Maritime Safety and Security Standard Operating Procedure (SOP) for Homeland Security

A Master Thesis

Submitted to

of

University

by

Name

DEDICATION

I dedicate this thesis to my parents. Without their patience, understanding, support, and, most of all, love, the completion of this work would not have been possible.

ACKNOWLEDGMENTS

ABSTRACT

The maritime industry is the largest service industry in global trade and has to keep up with modern trends to service world trade effectively. In keeping up with modern trends it has he maritime industry has adopted modern technological solutions to deal with age-old challenges of risk and security, which now comes through cyber-attacks. In adopting modern solutions there is need to developing standard operating procedures for responding and handling cybersecurity. This Standard Operation Procedure (SOP) project aims at researching and putting together a critical guideline to facilitate preparedness, response, and handling of cybersecurity issues in maritime industry based on the fundamental pillars; people, process, and technology for Maritime Operations. The research drew on material written in previous studies on maritime and cybersecurity and the operationalization of the fundamental pillar for preparedness, response, and handling of attendance. The research process relied on analysis of secondary data. The process involved researching the library, the web and other databases for books, research articles among other publications. Government and private organizations were also consulted since they have huge repositories of information. The Analysis of the information from the provided sources supported the significance of realizing a synchronization of the three critical pillars.

TABLE OF CONTENTS

Introduction

The The significance of the maritime industry in global trade cannot be overstated. According to Minim and Sachramm (2018), over 80% of global trade is seaborne. As global trade and gross domestic product (GDP) continue to grow, seas will be called upon to transport even more cargo. The importance of seaports will also continue to grow. Ports no longer handle loading and offloading of cargo alone, they have become critical logistical century influencing multiple supply chains. Alongside the growth of maritime shipping industry, there has been the advancement in technology that has facilitated interconnectivity through the internet and automation of processes. The technological advancements have been adopted by most industries across the world. Due to the significance of the maritime industry, the industry, thus has to keep up with technological advancements that are taking place in the world. The industry had to incorporate the new technologies to improve efficiency and security of the cargo transported through the different global maritime shipping routes. The maritime industry is increasingly moving towards the adoption of systems that rely heavily on digitization, automation, and integration (Hayes, 2016). ICT development has disrupted the maritime industry and created new operational modalities that are technology depended (Bălan, 2018). The extensive use of advanced technological solutions in the maritime industry is driven by the urgent need to maintain the industry in sync with all other industries that seem to have a step forward in adopting technological solutions. As a result of this growth and development in technological solutions, the security of data and other sensitive information has increasingly become a huge concern for the industry (Bueger, 2015). Cybersecurity has become a priority for the maritime industry. With many of the operational and critical system having already been digitized, automated, and integrated, the concern has now shifted to how entities within the maritime industry should implement appropriate procedures

and policies to respond to cybersecurity incidents effectively. The automated and digitized system, irrespective of how modern they are cannot function on their own without interaction with humans, who are the users. The systems also merely execute processes initiated by humans. In order to get the best out of these systems, there is a need to synch between the people, the processes and the technology. A sync of the three pillars will enhance the response to maritime incidences and thus enhance security within this industry. A sync means that all the systems, processes, persons and technologies necessary to detect, prevent or respond to an attack work together a single unit. The sync can be realized by developing Maritime Safety and Security Standard Operating Procedure (SOP) for Homeland Security. The development of the Standard Operating Procedure (SOP) is the primary objective of this project. In this regard, the project is committed to providing a critical guideline of preparing for, dealing with, and responding to cybersecurity issues based on three fundamental pillars; people, process, and technology.

Background

Cybersecurity refers to the ability of entities to prepare for possible attacks initiated through the internet, react to those attacks, and be able to recover from those cyber incidents (Kimberly, 2018). Cybersecurity in the maritime industry is not an isolated development, and recent incidents such as the Estonia cybersecurity attack in 2007 and Stuxnet in 2009 should have served to demonstrate to the Maritime industry the disruptiveness of cybersecurity breaches (Herzog, 2011). The maritime industry has not had major cybersecurity issues in recent times, and thus the industry seems to have let its guard down. The maritime industry has played down any of the legitimate fears of a potential cybersecurity attack, despite 90% of the world trade being facilitated by the maritime industry (Hoffmann, 2018). Expectations, competition, and tensions are at highest as different entities within the maritime sector to streamline their services,

add value, and strategically try to meet the demands of their customers and those of global safety and sustainability. Despite the technical dimension, cybersecurity has, there a growing consensus that cybersecurity can no longer continue being treated exclusively as a technological issue. There is an increasing need that guidelines established to maintain an effective maritime cybersecurity framework adopt a commitment to people and processes too other the current exclusive commitment on technology (Fitton, 2015). The underlying commitment of this project is to provide a critical guideline of preparing for, dealing with, and responding to cybersecurity issues based on three fundamental pillars; people, process, and technology.

