JOURNAL OF MARITIME RESEARCH

Vol XIX. No. III (2022) pp 89–95

ISSN: 1697-4040, www.jmr.unican.es

Addressing cyber security vulnerabilities and initiatives in Malaysia maritime industry

Marhaini Mohd Noor[1]

ARTICLE INFO

Article history:
Received 30 Nov 2022;
in revised from 30 Nov 2022;
accepted 6 Dec 2022.

Keywords:
Cyber security, cyber-attack, cyber risk, vulnerability, maritime industry and cyber safe.

ABSTRACT

Cyber security is a global issue to any organisations, sectors and industries. Thus, this piece of article is important for this journal as it focuses on interdisciplinary cyber security in human aspects and policy perspectives. The issue is emerging on cyber-attack across the globe. The cyber-attack leads to physical consequences especially loss of data, environment and human. This has created concern on level of awareness within maritime management and industry. The level of awareness provides understanding how these affect the industry in order to minimize cost. Main problems are there is no alarm warning for vulnerability of cyber security and there is no mandatory framework on this issue. Thus, this is a conceptual paper reviews concepts and studies to propose the ideas and solution. Therefore, this has brought the idea of cyber risk management whereby involves top-down approach. This does affect the organisation or industry. In addition, investing in maritime cyber security needs a thorough analysis. This could reduce the cyber risk with the use of cyber risk assessment. On the other hand, information sharing is also crucial which reflects this issue on cyber security. Information sharing can also be used with the collaboration from stakeholders. The use of information and communication technology (ICT) makes the process easier, efficient and effective. Maritime industry needs to have smart ports and digital solution with the age of revolution 4.0. Maritime industry players need to integrate the system and services to ensure resilient to such attacks. Required cyber security standards for maritime industry and increase level of awareness can address this issue. Future research will further investigate the cyber risk assessment analysis for cyber safe approach with the understanding of maritime logistic sector to ensure information sharing in supply chain. With the technology, this will improve logistic processes.

1. Introduction.

Cyber security is a global issue to any organisations, sectors and industries. The issue is emerging on cyber-attack across the globe. The cyber-attack leads to physical consequences especially loss of data, environment and human. This has created concern on level of awareness within maritime management and industry. Cyber security consists of technologies, processes, and controls designed to protect systems, networks, programs, devices and data from cyber-attacks. Cyber transformation depends not only on technology, but also on human capital. Therefore, raising awareness of cyber security among human or people is a need. This study focusses on cyber security vulnerabilities in Malaysia maritime management and industry. The review and analysis made based on previous studies from different countries.

Cyber security vulnerability is flaw or weakness in a computer system, its security procedures, internal controls, or design and implementation, which could be exploited to violate the system security policy. This vulnerability is also relating to cyber-risk and cyber-attack. When there is a risk, the cyber security will be vulnerable. Hence, the higher the exploitation to vulnerability, the higher the risk. Therefore, cyber security vulnerability occurs at the beginning of network system or operating system which is an internal event that occurs. This is different from cyber threats which occurs in an outside or exter-

[1]Universiti Malaysia Terengganu.
*Corresponding author: Marhaini Mohd Noor. E-mail Address: marhaini.noor@umt.edu.my

nal event such as downloading virus (Hewitt, 2021).

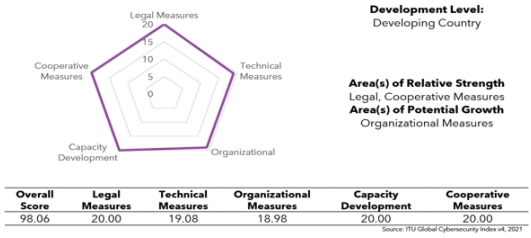
1.1. Cyber security concept.

Cyber Space is an environment where communication takes place between computer networks. Cyber security means a situation where data protection from the occurrence of a crime or unauthorized access; or steps taken to protect data from misuse. In Malaysia, these two terminologies refer to initiatives, programs and best practices in maintaining data security and the well-being of cyberspace played by expert agencies in the field of cyber security.

