognition of suspicious activities by employees, which makes them report such incidents to authorities and take essential measures to minimize risks. An organization's proactive position can scare up potential attackers.

The big question is: do those cyber training courses really work? Imagine a situation where a worker has to do cyber training but doesn't really want to. We need to know if this training helps people understand the dangers of online threats.

For example, let's say an employee often clicks on links without really thinking about it. After the training, they might be less likely to do that, but there's still a chance they could click on suspicious links out of habit. We all know how risky it can be to click on just one link. So, it's important to figure out how much these cyber training courses really help in making our online actions safer. This is covered in Chapter 6.

Human errors, especially those related to social engineering attacks play a big role in the vulnerabilities that are in the maritime cybersecurity industry. Social engineering is a technique to manipulate individuals into revealing sensitive information. Other social-engineering methods are baiting, email, voicemail and SMS phishing and malicious email attachments. These methods can then be used to gain access to the computers of crew members and then infect the maritime systems.

In today's society hackers can do all their research on social media. The attackers can search and exploit the crew's social media networks, and to gather more information they can start a phishing campaign to gain even more knowledge. With that amount of information hacking or tricking a crew member will become easier the more you know about them. (William Loomis, 2021)

An example of this is that the crew uses e-mail applications that have an important role in the operations of the ship. Here the human factor plays a large role in the security of the ship. Only humans can detect if it is a risk and to get rid of that danger. (Thanasis Pseftelis, 2021)

As of today, the issue of weak passwords continues to exist in cybersecurity. In August 2015, Colby Moore, a researcher who works at Synack, highlighted a concerning vulnerability. He disclosed that he possessed the capability to intercept and manipulate data traversing a satellite network managed by Globalstar. This network, crucial for providing communication services and equipment to various entities, including militaries and oil companies, faced a potential risk due to the identified security flaw. (Tucker, 2015)

Crew members on ships or operators at ports might not realize the risks associated with downloading files from the internet, not using multifactor identification, clicking on email links, or having inadequate antivirus software and firewalls on their computers. Hackers could take advantage of the crew's lack of awareness by sending phishing emails. Additionally, during an attack, the separation between the crew network and the bridge network may weaken, leading to more problems. There are stories of poor cybersecurity practices, such as bridge crews setting up different password controls only to write the new passwords on sticky notes. (William Loomis, 2021)

The increasing complexity of technology in recent years, with new automation and improved systems, has made tasks easier for crews but has also introduced new security threats. The new systems that come onboard ships can cause faults in the systems because everything can be automated. This may lead to the crew using less of the automation, so they won't have to deal with all those faults. (T. Christian Miller, 2019)

For visualization and additional information, below is a chart showing the percentage of human errors in maritime incidents. This chart provides valuable insights into the causes of these incidents, and there are numerous other incidents with a similar percentage of human errors.

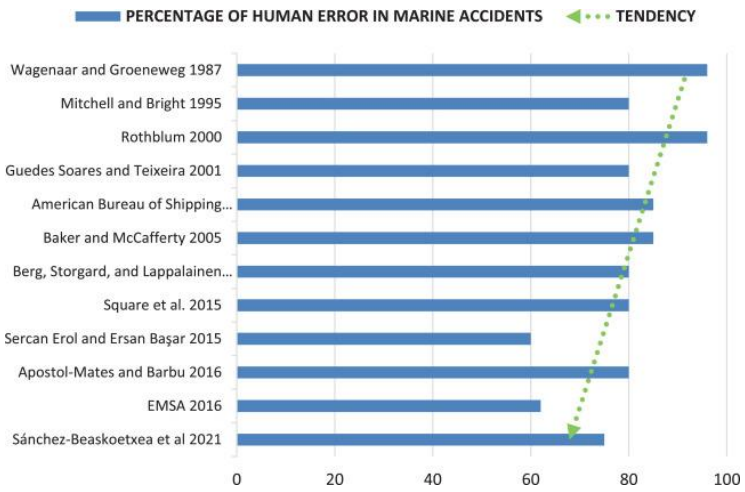

Figure 1 - Percentage of human error in marine accidents. Source: sciencedirect.com

