Cybersecurity in the maritime industry: a literature review

Changki Park[a], Wenming Shi[b], Wei Zhang[b], Christos Kontovas[a], Chia-Hsun Chang[a*]

[a] Liverpool John Moores University, 3 Byrom Street, Liverpool, L3 3AF, UK
[b] Australian Maritime College, Maritime Way, Newham, Tasmania, 7248, Australian

*Corresponding author. E-mail: c.chang@ljmu.ac.uk

Keywords: cybersecurity, risk management, maritime industry

ABSTRACT

Cybersecurity has become an important issue in the maritime industry due to many reported cyberattack incidents that caused a lot of economy loss, personal or company information breach, and so on. However, there is limited research for maritime cybersecurity in the existing literature. This research aims to identify threats influencing cybersecurity in maritime operations and their control options through a state-of-the-art literature survey. A list of cyberattack incidents in various industries are presented. By restricting our attention to the maritime industry, this research identifies three maritime cyber threats, including the lack of training and experts, the use of outdated system, the risk of being hacker's target. To deal with the identified threats, a number of mitigation strategies are also proposed in this study, including developing cyber security process, providing cybersecurity training course, updating and upgrading programme regularly, and fostering cybersecurity climate.

1. Background

Around 80% of international trade is transported by sea [1]. At the same time, increased communication in international trade causes higher concerns on cyber-attacks as an emerging issue to maritime operations [2]. For example, Maersk, the largest container shipping company in the world, suffered a cyber-attack in 2017, which led to a loss of $200-300 million [3]. The COSCO terminal in Port of Long Beach was cyberattacked in 2018 [4]. These cyber-attacks emphasize the importance of cybersecurity in the maritime industry as they caused not only economy loss, but also personal or company information breach, companies reputation harm, etc.

Cyber-attack incidents have resulted in unquantifiable losses of monetary assets, intellectual property, and customer confidence [5]. However, to the best of authors' knowledge, there is limited research for maritime cybersecurity in the existing literature. In the aspect of maritime cyber risk, it has been defined as a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised [6].

In order to deal with hazards in the maritime industry, risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the maritime industry [6]. Compared to other industries such as military, financing, airlines, cybersecurity related studies in the maritime industry is sitting at the backseat (e.g. ten to twenty years behind other computer-based industries [7]). In light of the above evidence, the authors have found that the cybersecurity in the maritime industry needs to be addressed in urgency. This research thus aims to identify threats influencing cybersecurity in maritime operations and their control options through a state-of-the-art literature survey.

The rest of this paper is structured as follows. Section 2 reviews the definitions of cybersecurity and revisits cyberattack incidents in various industries. Section 3 identifies the cyber threats within the maritime industry. Section 4 proposes the potential control options. Discussion and conclusion are drawn in Section 5.

2. Literature review

2.1. The definition of cybersecurity

It has been used in a wide range of academic disciplines including computer science, engineering, political studies, psychology, security studies, management, education, and sociology [8]. Cybersecurity is commonly defined as "the protection of cyberspace as well as individuals and organizations that function within cyberspace and their assets in that space" [9]. [8] also re-defined cybersecurity as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure de facto property rights".

2.2. Cyberattack incidents

The top 5 industries at greater risk of cyber-attack are government, financial services, manufacturing, education and law [10]. For instance, Department of Justice in the U.S was

hacked in 2016, and it took a week for the organization to recover the system [11]. Equifax, an American credit company, had suffered a cyber-attack in 2017 and caused 143 million customers' personal data were hacked, as well as 200,000 credit card numbers [12]. Marriott hotels had suffered cyberattack in 2018 and 500 million customers' personal data were hacked [13].

2.3 Maritime cyberattack incidents

Comparing to the past, more and more maritime cyberattacks are reported in this decade due to the development of ICT and largely relay on such technology in the maritime industry. Table 1 lists the reported maritime cyberattack incidents from 2001 to 2018.