The Global Cyber Security Index (GCI) is an initiative of the International Telecommunication Union (ITU) involving experts from different backgrounds and organisations. The Global Cyber Security Index (GCI) is a composite index produced, analysed and published by the International Telecommunication Union (ITU) to measure the commitment of countries of its members on cyber security in order to raise cyber security awareness. Each member countries are measured by Legal, Organisational, Technical, Capacity building and also Cooperation (ITU, 2020).

Malaysia

Figure 1: Global Cyber Security Index 2020 - Country profiles.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.06	20.00	19.08	18.98	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Source: ITU Global Cybersecurity Index v4, 2021.

In 2018, Malaysia ranked 8th out of 193-member countries in the world. Malaysia was ranked eighth out of the top ten countries in the 2018 Global Cyber Security Index. As of now, Malaysia's strength is in the area of technical, organisation and also capacity building. Malaysia also ranks second with the highest score in the organisational and the capacity building pillar in the Asia Pacific region. Compared to achievement of higher-ranking countries, Malaysia's weaknesses are in the area of legal and cooperation pillars. In 2017 GCI ranking, Malaysia was at number three in the world. As GCI has been regarded as one of the best and reliable measurement related to cyber security achievement, other countries have actively improved their ability in all five measured areas. The GCI is one of the best measurements that can be used as benchmark to identify the achievement of a nation in combating cyber-attack (ITU, 2020).

Cyber security Malaysia has produced a report related to the GCI 2018 result. The suggestion among others, in the legal area are to focus on enforcement, investigation, prosecution and punishment. There is also a need for coordination and understanding among law enforcement agencies. Suggestion also included to improve the existing law for local implementation and up-to-date with global and international legislation development particularly related to cross-border crime activities. Another area of measurement is the cooperation which looking at improvement on bilateral and multilateral cooperation with other countries and region. This also includes the cooperation with other sectors such as industry and private sectors.

1.2. Cyber security vulnerability in Maritime industry.

Cyber security is a process to protect networks and devices from external threats. Therefore, there is a need for legal protection and monitoring from unauthorised access. Cyber security is also known as information security. As such it protects the personal, organisation or industry and government data from being attack. Cyber-attack is aim to disrupt, destroy, or control computer systems and networks or even delete, manipulate or steal data within the system. This is a critical issue to be tackled by maritime administrations, which claimed cyber security awareness and culture are part of companies' administrations. Different companies and administrations have different companies and administration of cyber risks. Overall, there is no major incident and loses recorded as a result of cyber-attack. However, the risk of cyber-attack is very high and could have adverse impact on maritime logistics (Chronis, 2019).

As a consequence, maritime logistics should be more prepared and alert with the issues and challenges. "Maritime port infrastructures rely on the use of information systems for collaboration, while a vital part of collaborating is to provide protection to these systems" (Polatidis et al., 2018). Therefore, maritime logistic is vital to explain its complex features and environment of maritime logistic network. This arrangement would customise ports or maritime logistic operations to better face the challenge of cyber threats and cyber-attacks. This is a combination of cyber security and risk management to tackle the issue of governance in maritime logistics environment. With the emerging of technologies, the demand for high resilience in global logistics is essential for cyber security to be well-prepared (Pyykkö et al., 2020).

According to Microsoft vulnerabilities report 2021, vulnerability is soaring as threat continues to expand and accelerated by the mass shift to remote working. Many attackers gain access to accounts and increase the level of privileges to compromise other IT assets. Therefore, enforcing least privilege is the fastest and most effective measure to address this problem (BeyondTrust, 2021). According to Maurushat (2013), vulnerability refers to a feature or weakness of a computer or data system's design, integration, and maintenance. Thus, vulnerability can either be direct (weak passwords) that lead to unauthorized access, or indirect (UNCTAD, 2020). More than 90 per cent of attackers are familiar with the target's vulnerabilities. The vulnerabilities can be divided into three categories: 1) known vulnerability, 2) zero-day attack, and 3) future threat (Maurushat, 2013; Ahokas et. Al, 2017).