Best Practices Guidelines

In addition to the cyber awareness training discussed in Chapter 5, Cybersecurity Practices and protocols are also crucial in preventing incidents. These protocols need regular updates to stay aligned with reality. An organization can create its own protocols and/or adhere to established standards. A good example from the European Union Agency for Cybersecurity (ENISA) is: “main measures intend to serve as good practices for people responsible for cybersecurity implementation in Port Authorities and Terminal Operators.” According to ENISA, the mentioned practices provide a solid foundation and are essential for cybersecurity alongside training.

Here are some of these mentioned practices by ENISA:

4. Set clear rules involving everyone in port operations to ensure everyone understands and participates in keeping the port secure.
5. Make sure everyone working at the port knows about and understands how to keep things secure. Train them to be aware of potential cyber threats.
6. Follow basic cybersecurity steps like keeping networks separate, updating regularly, using strong passwords, and limiting access to sensitive areas. Especially for older systems, protect networks and passwords.
7. Design applications with safety in mind, especially those that exchange data with others. This helps prevent problems that could harm the port.
8. Strengthen the ability to spot and stop cyber problems quickly. This includes using alerts, checking for signs of trouble, and using advanced methods like machine learning to identify issues.

One of the points also mentions awareness training, indicating its importance. These mentioned points are likely covered in cyber awareness training. Otherwise, professionals may encounter these protocols without much understanding, jeopardizing the standards.

In summary, cybersecurity practices and protocols, coupled with cyber awareness training described in Chapter 5, are pivotal for preventing maritime incidents. Regular updates are crucial for alignment with evolving threats. Organizations can create or adhere to protocols, like ENISA providing essential good practices.

5. Navigating cybersecurity training and sustainment strategies in the maritime industry

The human factor is addressed in the previous chapter. With that, offer courses for crews and shore staff to raise awareness concerning cyber security to prevent human mistakes. How can these training programs be offered to the maritime people? Hire a third party like DNV or start an internal campaign with a course that all personnel must take.

To reduce the risk of a cyber incident, it is most useful to provide maritime personnel with training on this subject. The impact of this training on people's awareness varies from person to person. Some individuals are eager to learn a lot to prevent future mistakes, while others have no interest in such training. The person who is interested logically benefits more from cyber awareness training. As an employer, it is therefore necessary to encourage and, in turn, obligate employees to take an offered course. It is the responsibility of employers to set up and execute this effectively to limit the danger of data breaches. In this day and age, this is particularly important because the systems and software on ships and on land are becoming larger and more crucial. Consequently, social engineering becomes an even more feared attack on employees, as it already constitutes 97% of attacks according to Det Norske Veritas (DNV).

Firstly, it is the responsibility of the organization that aims to educate its employees in the field of cybersecurity to make training as appealing as possible. This begins with advertising the training to the employees. If such training is not attractive or not taken seriously, it is already not effective.

The format of the training is a major factor in what someone prefers, such as an in-house instructor-led training program, an online live training program, or a video-recorded training program. A training may offer a choice for the person taking the training, but it will be a costly training. It is then up to the organization to determine which training format best suits the industry and the preferences of the staff.

In addition to the fact that cyber training is often mandatory from the organization, a rewarding factor can also be added to make it more attractive. Consider for example, a gift card, a contest, or a certificate after completing a training. If the organization requires employees/employers to take a well-known training, such a certificate also means something. Something that can be flaunted, as perhaps many people have completed that training or are familiar with the reputation of that certificate. Even if there is a change of client, it can be proven that you have that cyber knowledge.

There are many general, easily understandable training programs suitable for any maritime employee, such as those offered by DNV. These provide a broad overview of key elements in cybersecurity. This already tests the competence of the employee well. The goal of an organization is, therefore, that such basic training must be useful to prevent more human cyber mistakes.