Table 1 Maritime cybersecurity incidents

Year	Organization	Details
2011	IRISL	An Iranian shipping line, IRISL, were cyberattacked in 2011 and lost all data related to rates, loading, cargo number, date and place. [14]
2011-2012	Port of Antwerp	Drug traffickers hired hackers to breach IT system of Port of Antwerp. Hackers accessed secure data giving them the location and security details of containers which contained heroin and cocaine. [15]
2012	Australian Border Force	This incident allowed criminals to check whether their shipping containers were regarded as suspicious by the Customs authorities. [16]
2012-2014	Danish Maritime Authority	Danish Maritime Authority was subjected to a cyberattack from 2012 but been discovered until 2014. The attack was introduced by a PDF document infected with a virus, and the virus was propagated from the Danish Maritime Authority to other government institutions. [17]
2013	Mobile Offshore Drilling Unit	A group of hackers remotely attacked a floating oil rig off the Gulf of Mexico and gained control of its stabilization systems and programmed the platform to tilt dangerously to one side. The platform had to be shut down for 19 days. [18]
2016	Korean vessels	South Korea reported that 280 vessels suffered problems with their navigational systems. The GPS signal was jammed by hackers; consequently, some of the GPS signals died and others received false information. [19]
2017	Maersk	Maersk, the largest container shipping company in the word, was cyberattacked by a ransomware (NotPetya) in 2017, which shut downed Maersk's network system. It took almost three weeks to recover and caused a $200-300 million financial lose. [3]
2018	COSCO terminal at Port of Long Beach	COSCO terminal at the port of Long Beach has been attacked by ransomware in July 2018 and took 5 days to recover. However, they did not suffer serious financial loss, as they took a lesson from Maersk incident in 2017 and separated their network in different servers. [20]

2018	Port of Barcelona	Hackers attacked several servers in the port's security infrastructure, without interrupting the maritime and land operations. [21]
2018	San Diego Port	The attack had not stopped vessels or boat using the port, or put members of the public in danger. The main impact would be on the issuing of park permits, public records requests and general business services. The Port said some of the disruption was because of staff shutting down computers that were in danger of being compromised as the ransomware started to spread. [22]

Based on the above cyber-attacks reports, it can be found that the number of cyber-attack incidents in the maritime industry are increasing in this decade. The impacts of maritime cyberattack include economy loss, personal or company information breach, company's reputation harm, etc. Therefore, maritime cybersecurity is becoming an important issue that needs to be emphasized more than before.

3. Threats identification to maritime cybersecurity

This section identified several threats that impact on cybersecurity in the maritime industry from the existing literature, including the lack of training and expert, the use of outdated IT system, the risk of being hackers' target, and fake website and phishing email.

3.1. Lack of training and expert for cybersecurity

Human error has been previously identified as the most significant factor that causes around 80-90% of shipping accidents directly and indirectly [23], [24]. Human can be tired to make some mistakes that cause cyberattack incidents [25]. Cyberattacks might also come from unintentional actions via individuals with little or no cybersecurity training and awareness [26]. This allows malware to deliver through individual's activities. For example, computers are infected by accidently open unknown e-mail and access false website with virus.

3.2. Use of the outdated IT system

[27] and [28] analysed vulnerability of cybersecurity in the maritime industry and found a major problem as the over reliance on outdated technology and security practices. For instance, maritime employees still believe that firewalls and antivirus software are sufficient to deal with cyberattacks. However, hackers can attack through viruses and other assorted malware and it is difficult for traditional antivirus software to deal with such advanced cyberattacks [27]. On the other hand, as large ships are expensive and take a long time to build, many ships were built before cybersecurity as a major concern. Thus, some vessels are still operating through outdated software systems that might cause cyberattack [28].

3.3. Risk of being hackers' target

Hacktivism is the most common threat for cybersecurity in the maritime industry [6]. Hacktivism has two types of actions: targeted and untargeted [26], [29], [30]. Targeted attacks refer to a company or a ship's systems and data are the intended target, hackers usually use tools and techniques specifically created for a company or ship; whereas untargeted attacks are likely to use tools and techniques available on the internet, which can be used to locate,

discover and exploit widespread vulnerabilities that may also exist in a company and on-board a ship [29].

[31] suggested that cyberattack with purpose would be practiced by three categories: hacktivism or activist group, terrorist group, and criminals. For hacktivism or activist group, they are made up of ideologically motivated people, for whom the main action is an online protest aimed at accessing the system and stealing sensitive information and data for malicious purposes. For terrorism, they can use electronic and computerized media as a new modus operandi to carry out their terrorist acts against other groups, nations, and companies, gaining access and interrupting the operating system, for ideological, religious or political interests or purposes. For criminals, individuals or criminal organizations use cyber-attacks against interconnected systems and networks, with the intention to carry out criminal activities, mainly focused on fraudulent operations, extortions or theft of intellectual property. It is also recognized that these criminals, when they obtain access to the different systems, can control operating systems to facilitate the trafficking of drugs, arms and contraband money to obtain economic benefits or to sell valuable information to another.

3.4. Fake website and phishing email

Sea crew using private devices (e.g. smart phone, tablet, personnel USB device, etc.) could cause cyberattacks through accessing fake websites and phishing emails, and further installing malicious virus into vessel system [32]. Malware is one of the well-known malicious software, which assesses or damages the victim`s devices without the knowledge of the victim, and spread by opening infected email attachments or access fake website with malicious malware program such as Trojan horses, worms, exploits and backdoors [33]. Cyber incident of Petya and Notpetya have spread over the world recently. The idea of ransomware attacks is, encrypting and locking the files on a computer until the ransom is paid. These attacks usually enter the system by using Trojans, which has malicious programs that run a payload that encrypts and locks the files. The basic goal of this type of attack is getting money, so hackers usually unlock the files when they receive the money [34].