1.3. International Maritime Organisation (IMO)- United Nations UNCLOS.

The International Maritime Organization (IMO) is the pre-eminent international organization with competence to establish international rules and standards for the safety, security and environmental performance of international shipping (NUS, 2022). In this context focuses on security, which is cyber security. IMO is a specialized agency of the United Nations. Established by the Convention on the International Maritime Organization, 1948.

UNCLOS is internationally and applicable agreed international regulations and recommended procedures. The roles where navigation and shipping are concerned. The codes, guidelines, procedures, recommendations within the framework of IMO Conventions (safety, environment, security, trade facilitation).

Therefore, the cyber security could reduce vulnerability and protect the industry or organisation from cyber-attacks. This paper addresses and reviews the weaknesses or vulnerabilities occur in maritime communities.

2. Literature Review.

2.1. Cyber security in Malaysia context.

Malaysia has been witnessed on the development of Information and Communication Technology (ICT) since couple of years. Everyone in a community, organisation and industry were not being left out as part of this digital age. People must learn and use ICT in their daily life and no one is excluded from not using the technology. Industries are becoming more attached to this digitalization. It becomes necessity to individuals, organisations, industries, government and civil society. Thus, whatever that is connected to the ICT, particularly internet is exposed to cyber risk. As a result, Malaysia introduced cyber security strategy that is holistic and the idea is to have secured, trusted and resilience cyberspace. This is a strategy to respond to cyber threats by strengthening cyber security governance (National Security Council, 2020).

In addition, whenever there is a connection, there is the possibility of leakage and also the possibility of instruction. Emerging cyber threats have become a lot more sophisticated, disastrous; and pose serious risks and challenges to individuals and nations.

2.2. Cyber security challenges.

The awareness on cyber security needs and challenges in the maritime logistic is currently low to non-existent. Maritime logistics should consider a crisis protocol to develop and implement awareness among the maritime actors. In particular, it is highly recommended to provide cyber security training to relevant organisation such as shipping companies, port authorities, etc. Lack of awareness and focus on cyber security leads to low sense of urgency and less preparedness in facing cyber risks (Gard, 2016). The main challenge posed by cyber security are process, people, and technology.

2.3. Multi actors' roles.

The maritime industry need to adapt more innovative, aggressive and proactive approaches in order to stay ahead of cyber threats. The industry also has to effectively face the challenges with dynamic approaches, inter-agency cooperation and also strengthening the public-private partnerships. In addition, the need for cyber security encompassing people, process and technology is rather critical and such need will continue to grow in many more years to come. All in all, there is a necessity to enhance domestic and international collaboration in information sharing, practical legal and technical approaches, capacity building and also cyber security awareness and education (Gard, 2016).

2.4. Mitigation vulnerability.

Cyber security is essential to individuals, organisations, industries and government agencies. Cyber security is like infrastructure and people are taking it for granted. When they are facing problems, only then they realised the importance of cyber security. It is also regarding as common good where there is no ownership but everyone is involved and affected by the incidents. Thus, difficult to declare who is responsible to act or response to ensure safety and security.

Sea paradoxes on cyber security policy making (as shown in Table 1). This is an overview of policy making paradoxes to control and mitigate vulnerabilities. Mitigation plan in risk assessment is also known as risk mitigation plan. This is also required to safeguard the cyber-attacks and risks within the assessment plan. The mitigation plan is to help the organisation or industry to be prepared for the worst and having the system in place. However, for this study the focus is on cyber security risk assessment. The assessment is a continuous assessment where time and resources are needed to improve the future security of the industry (Cobb, 2021).

2.5. Cyber security policy framework.

This policy shall be operationalised by having detailed guidelines and plans of action at various levels such as organisation, industry, district, state, national, regional and global. This is to address the challenging requirements of cyberspace security.