Now there are also more specific cyber training programs for certain parts of the maritime organization. The problem is that not every training is suitable for every maritime employee since everyone has a different role. In a training for example, bridge systems, there will likely be training components that are not entirely applicable to that role because there are so many different functions and variations thereof. According to The International Maritime Organization (IMO), which creates certain guidelines, there are several vulnerable systems. For example, Bridge systems, Cargo handling and management systems, and Access control systems are vulnerable. They also say that these are not the only vulnerable systems because, in principle, everything is hackable, so vulnerable. IMO has developed training for these specific systems.

Another approach can be from the government. The government offers training to organizations in critical infrastructure. The Netherlands is an example of this with ISIDOOR, the largest cyber exercise in this country. ISIDOOR is a large-scale cyber exercise organized by the NCSC (National Cyber Security Center) in collaboration with the NCTV. During ISIDOOR, agreements, structures, and processes from the National Digital Crisis Plan (LCP-Digital) are practiced. Here, the national government exercises with organizations that have a role during or are involved in a (potential) digital crisis. These are organizations within critical infrastructure, but also safety regions and organizations from the National Covering System. By practicing, faster and more adequate action can be taken during a real digital crisis.

This is therefore a large-scale training that many organizations can benefit from. This saves them from organizing a training themselves. This is a different form of training in terms of what you learn from this training because in the ISODOOR training, you learn to act in a crisis situation, which may be different from cyber awareness training. Therefore, it is useful for an organization to internally offer these cyber awareness training programs even if an organization participates in such a large-scale training like ISODOOR.

So far, there is discussed how training can be provided and in what ways. A next step to keep the awareness of employees up to date is to come up with a way to not immediately forget everything you have learned after training. It is human to gradually forget critical elements in the field of cybersecurity after a long time. For an organization, it is important not only to organize training but also to keep the knowledge up to date among employees (and employers). The cyber field can change incredibly quickly, and the knowledge must remain relevant to stay one step ahead of hackers and cybercriminals.

There are already several existing methods for regularly maintaining knowledge. It is useful for the employee to realize this and take the initiative, but it remains the responsibility of the organization to initiate this. Smart Data Collective has a handy list of a few methods for this. To start, there are platforms, feeds, and websites that constantly monitor info security and post or share relevant elements. For example, you might receive an occasional notification with a short piece of news. This way, you stay both up-to-date and knowledgeable. A similar method is for example the news feed of Google Chrome. Every time the browser is opened on a laptop or phone, a number of news articles are presented. Usually, Google tries to give you articles they think you find interesting. So if you're already

interested in IT, for example, you'll automatically get more articles in the IT category. Long live cookies. Another possibility is to subscribe to certain sites so that articles from that site are standard in your Google Chrome feed. Organizations can also integrate to this in some way.

Then there are also refresher training courses, perhaps from the same publisher as the original training, to regularly refresh cyber knowledge. For example, the Center for Development of Security Excellence (CDSE) has an annual DoD Security Awareness Refresher training. This training meets certain security training requirements so that the training has the right quality. You also need to have a score of 75% to get the certificate.

Lastly, an organization can organize conferences, webinars, and meetings on cyber awareness. Perhaps even easier for the organization to do this with a third party. Nowadays, this is very easy through webinars and virtual meetings. Current cyber events can be well incorporated into these to stay up-to-date and perhaps become a bit more aware.

To remain relevant in cyber knowledge, employees and employers must stay as close to reality as possible. Given the rapidly changing technology, organizations are better off preparing themselves to be as ahead of hackers as possible.

6. Cybersecurity Training Effectiveness

With the previous chapter, we discussed various cybersecurity training programs, outlining what needs to be done, how to do it correctly, and the frequency of such training. However, the crucial question remains: How effective is all of this? Does it have any real value, or is it a necessity for everyone to partake in?