Literature Review

Traditionally, attacks in the maritime industry, especially on ships, were often in the form of pirating, theft, boarding, and at times, destruction. Such attacks were hugely successful, especially in the Indian Ocean near Somali waters, where several ships were frequently hijacked, held hostage. The hijackers often demanded ransom in exchange for the release of the ships and crew. This process was the norm for over 5 years, and the pirates were always successfully since they recognized how difficult it was for the ships to call and receive help promptly (Hareide, 2018). Once technological solutions are integrated extensively within the maritime industry, threat of attacks and hijacking along maritime routes will decline. The experience of mitigating those attacks for a while got the maritime industry thinking it had finally succeeded in making the industry completely safe and insulated from further attacks. Unfortunately, that sense of security and confidence started to be compromised as criminals started to exploit other means to disrupt the industry (Kalogeraki, Apostolou, Polemi, & Papastergiou, 2018). With the industry keen on adopting technological solutions to ensure efficiency in the delivery of its services, criminals identified a way to cause disruption, earn financial gains, and exact their control in the industry

(Boyes, 2015). According to Boyes (2015), Cybersecurity attacks became the new vulnerability that could hurt the maritime industry to its core.

Cybersecurity attacks require cyber criminals not to be at the scene of the attack as was required some years back. Cybercriminals who are miles away could cause damage and disruption to the maritime industry or part of it with a click of a computer button. The criminals need only expose vulnerabilities, which then they will use to plant malicious content of maritime industry systems causing damage and ending up compromising the functioning of systems. Cybersecurity framework has heavily been interested in improving the technological aspects of cybersecurity and in the process, neglects the people and process aspects (Bowen, 2011). People in this respect included, all individuals involved in the maritime industry, need to be made aware of the potential cybersecurity risks that face their industry. The processes pillar, on the other hand, involves the activities and procedures that take place in the process of conducting maritime shipping activities. Addressing processes entails the need to have in-depth conversations on how various interconnected processes and procedures should be defined in light of the evolving developments of cybersecurity (McPhee, 2015). The technology pillar explores how various software technologies can be leveraged to mitigate cybersecurity risks.

Project Design

To investigate how cybersecurity threats to the maritime industry, the project relied on a qualitative research design. The research design used secondary data and thus relied on searching, reading and reviewing of published data (Johnston, 2013). The design was both exploratory and descriptive. The search for secondary sources involved search for reports, studies and related documents from websites, public libraries, books, and data from already filled in surveys. In the same vein, some government and nongovernment agencies store information which this

project can retrieve and use. Many organizations are likely to implement the findings of this project to ensure that their networks, data, and systems are safe from cyber-attacks. The researcher will provide the results to all institutions and organizations to allow them to practice by the proposed recommendations. The sources found were evaluated for the information they provided on preparedness, response, and handling of cybersecurity threats. Only sources the met the criterion for inclusion was included in the finding of this project. The sources had to deal with either one or all the three factors; preparedness, response or handling of cybersecurity threats and incidents, and the role the three primary pillars (processes, people and technology) play in the preparedness, responding and handling of risks and incidences.

Findings

There are several processes involved in handling maritime activities which have been digitized. The activities include ship tracking, cargo tracking, logistics management, port operations management, communications, and financial transactions. The processes involve the movement of ships, movement of cargo, flow of information and the flow of funds among others. Ports also support several cargo handling procedures, which include loading, offloading, documentation inspection among others. All these recesses are digitized and are thus remotely accessible and can be vulnerable to cyber-attacks. For instance, through remote access to port systems, hackers can execute a "swarming" DDoS strategy that can render a port inoperable for the duration of the swarming (Herzog, 2011). Therefore, identification of processes that are likely to fall victim to cyber-attacks can help imbue some resilience into the processes as well as establish back up processes that ensure cyber-attack incidences do not disrupt service.