4. Risk control options for cyberattacks

4.1 Develop cybersecurity process

[6] and [29] recommended the functional elements that support effective cybersecurity process: identifying, protecting, detecting, responding, and recovering. In fact, there were some changes of cybersecurity process after huge cyber incident such as Maersk in 2017. COSCO has learnt the importance of cybersecurity process, and divided data in several servers. Therefore, when they suffered the cyberattack in 2018, they cut down the connection of the infected server and operated through other non-infected servers. In addition, their quick response and notification to customer was the reason to minimize risk of cyberattack [35].

4.2. Education and training for cybersecurity

In order to deal with the threat of lack of training and expert for cybersecurity, training sea crews and staffs may be an effective method to enhance maritime cybersecurity. [28] suggested that ship crews can be educated to deal with cyberattack by protection of password and access keys. Companies need to train their staffs and sea crews how to use digital equipment in a

correct way, which can not only reduce the damage to the equipment, but also protect from cyberattacks. An event tree or standard operation process should be established to guild the staffs and sea crews to avoid or deal with cyberattacks. Companies can also follow the suggestion related to cybersecurity training from IMO STCW (International Maritime Organization Standards of Training, Certification, and Watchkeeping) code and ISM (International Safety Management) code.

4.3. Upgrade and update system

In order to deal with the threat of use of the outdated IT system, it is necessary to keep update vaccine software and using updated program to mitigate cyber risk [36]. Through the development of advanced technology, many virus and malicious program are also created simultaneously. The maritime industry need to update or even upgrade IT system for not only keep their competitiveness, but also deal with the threat from cyberattacks.

4.4 Cybersecurity climate

Cybersecurity climate is a control option for cyber threat. This concept is adapted from safety climate, which is defined as the coherent set of perceptions and expectations that employees have regarding safety in their organization [37]. Safety climate can be used to proactively assess an organization's effectiveness in identifying and remediating work-related hazards, thereby reducing or preventing work-related ill health and injury [38]. Based on the above safety climate related literature, we develop cybersecurity climate as the environment of company to enhance awareness cyber risk and to prevent for cyber accident.

To foster cybersecurity climate in a company, several activities are adopted from safety climate, such as cybersecurity attitudes of management, cybersecurity education and training program, cybersecurity regulation and the status of security personnel, etc.

5. Conclusion

It has been growing relying many electronic and automated devices in maritime industry, cybersecurity issue has been increasing in this decade. Maritime industry is nationally and globally significant; the importance will be increased. Therefore, we focused on identifying cyber threats and developing risk control option in the maritime industry. In this study, four cyber threats have been identified, including lack of training and expert, use of the outdated IT system, Hacktivism, and fake site and phishing email. Four risk control options are also proposed, including developing cybersecurity process, education and training, upgrade and update system, and change cybersecurity climate.

For the further research, a set of interview will be conducted to validate the identified threats and risk control options and explore more if they are not identified from the literature review. Based on the results of interview, another questionnaire will be sent out to collect the likelihood, consequence, and probability of failure detection of each threat. Failure Modes and Effects Analysis (FMEA) with Fuzzy Rules Bayesian Network (FRBN) and Evidential Reasoning (ER) are used to evaluate the importance of the threats in maritime cybersecurity. Risk matrix will also be conducted to present in a simple and common way of the results to the maritime industry.

Acknowledgement

This project is funded by the International Association of Maritime Universities Young Academic Staff in FY2019.

6. REFERENCES

[1] UNCTAD, *Review of Maritime Transport*, 2016, Available at: http://unctad.org/en/PublicationsLibrary/rmt2016_en.pdf

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

[3] Novet, J., Shipping company Maersk says June cyberattack could cost it up to $300 million, 2017, Available at: https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

[4] World Maritime News, COSCO Shipping Lines Falls Victim to Cyber Attack, 2018, Available at: https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/

[5] Julisch, K., Understanding and overcoming cyber security anti-patterns, *Computer Networks*, 2013, 57 (1), 2206-2211.

[6] IMO, guidelines on maritime cyber risk management, 2017 MSC-FAL.1/Circ.3REFERENCES.

[7] Caponi, S., and Belmont, K. Maritime cybersecurity: A growing threat goes unanswered, *Intellectual Property and Technology Law Journal*, 2015, 27 (1), 16-18.