Although errors can happen to anyone, some employees may not fully grasp the security risks prevalent in today's world. According to research by Tessian, while 99% of IT and security professionals acknowledge the significance of a robust security culture in maintaining a strong security posture, there is a noteworthy 30% of employees who believe they have no part to play in upholding cybersecurity measures. (Keary, 2022)

For an average employee cybersecurity probably isn't the number one priority. Especially if they haven't experienced an attack. TalentLMS made a quiz with Kenna security on how much employees already know about cybersecurity principles. Achieving a passing grade on the quiz requires answering at least four questions correctly, and unfortunately, 60% of participants fell short of this benchmark. The result might be viewed as acceptable if employees had not undergone prior training, but the surprising fact is that 69% had received training from their employers. (Marousis, 2021)

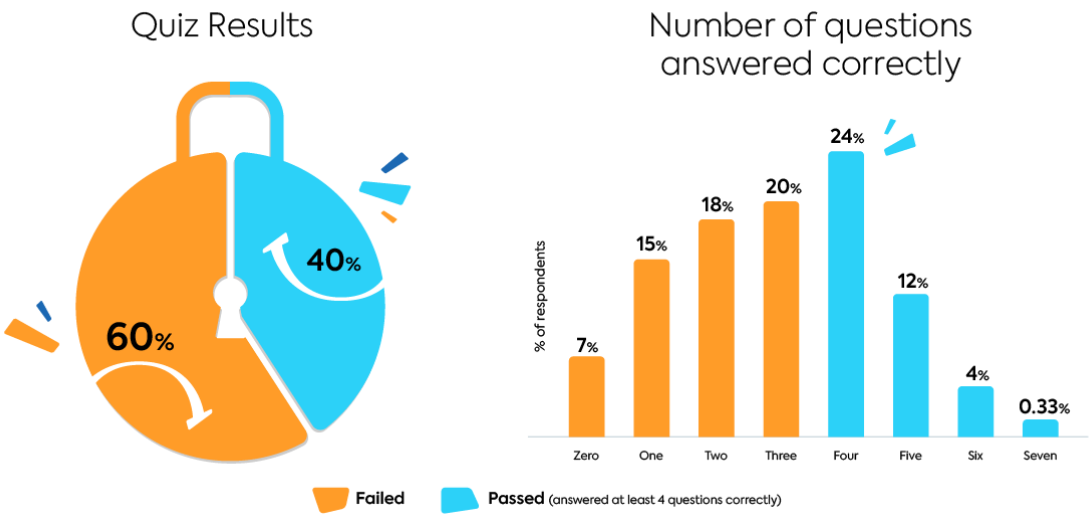

Figure 2 Quiz results on cybersecurity. Source: Talemtlms.com

In 2017, I.H.S. carried out a survey on maritime cybersecurity, and 284 people shared their thoughts and experiences. What stood out was that a significant portion, around 30 percent of those who took part in the survey, mentioned that their organizations didn't have anyone specifically looking after information security or a dedicated department for it.

This finding suggests that a good number of maritime-related businesses might be missing out on having someone keeping an eye on cybersecurity matters. Not having an information

security manager or department can make these organizations more susceptible to potential cyber threats, which is a bit of a concern in today's digital world.

Another interesting point that came up in the survey was about employee training. It turns out that some employees in the maritime sector haven't received any training to be aware of potential cyber risks. This is like missing a step in making sure everyone in the organization knows how to protect against online threats. (Ozdemir, 2018)

The effectiveness of cybersecurity training may vary among employees, but its value is undeniable, making it crucial for everyone to actively participate to gain a more secure company environment.

7. Conclusion

The maritime industry faces significant cybersecurity challenges that are linked to human factors. The main question for this paper is: “How does the human factor influence the effectiveness of cybersecurity measures in the maritime industry?”