The National Institute of Standards and Technology (NIST) Cyber security Framework consists of five core elements which are: identify, protect, detect, respond and recover. Buildings Cyber security Framework (BCF) provides the organizations with a set of cyber security best practices, policies and procedures to improve their cyber security posture; defines structured methodologies to interact cyber security activities and outcomes from the executive to operations levels. Thus, BCF use the NIST framework as the basis for the cyber security. Those five core elements were crafted to address evolving cyber security threats and vulnerabilities. With the BCF, an organization will be able to: assess their target cyber security state and current cyber security posture; identify and prioritize improvement opportunities and necessary actions by continuous and repeatable

Table 1: Overview of policy-making paradoxes.

Policy-making question	Description of the paradox
What is the desired level of protection of systems?	Governments want companies and citizens to protect themselves. Nevertheless, government want to have a backdoor to control and detect criminality and terrorism.
How much (cross-border) collaboration is necessary to fight cybersecurity?	Countries need to collaborate as cybersecurity is a global phenomenon, however, they do not trust each other as they might be active in hacking each other.
Who to fight to?	Despite that impact of attacks are often visible, the attacks and villains are hard to determine.
What is the right amount of spending on cybersecurity?	Too little spending on cybersecurity might indicate that they are not well protected, while too much spending might send the message that they are overly concerned and there might be something wrong.
What is the right level of visibility?	Organizations do not benefit from making the problems and attacks visible to their customers as they might decrease faith and trust. Yet, this visibility is necessary to create a greater sense of urgency and initiate action.
How will the data be used?	The same data that can be used to improve the quality of life can also be used against citizens.
Who should ensure the cybersecurity of systems?	Organizations providing or who can provide security might not suffer from its impact.

Source: Janssen & Bruijn, 2017.

process; assess progress towards the target state; and communicate cyber security risk among internal and external stakeholders. This involves regulators to execute policy on cyber security or information security in this context (NIST, 2018).

Figure 2: NIST-BCF Cyber security framework.

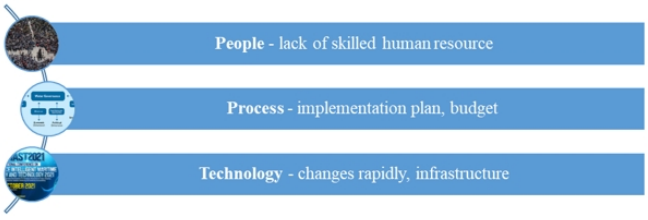
Source: NIST, 2018.

3. Methodology.

This study applied a systematic literature review on the concepts of cyber security in Malaysia context as its operations in Maritime management and industry. The review also includes framework applies in other countries and issues as well as challenges facing the industry and Malaysia. Relevant secondary data from government official websites, publications, reports, national data sets and policy frameworks have been reviewed and thematically analysed.

This research is based on previous studies and maritime sector in Malaysia deploying document analysis approach using secondary data from key officers in the organization. The data were analysed using policy-making paradoxes and cyber security policy framework. The findings clustered under three pillars of success namely People, Process and Technology. Under the pillar of People, the challenges are lack of skills, cyber security is everyone's responsibilities and human error, whilst under Process, challenges identified are lack of implementation plan, wrongly placed human resource and lack of budget. The challenge in Technology is that it moves too fast. The findings are useful for the cyber security policy makers and implementers (Chooi, A. Kamil & Suhazimah, 2018).

Figure 3: Cyber security policy framework.



Source: Author, 2021.

4. Results and Discussion.

4.1. Cyber awareness.

In general, the level of awareness of the Malaysian community on cyber security is increasing increased and showed a positive change. This is evidenced by the demand for the implementation of cyber security programs implemented specifically by Cyber Security Malaysia. Apart from that, the efforts implemented by the industry, NGOs and government agencies in the cyber security program are also gaining popularity among the community. Various initiatives and programs developed and implemented to ensure issues related to cyber security can be communicated to the grassroots community so that no dropouts in ensuring community social networks are preserved especially in use of ICT.