[8] Craigen, D., Diakun-Thibault, N., & Purse, R. Defining cybersecurity, *Technology Innovation Management Review*, 2014, 4(10), pp.13-21

[9] Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., and Kusev, P. Risk perceptions of cyber-security and precautionary behavior, Computers in Human Behavior, 2017, 75 (1), 547-559.

[10] Bendovschi, A., Cyber-attacks–trends, patterns and security countermeasures, *Procedia Economics and Finance*, 2015, 28, pp. 24-31.

[11] Department of Justice in the U.S cyberattack, 2016, Available at: https://edition.cnn.com/2016/02/08/politics/hackers-fbi-employee-info/index.html

[12] Equifax, 2017, Available at: https://www.bbc.co.uk/news/business-41575188

[13] Marriott hotels cyberattack, 2018, Available at: https://www.bbc.co.uk/news/technology-46401890

[14] IRISL, 2015, Available at: https://www.joc.com/maritime-news/container-lines/carriers-threatened-cyber-attacks-experts-warn_20150303.html

[15] Antwerp Bateman, T., Police warning after drug traffickers' cyber-attack, BBC News, 2013. Available at: http://www.bbc.com/news/world-europe-24539417

[16] PORTSTRATEGY, 2017, Available at: https://www.portstrategy.com/news101/port-operations/planning-and-design/cyber-security-feature

[17] Linton Art, Port Authority Role in Cyber-Security, Linked in, 2016, Available at: https://www.linkedin.com/pulse/port-authority-role-cybersecurity-art-linton

[18] MODU, 2013, Available at: https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities

[19] Saul, J., Cyber Threats prompt return of radio for ship navigation, Reuters, 2017, Available at: https://www.reuters.com/article/us-shipping-gpscyber- idUSKBN1AN0H
[20] COSCO World Maritime News, COSOCO shipping lines falls victim of cyberattack, 2018, Available at: https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/
[21] Information Security Newspaper, Hacking attack in port of Barcelona, 2018,Available at: https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/
[22] BBC New, San Diego port hit by ransomware attack, 2018, Available at: https://www.bbc.co.uk/news/technology-45677511
[23] Schröder-Hinrichs, J. U., 'Human and Organizational Factors in the Maritime World – are We Keeping up to Speed?', *WMU Journal of Maritime Affairs*, 2010, 9 (1), pp.1–3.
[24] Heij, C. and Knapp, S., 'Predictive Power of Inspection Outcomes for Future Shipping Accidents – An Empirical Appraisal with Special Attention for Human Factor Aspects', *Maritime Policy and Management*, 2018, 45 (5), pp.604-621.
[25] Cole, Connected Ships and Cybersecurity Frank J Coles, Transas CEO Shipping Insight Fleet Optimization Conference, 2017.
[26] North P&I club, Cyber risk in sipping, North of England P&I group, 2017
[27] Sen, R., Chpter 9. Cyber and information threats to seaports and ships. McNicholas, MA, *Maritime Security*, 2016, 2, pp. 281- 302
[28] Jones, K. D., Tam, K., & Papadaki, M.,Threats and impacts in maritime cyber security, 2016.
[29] BIMCO, The Guidelines on Cyber Security Onboard Ships (Version 3), 2018.
[30] Ahokas Jenna, The finnish maritime sector and cybersecurity, *PUBLICATIONS OF THE HAZARD PROJECT*, 2019, University of Turku.
[31] IET, Code of Practice, *Cyber security for Ports and Port System*, Available at: https://cybersail.org/wp-content/uploads/2017/02/IETCyber- Security-Code-of-Practice-for-Ports-Port-Systems.pdf
[32] Japan P&I Club, Cyber risk and Cyber security countermeasures, 2018, Available at: https://www.piclub.or.jp/wp-content/uploads/2018/05/Loss-Prevention-Bulletin-Vol.42-Full.pdf
[33] Teoh, C.S. and Mahmood, A.K., Cybersecurity Workforce Development for Digital Economy. *The Educational Review*, 2018, USA, 2(1), pp.136-146.
[34] Fayi, S.Y.A., What Petya/NotPetya ransomware is and what its remidiations are, *In Information Technology-New Generations*, pp. 93-100, Springer, Cham.
[35] COSCO JCO.com, Cosco's pre-cyberattack efforts protected network, 2018, Available at: https://www.joc.com/maritime-news/container-lines/cosco/cosco%E2%80%99s-pre-cyber-attack-efforts-protected-network_20180730.html
[36] Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cyber security, 2015, Lancaster University.
[37] Zohar, D., Safety climate in industrial organizations: theoretical and applied implications. Journal of Applied Psychology, 1980, 65, pp. 96-102.
[38] Schwatka, N. V., Hecker, S., & Goldenhar, L. M., Defining and measuring safety climate: a review of the construction industry literature. *Annals of occupational hygiene*, 2016, 60(5), pp. 537-550.