Human-related vulnerabilities pose significant cybersecurity risks in the maritime industry. Issues like clicking on suspicious links, falling victim to social engineering attacks, and poor cybersecurity practices, especially concerning password security, contribute to these vulnerabilities. Additionally, the increasing reliance on technology and automation, along with potential misuse of personal information from social media, further heightens the susceptibility of maritime systems.

To tackle these vulnerabilities, tailored training and education programs are crucial in improving the awareness and response of maritime professionals to cyber threats. These programs should not only cover the technical aspects but also focus on the human element, such as recognizing and mitigating social engineering attacks. The success of these programs depends on engaging maritime professionals, making it essential for organizations to offer diverse and appealing training formats, potentially using rewards or certifications to encourage participation.

The effectiveness of cybersecurity training varies among industry professionals due to several factors. Research indicates that while most professionals receive training, a significant portion may not fully grasp security risks or prioritize cybersecurity. This gap in understanding emphasizes the need to make training programs more engaging, relevant, and mandatory to ensure active participation. The choice of training format, incentivizing completion, and tailoring training to specific roles within the maritime sector are critical factors influencing effectiveness.

In conclusion, the human factor plays a crucial role in the effectiveness of cybersecurity measures in the maritime industry. Identifying vulnerabilities related to human behavior, customizing awareness and response programs, and understanding factors influencing training effectiveness are all essential components of a comprehensive cybersecurity strategy. Organizations must actively address these human-related aspects to establish a robust cybersecurity posture in the maritime sector, recognizing that technology alone is insufficient without considering the human dimension. By doing so, the industry can better mitigate risks, protect critical infrastructure, and ensure the secure and resilient operation of maritime systems in the face of evolving cyber threats.

8. Discussion

Turning to the methodological aspects of this research:

Reliability:

Efforts were dedicated to ensuring the reliability of our study. Using diverse sources, such as surveys, interviews, and existing studies, contributed to a comprehensive understanding of maritime cybersecurity.

Validity:

Alignment with prior research and real-world scenarios enhances the validity of the findings. By connecting the methods with established knowledge, the aim was for accuracy and credibility.

Usability:

Practicality was a key consideration. The chosen methods, including surveys and interviews, generate insights applicable to the maritime industry. The study is designed not just for theoretical value but with a practical intent to enhance cybersecurity measures in real-world contexts.

In summary, the research methodology prioritized reliability, validity, and usability, making it a robust resource for practical improvements in maritime cybersecurity.

Source list

Chrome heeft eigen RSS-feed voor nieuws, zo gebruik je het. (2021, 18 juni). Androidworld.nl. https://androidworld.nl/tips/chrome-heeft-eigen-rss-feed-voor-nieuws-zo-gebruik-je-het

Cyber security: defending the tanker at sea, in port and from the crew. (z.d.). Riviera. https://www.rivieramm.com/news-content-hub/news-content-hub/cyber-security-defending-the-tanker-at-sea-in-port-and-from-the-crew-64671

DOD Annual Security Awareness Refresher. (z.d.). Https://securityawareness.usalearning.gov/awarenessrefresher/index.html

Fig. 3. The overview of HFACS-MA framework applied here, adopted from. . . (z.d.-b). ResearchGate. https://www.researchgate.net/figure/The-overview-of-HFACS-MA-framework-applied-here-adopted-from-31_fig1_315632140

Ginger, G. (2023, 9 mei). *Why is cyber security so important to mariners? - Maritime Institute of Technology and Graduate Studies (MITAGS)*. Maritime Institute of Technology and Graduate Studies (MITAGS). https://www.mitags.org/why-is-cyber-security-so-important-to-mariners/

Global, D. (2021, 2 juni). Maritime Cyber Security & Threats 23-31 May 21. *Maritime Cyber Security & Threats*. https://channel16.dryadglobal.com/maritime-cyber-security-threats-12-18-apr-1

Guillermo Francisco Perez (2019,). *Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry* https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2102&context=gscis_etd