Table 2: Summary of findings on cybersecurity vulnerabilities.

Authors	Results	Actors
Gard, 2016 National Security Council, 2020	Cyber awareness – low, moderate	Maritime industry, government, NGOs
NIST, 2018, Alexander, 2021	Cyber-attacks - low	Maritime industry, government, community
NIST, 2018, Li & Liu, 2021 A. Chodakowska, S. Kańduła & J. Przybylska 2022	Cyber threats – cyber crime	Maritime industry, NGOs, government, community
Chooi et al, 2018 Alexander, 2021, ITU, 2020, Hewitt, 2021, Cobb, 2021	Cyber resilience	Maritime industry, NGOs, government, community

Source: Author, 2021.

Maritime communities are well received by the development and use of ICT in society. This is evidenced by the application of technology used by the outside community the city encompasses various functions of life including socializing, doing business, buying necessities, performing banking activities and others (A. Chodakowska et.al, 2022). This is directly related to the maritime industry involved in the process. Even during the implementation of the Movement Control Order (MCO/*PKP*) recently, the Malaysian society began to shift with the use of electronic applications and cars to ensure necessities and the smooth running of life as usual. Malaysians are easy to adapt and accept well the current technological developments that affect their lifestyle.

Social connections or social networks are important in ensuring a level of security cyber in society today. In ensuring the level of cyber security is at the desired level, a lot of factors that influence such success include the completion of the planned program, social relations of the community, time and place of implementation of the initiative or program. Support from various parties (NGOs, agencies, individuals and government) are also among the factors of something success. This social relationship allows the community to connect and communicate with each other as well as disseminating the delivery of cyber security messages more effectively in addition to the use of easy to understand language. This presentation is not limited to the cyber world only, but it also includes the world reality. However, there are limitations to the delivery of cyber security messages particularly in terms of understanding of an issue. But this can be overcome with the method of implementing the field program as well as the cooperation between agencies, industry players as well as NGOs to ensure cybersecurity messages reach the roots grassroots so that they are spared from becoming victims of cyber-crime (Mamade & Dabala, 2021).

4.2. Cyber-attacks & cyber threats.

To understand the challenges faced in handling the cyber-attacks and cyber threats in Malaysia, first, have to understand our current environment and surroundings. In this digital age, as the technology changes, the threat trends also change, in a dynamic way. Cyber security also has evolved with the technology. If not, the consequences will be very severe. There are also challenges in the ability to understand the changing situation and how prepared in term of people, process and technology.

The industry might be secure today, but as the environment is changing, there must be equivalently innovative and dynamic. Furthermore, at times, cyber security even cannot cope with technology. That is why the industry have to be cyber resilient. The is a need to make continuously improvement regarding cyber security. The need to understand and assess the risk involve and put in place the necessary measures. Hence, regular assessment is needed to secure one's system. The need to put the safeguard in place according to standards that is define. That will be the country's benchmark on cyber security. The industry cannot afford cyber security implementation less than the standard. On the other hand, there is no such thing as too secure. No matter how mature or secure is an organisation, it can still be attacked and it can be compromised. Thus, an organisation can always respond and minimise the impact of the attack such as they know what to do, they have the right person, they have the proper procedure in place, who can do what in what circumstances following the procedures (MCSS, 2020).

4.3. Cyber resilience.

The maritime industry must also have predictive capability. The trend can predict the cyber-attack or possible cyber-attack can describe the actors that can put in place necessary measure. If the attack does happen, the industry will already have the necessary step in place to detect, to respond, and to recover. Other than predictive, there is also the preventive, detective, responsive and eradication/corrective measure.