People are the leading resource in dealing with cyber-attacks. It is people who issue the commands executed by the automated systems. It is people who monitor these systems. It is peo-

ple who respond to the attacks. Their involvement makes them a critical component in dealing with cybersecurity (Hadlington, 2018).. The people could benefit from frequent training on new security threats to keep up with what is happening around them. The users may be trained in various aspects of cybersecurity such as email, internet usage, passwords, use of antivirus, handling of sensitive information physical security, and reporting of incidents as soon as they occur. People and organizations can create networks for knowledge sharing to share information on new and potential threats, as well as ongoing breaches (Kalogeraki et al., 2018). They can share information instantly and stop attacks before they cause harm to the industry.

Technology is critical in cyber activities and thus vulnerable to cyber-attacks. Using newer secure technologies helps to increase cyber resilience in the maritime industry (Jensen, 2015). Besides providing physical security to information communication technology, assets help to improve protection against direct physical attacks. The stakeholders in the maritime industry should maintain an inventory of their cyber assets and the risk that they are likely to face (Boyes, 2015). The list of potential risks should be updated every time a new risk is reported. They should also maintain possible response approaches to different risks on different assets and also keep update and revising the response as new cybersecurity approaches emerge. Using the available technologies appropriately also can facilitate quick detecting of risk and prompt communication to other stakeholders. For instance electronic data exchange facilitates communication between ships, ships, and ports and between ports (Fruth, Teuteberg, & Liu, 2017). Every ship can easily communicate to other ships around it and also surrounding port, thus ensuring that incident can be communicated promptly. Prompt exchanges result in prompt responses, which in turn minimize losses.

Conclusion

The growth of Information communication technologies and their incorporation in human economic activates occasion the emergence and growth of cybersecurity threats. In response, cybersecurity concerns have hugely been centered around technical protection measures, which largely dictate concentrating on physical security. This approach has hugely neglected the people and processes which have equally huge importance to how the industry detects, deters, and recovers from cybersecurity issues. The current cybersecurity concerns demonstrate the need to have people-oriented, procedural, and technologically oriented guidelines to ensure comprehensiveness of the contingency, response, and recovery plans.

References

Bălan, C. (2018), The disruptive impact of future advanced ICTs on maritime transport: a systematic review, *Supply Chain Management, Vol*. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/SCM-03-2018-0133

Bowen, B. M. (2011). Measuring the Human Factor of Cyber Security. *IEEE International Conference on Technologies for Homeland Security*, 230-235. DOI: 10.1109/ THS.2011.6107876

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review, 5*(4): 28–34.

Bueger, C. (2015). What is Maritime Security? *Maritime Policy, 53*, 159-164.

Fitton, O. P. (2015). *The Future of Maritime Cyber Security*. Lancaster: Lancaster University.

Fruth, M., Teuteberg, F., & Liu, S. (2017). Digitization in maritime logistics—What is there and what is missing?, Cogent Business & Management 4(1). Article: 1411066

Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider. *Psychological and Behavioral Examinations in Cyber Security*, 46-63.

Hareide, O. S. (2018). Enhancing navigator competence by demonstrating maritime cyber security. *The Journal of Navigation, 71*(5), 1025-1039.

Hayes, C. R. (2016). *Maritime Cybersecurity: The Future of National Security*. Monterey, California: Naval Post Graduate School.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*(2), 49-60.

Hoffmann, J. (2018). *Review of Maritime Transport*. New York: UNCTAD.

Jensen, L. (2015). Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*, 5(4): 35–39

Johnston, M. P. (2013). Data Analysis:A Method of whichtheTime Has Come. *Qualitative and Quantitative Methods in Libraries (QQML) 3*:619 –626

Kalogeraki, E-M. Apostolou, D., Polemi, n., & Papastergiou, S.. (2018). Knowledge management methodology for identifying threats in maritime/logistics supply chains. *Knowledge Management Research & Practice, 16*(4), 508-524.

Kimberly, T. K. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy, 3*(2), 147-164.

McPhee, C. K. (2015). Cyber-Resilience in Supply Chains. *Technology Innovation Management Review,* 1-28.

Minim Z. H., & Schramm, H. J. (2018). The impacts of port infrastructure and logistics performance on economic growth: the mediating role of seaborne trade. *Journal of Shipping and Trade 3*(1). doi:10.1186/s41072-018-0027-0