Hasanspahić, N., Vujičić, S., Frančić, V., & Čampara, L. (2021). The role of the human factor in marine accidents. *Journal of Marine Science and Engineering*, *9*(3), 261. https://doi.org/10.3390/jmse9030261

How to keep your data security knowledge up to date? (2022, 27 oktober). SmartData Collective. https://www.smartdatacollective.com/how-to-keep-data-security-knowledge-up-to-date/

Keary, T. (2022, Jul 26). *Report shows a third of employees don't understand importance of cybersecurity*. Retrieved from VentureBeat: https://venturebeat.com/security/importance-of-cybersecurity/

Lee, Y., Park, S., Lee, W., & Kang, J. G. (2017). Improving cyber security awareness in Maritime Transport : a way forward. *Journal of the Korean Society of Marine Engineering*, *41*(8), 738–745. https://doi.org/10.5916/jkosme.2017.41.8.738

Maritime Cyber Security Awareness E-learning - DNV. (z.d.). DNV. https://www.dnv.com/maritime/maritime-academy/cyber-security-elearning.html

Maritime Cybersecurity. (z.d.). https://www.maritime-cybersecurity.com/

Maritime Cybersecurity training. (z.d.). https://www.maritime-cybersecurity.com/Maritime_Cybersecurity_Training.html

Marousis, A. (2021, Apr 6). *Cybersecurity training lags, while hackers capitalize on COVID-19*. Retrieved from Talentlms: https://www.talentlms.com/blog/cybersecurity-statistics-survey/#How_much_do_employees_actually_know_about_cybersecurity

Miller, T. C. (2019, 20 december). *The Navy installed touch-screen steering systems to save money. Ten sailors paid with their lives.* ProPublica. https://features.propublica.org/navy-uss-mccain-crash/navy-installed-touch-screen-steering-ten-sailors-paid-with-their-lives/

Nationaal Cyber Security Centrum. (2023, 17 april). *ISIDOOR – de grootste cyberoefening van Nederland*. https://www.ncsc.nl/onderwerpen/isidoor

Ozdemir, A. B. (2018, May 28). *Maritime Cyber Security: Seafarers are at the frontline*. Retrieved from Linkedin: https://www.linkedin.com/pulse/maritime-cyber-security-seafarers-frontline-ahmet-bahad%C4%B1r-%C3%B6zdemir/

Port cybersecurity - Good practices for cybersecurity in the maritime sector. (2019, 26 november). ENISA. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

Pseftelis, T. (2021). *A Study about the Role of the Human Factor in Maritime Cybersecurity* https://spoudai.unipi.gr/index.php/spoudai/article/viewFile/2887/2724

Sánchez-Beaskoetxea, J., Basterretxea-Iribar, I., Sotés, I., & Maruri, M. (2021). Human error in marine accidents: Is the crew normally to blame? *Maritime Transport Research*, *2*, 100016. https://doi.org/10.1016/j.martra.2021.100016

The importance of cybersecurity in the maritime industry. (z.d.). https://marine-digital.com/article_importance_of_cybersecurity

Thanasis Pseftelis, G. C. (2021). *A Study about the Role of the Human Factor in Maritime.* https://spoudai.unipi.gr/index.php/spoudai/article/viewFile/2887/2724

T. Christian Miller, M. R. (2019, Dec 20). *The Navy installed touch-screen steering systems to save money.* Retrieved from ProPublica: https://features.propublica.org/navy-uss-mccain-crash/navy-installed-touch-screen-steering-ten-sailors-paid-with-their-lives/

Tucker, P. (2021, 11 april). *Hacker cracks satellite communications network*. Defense One. https://www.defenseone.com/technology/2015/08/hacker-cracks-satellite-communications-network/118915/

William Loomis, V. V. (2021, Oct 4). *A system of systems: Cooperation on maritime cybersecurity*. Retrieved from atlanticcouncil: https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-a-system-of-systems/