It is quite difficult to measure the success of a policy or strategy pertaining to cyber security. Although implementation of cyber security involves all three areas: people, technology and process, and using up-to-date approach, still there will be loop holes and gaps in defending the cyber environment against attack. The development of new and emerging technologies undeniable will also create gaps and vulnerabilities against cyber threat (Mohamed & Geir, 2015). Implementation of latest and up-to-date cyber security solution will not make an organization or a nation totally immune from attack. It will help to reduce attempt of attack, make it difficult to attack and increase the resiliency of organization to recover from such attack. This shows that cyber security is a journey where it will be a continuous effort to identify new tactic applied by threat actors, to

identify gaps and vulnerabilities in cyber environment, update with latest patches on systems and network, conduct awareness programs continuously and involve every level of population, revisit and improve policies and guidelines in daily operation etc. Apart from that cooperation is a must as this will be a platform for knowledge and experience sharing among members of the cooperation (MCSS, 2020).

Conclusions.

Cyber security has to be comprehensive because the technical in cyber security is very important, but it is not sufficient. And the traditional approach cyber security approach is still relevant, but it is not sufficient. Because in cyber resilience, no matter what the industry does in cyber security, cyber-attack will happen. Besides, the industry should assume that the perpetrators have already penetrated the system. The issues are how the industry detect and how industry respond and minimise the risk. Thus, the leaders or top level of management must embed cyber resilience because cyber security is insufficient and maritime industry needs cyber resilience to grow and sustain in the business.

Malaysia Cyber Security adopts a holistic and adaptive approach to cyber security. It is needed to secure the system, the network and the data from cyber-attacks. The need to see cyber security via people, process and technology. As such, people need awareness, training and knowledge. While process is a proper cyber security process and audit assessment. And technology is monitoring vulnerability, forensic, trusted anti-virus and others. In this complex and connected digital age, traditional cyber security measures are no longer enough. There is no 100% security for a public and private organisation, academia and a country as a whole. It is no longer the question of how to secure oneself from being attack. It is just a matter of time or when they will suffer cyber-attack. It is better to assume they will eventually break through the organisation's defences (MCSS, 2020). This is why cyber security should be top priority.

The maritime industry should work on a strategy to reduce the impact of cyber-attacks. This is called being cyber resilient. Therefore, Malaysia, as a nation, has successfully adopted a holistic approach to enhancing the security of its cyber environment. While at the same time, as a part of the global community, Malaysia also aims to strengthen its international cooperation to respond to global cyber challenges. With such an approach, the hope to be able to benefit and take the advantages of a secure, resilient and trusted cyber environment (NIST, 2018).

People are and will always be dependant and rely heavily on the Internet and digital technologies in their daily activities as well as business. The industry can't deny that there are a lot of advantages and opportunities by having digital technologies such as cloud computing, IoT, artificial intelligence, automation, machine learning, deep learning, big data, blockchain, etc. However, the Internet and digital technologies also act as a double-edged sword. The Internet and digital technologies can be misused by cybercriminals to conduct illegal and criminal activities. The cyber threat actors globally are individual actors, state actors, non-state actors, and others.

Cyber security will still be relevant for a long time. This is because technology keeps evolves very fast, and it is tough to keep up with the technology. As technology changes and as the industry expand, as there are more devices in place and the attack surface will also increase. Therefore, Malaysia as a nation has successfully adopted a holistic approach in enhancing the security of its cyber environment. Whilst at the same time, as a part of global community, Malaysia also aims to strengthen its international cooperation to respond to global cyber challenges. With such approach, the hope to be able to benefit and take the advantages of a secure, resilient and trusted cyber environment.

Acknowledgements.

This work has received funding from the Malaysian Ministry of Higher Education under Fundamental Research Grant Scheme (FRGS) 2019-1. Reference code: FRGS/1/2019/SSI10-/UMT/02/1.

References.

A. Chodakowska, S. Kańduła & J. Przybylska (2022). Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. Lex Localis - Journal of Local Self-Government. Vol. 20, No. 1, pp. 161 – 192, January 2022. https://doi.org/10.4335/20.1.161-192(2022) ISSN 1581-5374 Print /1855-363X Online © 2021 Lex localis Available online at http://journal.lex-localis.press.

Ahokas, Jenna; Kiiski, Tuomas; Malmsten, Jarmo; Ojala, Lauri M. (2017): Cybersecurity in ports: A conceptual approach, In: Kersten, Wolfgang Blecker, Thorsten Ringle, Christian M. (Ed.): Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23, ISBN 978-3-7450-4328-0, epubli GmbH, Berlin, pp. 343-359, https://doi.org/10.15480/882.1448

Alexander S. Gillis. (2021). NIST Cybersecurity Framework. TechTarget Network. https://searchsecurity.techtarget.com/definition/NIST-Cybersecurity-Framework?utm_campaign=202-10927

BeyondTrust, (2021). Microsoft Vulnerabilities Report 2021. https://www.beyondtrust.com/resources/whitepapers/microsoft-vulnerability-report

Chooi, S. T., A. Kamil, M., & Suhazimah, D. (2018). Cyber Security Challenges in Organisations: A Case Study in Malaysia. 4th International Conference on Computer and Information Sciences (ICCOINS). *Semantic Scholar*. DOI:10.1109/ICCOINS.2018.8510569 Corpus ID: 53094707

Cobb (2021). Cobb Technologies-Category: Cyber Security. https://discover.cobbtechnologies.com/blog/tag/cybersecurity

ENISA (2019). Port Cyber Security: Good Practices for Cyber Security in the Maritime Sector. European Union Agency for Cyber Security. ISBN 978-92-9204-314-8, DOI 10.2824/32-8515.

Gard (2016). Gard Alert: Managing cyber risks at sea. https://www.gard.no/web/updates/content/20912875/gard-alert-managing-cyber-risks-at-sea

Hewitt, K. (2021). What is a Cybersecurity Vulnerability? Definition and Types. *Security Scorecard* Retrieved from https://securityscorecard.com/blog/what-is-a-cybersecurity-vulnerability

ITU (2020). Global Cybersecurity Index. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Janssen & Bruijn, (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Delft University of technology, Faculty of Technology Policy & Management, Jaffalaan 5, 2628BX Delft, The Netherlands. Government Information Quarterly 34 (2017) 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Li Yuchong & Liu Qinghiu (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. Volume 7, November 2021, Pages 8176-8186. Elsevier

Mamade Bayisa Kune & Dabala Diriba Mangasha (2021). Exploring the Correlation between Cyber Security Awareness, Protection Measures and the State of Victimhood: The Case Study of Ambo University's Academic Staffs. Journal of Cyber Security and Mobility, Vol. 10 4, 699–724. doi: 10.13052/jcsm 2245-1439.1044 © 2021 River Publishers

Maurushat, A. (2013). Disclosure of Security Vulnerabilities: Legal and Ethical Issues. London: Springer

MCSS (2020). Malaysia Cyber Security Strategy 2020-2024 Report. National Security Council, Prime Minister's Department Putrajaya, Malaysia

Mohamed Abomhara & Geir M. Køien (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility Vol4. Issue 1. Page: 65-88 doi: https://doi.org/10.13052/jcsm2245-1439.414.

National Security Council, (2020). National Cyber Security Agency (NACSA). National Security Council Prime Minister's Department, Putrajaya, Malaysia. .https://www.nacsa.gov.my/

NIST, (2018). The Five Functions: Cyber Security Framework. National Institute of Standards and Technology, U.S. https://www.nist.gov/cyberframework/online-learning/five-functions

NUS (2022). IMO and Regulation of International Shipping. Activities at sea. https://cil.nus.edu.sg/research/ocean-law-policy/activities-at-sea/imo-and-regulation-of-international-shipping/

UNCTAD (2020). Review of Maritime Transport. United Nations Conference on Trade and Development. ISBN 978-92-1-112993-9. United Nations, Geneva.